En stärkt förmåga till modern datadelning

– integritetsfrämjande teknik i offentlig förvaltning

Betänkande av Utredningen om integritetsfrämjande teknik i förvaltningen

Stockholm 2026

STATENS OFFENTLIGA UTREDNINGAR

SOU 2026:44

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Multiply Solutions
Tryck och remisshantering: Multiply Solutions, Stockholm 2026

ISBN 978-91-525-1571-6 (tryck)
ISBN 978-91-525-1572-3 (pdf)
ISSN 0375-250X

Till statsrådet Erik Slottner

Regeringen beslutade den 19 juni 2025 att uppdra åt en särskild utredare att analysera förutsättningarna för den offentliga förvaltningen att använda integritetsbevarande metoder vid datadelning och föreslå åtgärder för att främja användningen av sådana metoder. Syftet är att öka den offentliga förvaltningens förmåga att dela data samtidigt som skyddet för uppgifterna upprätthålls.

Som särskild utredare förordnades rättschefen Erik Janzon från och med den 19 juni 2025.

Som utredningssekreterare i utredningen anställdes verksjuristen Fredrik Qvist mellan den 27 juni 2025 och den 31 december 2025 och därefter som huvudsekreterare. Som utredningssekreterare anställdes professorn Alexander Engström från och med den 1 september 2025, rättsliga experten Ann Sofie Silversved från och med den 1 oktober 2025 och utredaren Gabriella Jansson från och med den 9 februari 2026. Den rättsliga experten Liselotte Westerlind har biträtt utredningens sekretariat mellan den 7 januari 2026 och den 31 maj 2026.

Som sakkunniga att biträda utredningen förordnades den 24 september 2025 departementssekreteraren Mathea Franzén (Finansdepartementet), departementssekreteraren Katarina Lindh (Socialdepartementet) och ämnesrådet Alica Selmanovic Monokrousos (Försvarsdepartementet). Alica Selmanovic Monokrousos entledigades den 26 maj 2026.

Som experter att biträda utredningen förordnades den 24 september 2025 specialisten Sarah Amandusson (Myndigheten för digital förvaltning), AI-strategen Gintare Grigonyte (Skatteverket), it- och informationssäkerhetsspecialisten Mats Juhlén (Integritetsskyddsmyndigheten), enhetschefen Jenny Lindberg (Statistiska centralbyrån), rättsliga experten Linda Lindström (eSamverkansprogrammet), verksjuristen Simon Rose (Säkerhetspolisen), närings-

politiske experten Fredrik Sand (TechSverige), förbundsjuristen Olof Widgren (Sveriges Kommuner och Regioner) och verksjuristen Sofie Wildiér (Riksarkivet).

Utredningen, som tagit sig namnet Utredningen om integritetsfrämjande teknik i förvaltningen, överlämnar härmed betänkandet *En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning* (SOU 2026:44). Uppdraget är med detta slutfört.

Stockholm i juni 2026

Erik Janzon

Fredrik Qvist
Alexander Engström
Ann Sofie Silversved
Gabriella Jansson

Innehåll

Sammanfattning **15**

Summary **23**

1 Utredningens uppdrag och arbete **31**

1.1 Uppdraget 31

1.2 Utredningens arbete 32

1.3 Närmare om utredningsuppdraget 32
1.3.1 Syfte och utgångspunkter 32
1.3.2 Ramar och avgränsningar 33

1.4 Angränsande uppdrag av betydelse 34
1.4.1 AI-verkstaden 35
1.4.2 Stärkt samverkan för tillgången till data och utvecklingen av AI 36
1.4.3 Inrättandet av en funktion för främjande av datahantering 37

1.5 Utredningens begreppsanvändning 37
1.5.1 Integritetsfrämjande teknik 38
1.5.2 Data 41
1.5.3 Datadelning 42
1.5.4 Datadriven 43

1.6 Betänkandets disposition 43

2 Integritetsfrämjande teknik och datadelning 45

2.1 Inledning 45

2.2 Digitaliseringspolitiken 45
2.2.1 EU:s digitala decennium och en europeisk dataunion 46
2.2.2 Regeringens strategi för digitaliseringspolitiken 47

2.3 Artificiell intelligens (AI) 48
2.3.1 Regeringens strategi för AI 48
2.3.2 Rättslig reglering av AI 49

2.4 Dataskydd 49
2.4.1 Allmänt om regelverken 49
2.4.2 Grundläggande regler om behandling av personuppgifter 50
2.4.3 Inbyggt dataskydd och dataskydd som standard 53
2.4.4 Anonymisering och pseudonymisering 54

2.5 Offentlighet och sekretess 56
2.5.1 Handlingsoffentlighet 56
2.5.2 Sekretess och tystnadsplikt 56
2.5.3 Delning av data 57

2.6 Informationssäkerhet och cybersäkerhet 58
2.6.1 Informationssäkerhet 58
2.6.2 Cybersäkerhet 59
2.6.3 Säkerhetsskydd 60

3 Beskrivning av integritetsfrämjande teknik 61

3.1 Inledning 61

3.2 Utvecklingen av integritetsfrämjande teknik 61

3.3 Kategorisering av teknikerna 62

3.4 Etablerade avidentifieringstekniker 64
3.4.1 Anonymisering och pseudonymisering 64
3.4.2 Undertryckande 65
3.4.3 Generalisering 65

3.4.4 Randomisering ... 65

3.5 Moderna avidentifieringstekniker ... 66
3.5.1 Differentiell integritet ... 66
3.5.2 Syntetiska data ... 68

3.6 Utmaningar med avidentifieringstekniker ... 70
3.6.1 Utvärdering av vidtagna avidentifieringsåtgärder ... 70
3.6.2 Särskilt om pseudonymisering och kompletterande information ... 71

3.7 Uppgiftsminimerande tekniker ... 71
3.7.1 Federerad inlärning ... 71
3.7.2 Nollkunskapsbevis ... 73

3.8 Tekniker för skyddad bearbetning ... 73
3.8.1 Betrodda exekveringsmiljöer ... 73
3.8.2 Säker flerpartsberäkning ... 75
3.8.3 Homomorf kryptering ... 77

3.9 Framtiden för integritetsfrämjande teknik ... 80
3.9.1 Den kommande utvecklingen ... 80
3.9.2 Kryptering som regel ... 82

4 Användningen av integritetsfrämjande teknik ... 85

4.1 Inledning ... 85

4.2 Nuvarande användning i offentlig förvaltning ... 85
4.2.1 Användningen av moderna tekniker är begränsad ... 86
4.2.2 Användningsområden ... 87
4.2.3 Hinder mot användning ... 87

4.3 Undersökning av den privata marknaden ... 88
4.3.1 Om undersökningen ... 88
4.3.2 Undersökningens resultat ... 89

4.4 Exempel på användning av integritetsfrämjande teknik ... 90
4.4.1 Hälso- och sjukvård ... 90
4.4.2 Brottsförebyggande och brottsbekämpning ... 92
4.4.3 Socialförsäkring ... 94

4.4.4 Cybersäkerhet ... 95
4.4.5 Digitala tjänster och service till medborgare ... 95
4.4.6 Statistik ... 98

5 Styrning och standarder för integritetsfrämjande teknik ... 101

5.1 Inledning ... 101

5.2 Styrningen på EU-nivå ... 102
5.2.1 Förordningsreglerad styrning ... 102
5.2.2 Vägledningar och riktlinjer ... 107
5.2.3 Finansiering ... 107

5.3 Styrningen på nationell nivå ... 108
5.3.1 Statliga myndigheters författningsreglerade uppgifter och regeringsuppdrag ... 108
5.3.2 Vägledningar ... 112

5.4 Exempel på styrning från andra länder ... 113
5.4.1 Integritetsfrämjande teknik i våra grannländer ... 113
5.4.2 Styrning och specialreglering i övriga länder ... 116

5.5 Standarder ... 119
5.5.1 Standardiseringsorganisationer ... 120
5.5.2 Tekniska standarder för integritetsfrämjande teknik ... 124
5.5.3 Standarder för ledningssystem ... 128
5.5.4 Kostnadsfri tillgång till standarder ... 130

6 Möjligheter och hinder för användningen av integritetsfrämjande teknik ... 131

6.1 Inledning ... 131

6.2 Användningen av integritetsfrämjande teknik i förvaltningen bör öka ... 132
6.2.1 Teknikerna möjliggör modern datadelning i förvaltningen ... 132
6.2.2 Det finns flera lämpliga tillämpnings- och användningsområden ... 134

6.2.3 Integritetsfrämjande teknik vid datadelning kan medföra flera betydande nyttor 138
6.2.4 Den tekniska mognadsgraden varierar 143
6.2.5 Ökad användning förbättrar möjligheten att påverka den fortsatta utvecklingen..... 146

6.3 Begränsad kunskap och styrning begränsar användningen av integritetsfrämjande teknik 147
6.3.1 Kunskapen om vissa tekniker är låg 147
6.3.2 Det saknas styrning av användningen 149

6.4 Upplevd juridisk osäkerhet begränsar användningen av integritetsfrämjande teknik..... 150
6.4.1 Osäkerhet om teknikerna får användas..... 150
6.4.2 Osäkerhet om teknikerna har använts i tillräcklig utsträckning..... 151

7 De rättsliga förutsättningarna för att använda integritetsfrämjande teknik vid datadelning..... 153

7.1 Inledning..... 153

7.2 Ramarna för användning av integritetsfrämjande teknik vid datadelning 153
7.2.1 Närmare om dataskydd..... 154
7.2.2 Närmare om sekretess och sekretessbrytande bestämmelser..... 157
7.2.3 Förhållandet mellan teknikerna, dataskyddsregelverket och offentlighets- och sekretessreglerna..... 164

7.3 Det finns rättsliga förutsättningar att använda integritetsfrämjande teknik 166
7.3.1 Teknikerna kan förbättra datadelningen inom befintliga rättsliga ramar 166
7.3.2 Integritetsfrämjande teknik utgör skyddsåtgärder 168
7.3.3 Det måste finnas rättslig grund för att behandla personuppgifter vid användningen av teknikerna..... 170

7.4 Det bör inte införas nya krav för användningen av integritetsfrämjande teknik 172
7.4.1 De krav som finns på att teknikerna ska användas är tillräckliga 172
7.4.2 Det behöver inte införas särskilda krav när teknikerna används 174

7.5 Tillräcklig avidentifiering eller kryptering med integritetsfrämjande teknik 177
7.5.1 Bedömning av om en fysisk person är identifierbar eller om krypterade uppgifter är röjda 178
7.5.2 Det bör förtydligas när vidtagna avidentifieringsåtgärder är tillräckliga 179
7.5.3 Det bör förtydligas när krypterade uppgifter anses röjda 183
7.5.4 Andra åtgärder som offentlig förvaltning kan vidta 184

8 Förslag för att öka användningen av integritetsfrämjande teknik 187

8.1 Inledning 187

8.2 Förslagen ska främja och stödja en ökad användning av integritetsfrämjande teknik 187
8.2.1 Den privata marknadens kompetens bör tillvaratas 188
8.2.2 Styrningen bör vara långsiktig och flexibel 189
8.2.3 Myndigheternas nuvarande ansvars- och expertområden bör beaktas 190

8.3 Funktion för stöd och vägledning 193
8.3.1 Det behövs stöd och vägledning för att öka användningen 193
8.3.2 Digg får i uppdrag att tillhandahålla stöd och vägledning 194
8.3.3 Innehållet i uppdraget att ge stöd och vägledning 197
8.3.4 Uppdraget bör inledningsvis prioritera vissa tekniker 200

8.3.5 Stöd och vägledning ska tas fram i samverkan med berörda myndigheter 202
8.3.6 Uppdragen bör ges i regleringsbrev 203

8.4 Förvaltningsgemensamma tjänster 206
8.4.1 Det behövs förvaltningsgemensamma tjänster för att öka användningen 206
8.4.2 Skatteverket får i uppdrag att tillhandahålla förvaltningsgemensamma tjänster 208
8.4.3 Innehållet i uppdraget att tillhandahålla förvaltningsgemensamma tjänster 210
8.4.4 En förvaltningsgemensam tjänst för säker flerpartsberäkning bör prioriteras 214
8.4.5 Förvaltningsgemensamma tjänster ska utvecklas i samverkan med berörda myndigheter 216
8.4.6 Uppdragen bör ges i regleringsbrev 217

8.5 Finansiering av förvaltningsgemensamma tjänster för integritetsfrämjande teknik 220
8.5.1 Finansieringsmodeller för offentlig förvaltning 220
8.5.2 Offentlig upphandling 221
8.5.3 Statsstöd 222
8.5.4 Konkurrensrätt 225
8.5.5 En förvaltningsgemensam tjänst för säker flerpartsberäkning bör finansieras genom anslag 227
8.5.6 Finansiering av framtida förvaltningsgemensamma tjänster bör bedömas för respektive tjänst 231

8.6 Bearbetning av data i en förvaltningsgemensam tjänst för säker flerpartsberäkning 232
8.6.1 Beskrivning av användningsprocessen för analyser i en förvaltningsgemensam tjänst 232
8.6.2 Personuppgiftsansvaret i en förvaltningsgemensam tjänst 235
8.6.3 Bearbetning i en förvaltningsgemensam tjänst medför att underliggande uppgifter inte röjs 236

8.6.4 Resultatet från en förvaltningsgemensam tjänst är en ny allmän handling 238
8.6.5 Befintligt rättsligt skydd är tillräckligt för data i en förvaltningsgemensam tjänst 239

8.7 Fler åtgärder för att öka datadelningen med integritetsfrämjande teknik..... 241
8.7.1 Det finns behov av uppdrag för att utforska integritetsfrämjande teknik..... 241
8.7.2 Regeringsuppdrag att genomföra en samarbetsanalys med säker flerpartsberäkning ... 242
8.7.3 Regeringsuppdrag att utforska differentiell integritet inom hälso- och sjukvård 244
8.7.4 Regeringsuppdrag för att utforska opt-out-lösning 246

9 Konsekvenser 251

9.1 Inledning 251

9.2 Integritetsfrämjande teknik är en viktig pusselbit för en förbättrad datadelning..... 252
9.2.1 Förutsättningarna för att dela vissa datamängder är i dag begränsade 252
9.2.2 Teknikerna kan möjliggöra en förbättrad datadelning – men kunskapen behöver öka..... 253

9.3 Konsekvenser av att inga åtgärder vidtas för att öka användningen (nollalternativet) 254
9.3.1 Konsekvenser på kortare sikt 255
9.3.2 Konsekvenser på längre sikt 257

9.4 Utredningens förslag för att öka användningen av integritetsfrämjande teknik vid datadelning..... 259
9.4.1 Förslag om stöd och vägledning 259
9.4.2 Förslag om förvaltningsgemensamma tjänster.... 260
9.4.3 Förslag om särskilda regeringsuppdrag 261
9.4.4 Alternativa åtgärder som utredningen har övervägt 261

9.5 Konsekvenser i form av samhällsekonomiska nyttor 265
9.5.1 Nyttopotentialen vid datadelning med teknikerna 265

9.6 Konsekvenser för enskilda 268
9.6.1 Den personliga integriteten 269
9.6.2 Barn och andra särskilt skyddsvärda grupper 271
9.6.3 Jämställdhet och likabehandling 272

9.7 Konsekvenser för företag 272

9.8 Konsekvenser som är gemensamma för offentlig förvaltning 274
9.8.1 Offentliga aktörer som använder teknikerna 274
9.8.2 Digitaliseringen av offentlig förvaltning 275
9.8.3 Effektiviteten i offentlig förvaltning 276
9.8.4 Informationssäkerheten i offentlig förvaltning ... 277
9.8.5 Förpliktelser som följer av EU-rätten 277

9.9 Konsekvenser för kommuner och regioner 278
9.9.1 Betydande nyttor för kommuner och regioner ... 278
9.9.2 Inga ökade kostnader för kommuner och regioner 279
9.9.3 Det kommunala självstyret 279

9.10 Konsekvenser för statliga myndigheter 279
9.10.1 Betydande nyttor för statliga myndigheter 279
9.10.2 Förslagen medför ökade kostnader för statliga myndigheter 280
9.10.3 Förslagens kostnader har vägts mot nyttorna med ökad användning av teknikerna 280
9.10.4 Kostnader för Digg 282
9.10.5 Kostnader för Skatteverket 282
9.10.6 Kostnader för IMY 283
9.10.7 Kostnader för SCB 284
9.10.8 Kostnader för NCSC vid FRA 284
9.10.9 Kostnader för E-hälsomyndigheten 285
9.10.10 Kostnader för Socialstyrelsen 286

9.11 Finansiering av utredningens förslag 286
9.11.1 Stöd och vägledning för integritetsfrämjande teknik 286

9.11.2 Den förvaltningsgemensamma tjänsten för säker flerpartsberäkning 287
9.11.3 Finansiering av kostnaderna för förslagen..... 288

9.12 Tidsplan för uppdragen 290
9.12.1 Uppdragen som avser stöd och vägledning 290
9.12.2 Uppdragen som avser förvaltningsgemensamma tjänster för integritetsfrämjande teknik 291
9.12.3 Uppdraget att utforska en opt-out-lösning med integritetsfrämjande teknik 292

9.13 Uppföljning och utvärdering 292
9.13.1 Uppföljning av teknikernas användning..... 292
9.13.2 Utvärdering av genomförda åtgärder..... 293

Bilagor

Bilaga 1 Kommittédirektiv 2025:64..... 295

Bilaga 2 Samhällsekonomisk analys av potentialen för ökad användning av integritetsfrämjande teknik i offentlig förvaltning 301

Sammanfattning

Integritetsfrämjande teknik

Mängden data i samhället ökar och behovet av data blir allt större. Data kan användas för att förstå samband, fatta välgrundade beslut och hitta nya lösningar. För att uppnå det behöver data kunna delas både inom och mellan organisationer. Datadelningen är dock inget eget syfte, utan är bara ett medel för att nå det egentliga målet som är ökad kunskap. Senare års teknikutveckling har gjort det möjligt att utvinna kunskap ur datamängder från olika delar av en organisation eller från olika organisationer – utan att de underliggande uppgifterna nödvändigtvis tillgängliggörs för de andra parterna. Det innebär att insikter kan delas utan att data tillgängliggörs överhuvudtaget eller i varje fall inte i klartext. Om syftet är att identifiera vissa enskilda personer kan mindre delmängder av uppgifterna delas i klartext.

Teknikerna som hör till denna utveckling brukar samlas under benämningen *integritetsfrämjande teknik* (privacy-enhancing technologies, PET). Det finns ingen enhetlig definition av begreppet men vi använder det som ett samlingsbegrepp för tekniker som bidrar till att stärka skyddet för den personliga integriteten. Vi har i vårt arbete fokuserat på *moderna* integritetsfrämjande tekniker som differentiell integritet (differential privacy), syntetiska data, federerad inlärning, säker flerpartberäkning (secure multi-party computation) och homomorf kryptering. Härutöver finns det även en uppsättning äldre tekniker som vi kallar *etablerade*, främst anonymisering och pseudonymisering, och som vi endast berör i mindre utsträckning.

De moderna integritetsfrämjande teknikerna har på relativt kort tid gått från att vara akademiska produkter till att i dag kunna användas i praktiken. Utvecklingen sker fortsatt snabbt och är i många avseenden ännu i ett tidigt skede. Teknikerna har potential att bidra

till en effektivare offentlig förvaltning, förbättrad service för enskilda samt till att svenska leverantörer av teknikerna kan stärka sin konkurrenskraft internationellt. Det finns i nuläget goda förutsättningar för Sverige att inta en framskjuten position internationellt när det gäller användningen av teknikerna i offentlig förvaltning. Realisering av nyttorna förutsätter emellertid att regeringen och den offentliga förvaltningen mycket snart påbörjar genomtänkta, riktade och välfinansierade insatser. I ett längre perspektiv finns anledning att anta att teknikerna kommer få allmänt utbredd användning och att kryptering successivt utvecklas från att utgöra en kompletterande skyddsåtgärd till att bli standard vid all datahantering – kryptering som regel.

Användningen i offentlig förvaltning är begränsad

I den offentliga förvaltningen används i dag främst etablerade tekniker. Moderna integritetsfrämjande tekniker används endast i begränsad utsträckning. I den mån de används är det i huvudsak i utforskande syfte. Till exempel har federerad inlärning, syntetiska data och betrodda exekveringsmiljöer (trusted execution environment) utforskats i Integritetsskyddsmyndighetens innovationssandlådor.

Även internationellt har de flesta tillämpningar av moderna integritetsfrämjande tekniker hittills haft en utforskande karaktär. Trots detta finns det ett flertal goda exempel som visar på de nyttor som kan uppnås genom användning av sådana tekniker och när teknikerna kombineras med varandra. De internationella användningsfallen visar också att nyttorna med integritetsfrämjande teknik inte är begränsade till ett visst område utan kan finnas inom brottsförebyggande arbete, offentliga tjänster till enskilda, hälso- och sjukvård och statistikverksamhet. Det finns även exempel där användningen av integritetsfrämjande teknik har gått från utforskande till praktisk tillämpning. I Nederländerna används exempelvis säker flerpartsberäkning inom socialförsäkringen för att möjliggöra riktade insatser avseende ett underutnyttjat bidrag.

Integritetsfrämjande teknik möjliggör nya sätt att dela data och kan skapa stora nyttor

Integritetsfrämjande teknik skapar förutsättningar för en modern datadelning genom att göra det möjligt att dela data på nya sätt. Det kan ersätta traditionell datadelning som annars begränsas av dataskyddsregler eller sekretess. Teknikerna kan därmed göra det möjligt att dela eller behandla data på sätt som annars inte hade varit lagligt eller lämpligt. Det utgör ett tydligt exempel på hur den tekniska utvecklingen kan samspela med den juridiska, genom att tekniken gör det möjligt för myndigheter att fullt ut nyttja de utökade legala möjligheterna till datadelning som tillkommit under senare år. Utredningen bedömer att teknikerna är ett viktigt verktyg för att hantera de integritetsrisker som följer av ökad datadelning. Teknikerna kan vara en förutsättning för att de nya reglerna ska vara proportionerliga i praktiken.

Användningen av integritetsfrämjande teknik är relevant för hela den offentliga förvaltningen och bedöms bidra till ökad effektivitet, säkerhet, kvalitet och service samt till bättre beslutsunderlag och ökad innovation. Det samhällsekonomiska nyttopotentialen av ökad och förbättrad datadelning uppskattas till 30–80 miljarder kronor per år, varav 10–40 miljarder kronor bedöms vara direkt beroende av att integritetsfrämjande teknik används.

Den begränsade användningen beror på en låg kunskapsnivå, upplevd osäkerhet och bristande styrning

Utredningen har identifierat tre faktorer som bidrar till att integritetsfrämjande teknik enbart används i begränsad utsträckning i offentlig förvaltning. Det främsta hindret är att den offentliga förvaltningen saknar kunskap om integritetsfrämjande teknik. Det gäller kunskap om såväl teknikerna som deras användningsområden och vilka nyttor som användningen kan skapa. Att det finns en begränsad kunskap leder till att den offentliga förvaltningen upplever en osäkerhet om när och hur teknikerna kan användas samt om det finns rättsliga förutsättningar för att använda teknikerna. Vidare saknas det styrning, främst på nationell nivå, för användningen av teknikerna. Det finns inte heller några statliga myndigheter med utpekat

ansvar eller något uppdrag som avser integritetsfrämjande teknik, till exempel för att främja och stödja användningen.

Detta leder sammantaget till att användningen är fragmenterad och att de moderna teknikerna används i liten omfattning eller inte alls. För att öka användningen av integritetsfrämjande teknik i syfte att förbättra datadelningen inom offentlig förvaltning krävs det att kunskapsnivån ökar och att det finns tydligare nationell styrning.

Det finns rättsliga förutsättningar för att använda integritetsfrämjande teknik

Integritetsfrämjande teknik kan möjliggöra datadelning utan att personuppgifter eller andra skyddsvärda uppgifter röjs, vilket innebär att informationsutbyte som annars inte hade varit tillåtet av integritetsskäl kan genomföras med bibehållet skydd för enskilda. Genom exempelvis säker flerpartsberäkning och federerad inlärning kan gemensamma analyser och träning av AI-modeller ske utan att underliggande data delas i klartext.

I dataskyddsförordningen finns det krav på att personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder, såsom pseudonymisering och kryptering. Utredningen bedömer att integritetsfrämjande teknik är sådana skyddsåtgärder. Teknikerna bör därför användas när det är lämpligt. Även Europeiska dataskyddstyrelsen och Integritetskyddsmyndigheten har bedömt att integritetsfrämjande teknik utgör skyddsåtgärder.

Användningen av integritetsfrämjande teknik ger inte någon egen rätt till datadelning utan den rätten måste följa av annan lagstiftning, till exempel offentlighets- och sekretesslagen (2009:400). Teknikerna kan användas för att möjliggöra eller säkra en i grunden redan laglig datadelning. Bearbetningen med teknikerna sker även för samma ändamål som datadelningen. Det innebär att det bakomliggande syftet med datadelningen är avgörande för om bearbetningen med integritetsfrämjande teknik är tillåten eller inte.

Stöd och vägledning ska öka kunskapsnivån

Utredningen bedömer att offentlig förvaltning behöver ökad kunskap om integritetsfrämjande teknik för att stärka förmågan att använda teknikerna vid datadelning. Det behöver därför finnas en myndighet med ett övergripande ansvar för att tillhandahålla stöd och vägledning om integritetsfrämjande teknik till den offentliga förvaltningen. För att göra det på ett effektivt och ändamålsenligt sätt behöver den offentliga förvaltningen även ta tillvarata den kunskap och expertis som finns på den privata marknaden.

Vi föreslår att Myndigheten för digital förvaltning (Digg) får ett utpekat ansvar för stöd och vägledning. Vägledningen bör syfta till att stärka förvaltningens egen förmåga att använda teknikerna på ett verksamhetsanpassat sätt. Det bör kompletteras med mer praktiskt inriktat stöd, såsom metodstöd och riktade utbildningar. Mot bakgrund av Diggs ansvar för förvaltningsgemensam digitalisering, den nationella digitala infrastrukturen Ena samt myndighetens etablerade kompetens och strukturer för stöd och vägledning till hela förvaltningen är det lämpligt att myndigheten får i uppdrag att stödja användningen av integritetsfrämjande teknik. För att ta vara på den offentliga förvaltningens samlade kompetens och expertis ska Digg samverka med Integritetsskyddsmyndigheten, Skatteverket, Statistiska centralbyrån och Nationellt cybersäkerhetscenter vid Försvarets radioanstalt.

Stödet från Digg bör omfatta integritetsfrämjande teknik generellt, men särskild prioritet bör inledningsvis ges åt syntetiska data och differentiell integritet. Dessa tekniker kan i många fall ersätta etablerade avidentifieringstekniker och är centrala för ökad användning av AI i offentlig förvaltning. Utredningen bedömer även att det finns ett särskilt behov av vägledning om hur risken för återidentifiering ska utvärderas, för att minska den upplevda osäkerheten vid användning av avidentifieringstekniker. Sådan vägledning kommer också stödja en korrekt tillämpning vid skapande av syntetiska data och användning av differentiell integritet.

Förvaltningsgemensamma tjänster ska underlätta användningen

Många offentliga aktörer saknar i dag tillräcklig kunskap, erfarenhet och teknisk kompetens för att självständigt kunna använda integritetsfrämjande teknik. Det riskerar att leda till överdriven försiktighet och till att nyttorna med datadelning inte realiseras. Vissa integritetsfrämjande tekniker, till exempel säker flerpartsberäkning, ställer höga krav på kompetens och it-kapacitet vilket kan vara en utmaning, framför allt för mindre kommuner och myndigheter. För att sänka tröskeln för användning behöver kunskapshöjande insatser därför kombineras med förvaltningsgemensamma tjänster.

Utredningen bedömer att förvaltningsgemensamma tjänster för integritetsfrämjande teknik kan motverka bristfällig implementering samt minska risken för fragmentering och dubbelarbete. Tjänsterna kan också säkerställa en enhetlig och rättssäker tillämpning. Sådana tjänster kan omfatta plattformar, testmiljöer, testbäddar och tekniskt stöd, inklusive tjänster som på olika sätt stödjer användningen av integritetsfrämjande teknik.

Vi föreslår att Skatteverket får i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik. Myndigheten har hög it-kapacitet och är en viktig aktör i många datadelningssituationer eftersom myndigheten bland annat ansvarar för folkbokföringsregistret. Utredningen föreslår även att de förvaltningsgemensamma tjänsterna för integritetsfrämjande teknik ska ingå i Ena.

Vilka förvaltningsgemensamma tjänster för integritetsfrämjande teknik som bör tillhandahållas ska i huvudsak styras av behov och teknisk utveckling, och uppdraget bör inte vara begränsat till specifika tekniker. Särskild prioritet bör dock ges åt tekniskt mogna och brett användbara tekniker med stor potential men som i dag endast används i begränsad utsträckning. Vi bedömer att säker flerpartsberäkning är en sådan teknik, eftersom tekniken möjliggör säker analys över organisationsgränser utan att underliggande uppgifter delas, samtidigt som datakvaliteten bibehålls. Utredningen föreslår därför att Skatteverket särskilt ska prioritera att ta fram en förvaltningsgemensam tjänst för säker flerpartsberäkning. Tekniken anses vara väl lämpad för hantering av särskilt skyddsvärda uppgifter

och kan stärka förmågan till modern datadelning inom offentlig förvaltning.

För att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik på ett effektivt och ändamålsenligt sätt behöver Skatteverket tillvarata den kompetens som finns på den privata marknaden. Skatteverket ska också samverka med Digg, Integritetsskyddsmyndigheten, Statistiska centralbyrån och Nationella cybersäkerhetscentret vid Försvarets radioanstalt.

Riktade uppdrag ska starta användningen

Utredningen bedömer att det krävs ett aktivt genomförande för att integritetsfrämjande teknik ska få genomslag i offentlig förvaltning. Detta kan ske genom att regeringen ger utvalda statliga myndigheter i uppdrag att i praktiken utforska teknikerna. Redovisningar från sådana uppdrag kan leda till att erfarenheter och resultat systematiskt sprids för att främja bredare användning.

Utredningen föreslår att Försäkringskassan och Skatteverket ska få i uppdrag att testa säker flerpartsberäkning. Dessa myndigheter har kapacitet att omhänderta ny teknik och nya arbetssätt på ett effektivt sätt. Myndigheterna har också behov av att dela data med varandra i olika situationer.

Utredningen föreslår också att Socialstyrelsen ska få i uppdrag att utforska användningen av differentiell integritet inom hälso- och sjukvården. En ökad användning av differentiell integritet förutsätter tydlig vägledning, särskilt avseende valet av nivån för tillåten integritetsförlust och hur tekniken kan kombineras med andra metoder, så som syntetiska data. Tidiga tillämpningar inom integritetskänsliga områden kan dessutom ge vägledande erfarenheter för andra sektorer.

Vi föreslår även att E-hälsomyndigheten och Socialstyrelsen ska få i uppdrag att utforska om integritetsfrämjande teknik kan användas för opt-out-lösningar inom ramen för det europeiska hälsodataområdet (EHDS). Möjligheten för enskilda att motsätta sig användningen av sina personuppgifter är av intresse även i andra sammanhang inom offentlig förvaltning vilket gör att myndigheternas slutsatser kan återanvändas.

Summary

Privacy-enhancing technologies (PET)

The amount of data in society and the demand for it is increasing. Data can be used to understand patterns, support well-informed decision-making and identify new solutions. To achieve this, data needs to be shared both within and between organisations. However, data sharing is not the goal but rather a means to achieve the overarching objective of increased knowledge. Recent technological developments have made it possible to extract insights from datasets held in different parts of an organisation or across multiple organisations without necessarily making the underlying data accessible to the other parties. This means that insights can be shared without sharing the data itself, or at least not in a readable form. If the purpose is to identify specific individuals, smaller subsets of the data may be shared in readable form.

The technologies associated with this development are commonly referred to as *privacy-enhancing technologies* (PET). Although there is no single, universally accepted definition, the term is used here as an umbrella concept for technologies that contribute to strengthening the protection of individual privacy. This inquiry focuses on *modern* PETs such as differential privacy, synthetic data, federated learning, secure multi-party computation and homomorphic encryption. In addition to these, there is a set of older, *established* technologies, primarily anonymisation and pseudonymisation, which are addressed only to a limited extent.

Modern PETs have, within a relatively short period, developed from academic concepts into tools that now can be applied in practice. Technological development continues at a rapid pace and is still, in many respects, at an early stage. PETs have the capacity to contribute to a more efficient public administration, improve services

for individuals and strengthen the international competitiveness of Swedish PET providers. At present, Sweden has potential to assume a leading role internationally in the use of PETs within public administration. However, the realisation of the associated benefits requires the Government and public authorities to initiate well-considered, targeted and adequately funded measures in the near future. In the longer term, it is reasonable to expect that these technologies will become widely adopted and that encryption will become the rule for all data processing activities rather than the exception, as is the case today.

Use of PETs in public administration is limited

Within public administration, established technologies are currently the most widely used. Modern PETs are used only to a limited extent, and they are primarily for exploratory contexts. For example, federated learning, synthetic data and trusted execution environments have been explored in the regulatory sandboxes of the Swedish Authority for Privacy Protection.

Internationally, most applications of modern privacy-enhancing technologies have also been exploratory. Despite this, there are several good examples that show the benefits of using PETs and when these technologies are combined. International use cases also show that the benefits of using PETs are not confined to a single domain but can be realised in areas such as crime prevention, the provision of public services to citizens, healthcare and statistics. There are also examples where the use of PETs has moved from exploration to practical application. In the Netherlands, secure multi-party computation is used within the social security system to enable targeted measures in relation to an underutilised benefit.

PETs enable new ways of sharing data and can generate significant benefits

PETs enable modern data sharing by making it possible to share data in new ways. This can replace traditional forms of data sharing that would otherwise be constrained by data protection regulations or secrecy provisions. PETs may thus enable the sharing or process-

sing of data in ways that would otherwise not have been lawful or appropriate. This constitutes a clear example of how technological and legal developments can interact, as the technology enables public authorities to fully make use of the expanded legal possibilities for data sharing introduced in recent years. The inquiry considers these technologies to be a key tool for managing the privacy risks associated with increased data sharing, and they may also in some cases be a prerequisite for ensuring that the new legislations are proportionate in practice.

The use of PETs is relevant across the public administration and is considered to contribute to increased efficiency, security, quality and service, as well as to improved knowledge bases and greater innovation. The socio-economic value of increased and improved data sharing is estimated at SEK 30–80 billion per year, of which SEK 10–40 billion is assessed to be directly dependent on the use of PETs.

Limited use due to low level knowledge, perceived uncertainty and insufficient governance

The inquiry has identified three factors that contribute to the limited use of PETs within public administration. The primary obstacle is a lack of knowledge about PETs. This includes knowledge of the technologies, their areas of application and the potential benefits their use can generate. The limited level of knowledge contributes to a perceived uncertainty within the public administration regarding when and how PETs can be used, as well as whether there are adequate legal conditions for their use. In addition, there is a lack of governance, primarily at the national level, concerning when and how these technologies should be applied. There are also no government agencies with a clearly designated responsibility or mandate relating to PETs, for example to promote and support their use.

Overall, this results in fragmented use, with modern technologies being applied only to a limited extent or not at all. In order to increase the use of PETs with the aim to improve data sharing within public administration, the level of knowledge must increase and clearer national governance is required.

Legal preconditions for the use of PETs

PETs can enable data sharing without disclosing personal data or other sensitive information. This means that information exchange which would otherwise not be permitted for privacy reasons may be carried out while maintaining the protection of individuals. For example, secure multi-party computation and federated learning allow joint analyses and training of AI-models to take place without sharing the underlying data in plain text.

The General Data Protection Regulation requires controllers to implement appropriate technical and organisational measures, such as pseudonymisation and encryption. The inquiry considers PETs to constitute a safeguard that should be used where appropriate. This is consistent with the assessments made by the European Data Protection Board and the Swedish Authority for Privacy Protection.

The use of PETs does not in itself confer any right to share data; such a right must follow from other legislation, for example the Public Access to Information and Secrecy Act (2009:400). PETs can be used to enable or secure data sharing that is already lawful in principle. The processing is also carried out for the same purposes as the data sharing. Consequently, the lawfulness of processing through PETs depends on the underlying purpose of data sharing.

Support and guidance to raise the knowledge level

The inquiry assesses that the public administration requires increased knowledge of PETs in order to enhance their ability to use PETs in data sharing. There is therefore a need to assign a public authority overall responsibility for providing support and guidance on PETs to the public administration. To ensure effectiveness and appropriateness, the public administration should also use the knowledge and expertise available in the private sector.

We propose that the Agency for Digital Government (Digg) should be assigned a specific responsibility for the provision of such support and guidance. The guidance should aim to strengthen the capacity of public authorities to apply PETs in a manner tailored to their operational needs. It should also be complemented by more practice-oriented measures, such as methodological support and targeted training. Considering Digg's responsibility for public sector-

wide digitalisation, the national digital infrastructure Ena, as well as Digg's established structures and expertise for providing support and guidance across the public administration, it is appropriate to entrust the agency with this task. In order to make effective use of the public sector's collective expertise, Digg should cooperate with the Swedish Authority for Privacy Protection, the Swedish Tax Agency, Statistics Sweden, and the National Cyber Security Centre at the National Defence Radio Establishment.

The support provided by Digg should cover PETs in general; however, initial priority should be given to synthetic data and differential privacy. These technologies can replace the use of established technologies and are of particular importance for the increased use of AI in public administration. The inquiry further considers that there is a specific need for guidance on the assessment of re-identification risks, to reduce uncertainty regarding the application of de-identification techniques. Such guidance would also facilitate the correct application of methods for generating synthetic data and implementing differential privacy.

Government-wide services shall simplify the use of PETs

Several public organisations currently lack sufficient knowledge, experience and technical capacity to independently use PETs. This may lead to excessive caution and prevent the benefits of data sharing from being fully realised. Certain PETs, such as secure multi-party computation, entail high requirements in terms of expertise and IT capacity, which may pose particular challenges, especially for smaller public authorities. In order to lower the threshold for use, measures aimed at increasing knowledge should therefore be combined with government-wide services for PETs.

The inquiry considers that government-wide services for PETs can mitigate the risk of inadequate implementation and reduce fragmentation and duplication of efforts. They can also help ensure a consistent and legally sound application of the regulatory framework. Such services may include platforms, test environments, testbeds and technical support, including services for penetration testing and the preparation and adaptation of data prior to processing.

We propose that the Swedish Tax Agency should be entrusted with the task of providing government-wide services for PETs. The agency has significant IT capacity and is a key actor in many data-sharing contexts, due to its responsibility for the Swedish population register. The inquiry further proposes that such government-wide services for PETs should be integrated into the national digital infrastructure Ena.

As a general rule, the types of government-wide services for PETs should be determined by needs and technological developments, rather than being limited to specific technologies. Priority should, however, be given to technically mature and broadly applicable technologies with significant potential that are currently used only to a limited extent. The inquiry considers secure multi-party computation to be such a technology, as it enables secure analysis across organisational boundaries without sharing the underlying data, while maintaining data quality.

The inquiry therefore proposes that the Swedish Tax Agency should give specific priority to the development of a government-wide service for secure multi-party computation. This technology is well suited for the processing of particularly sensitive data and will strengthen the ability of modern data sharing within public administration.

In order to provide government-wide services for PETs in an effective and appropriate manner, the Swedish Tax Agency will need to make use of the expertise available in the private sector. The agency will also need to cooperate with Digg, the Swedish Authority for Privacy Protection, Statistics Sweden, and the National Cyber Security Centre at the National Defence Radio Establishment.

Targeted assignments shall initiate use of PETs

The inquiry considers that, although the necessary legal conditions are in place, a more proactive approach is required for PETs to gain traction within the public administration. This can be achieved by the Government assigning certain government agencies to explore the practical application of PETs. Reports from such assignments may contribute to the systematic dissemination of experiences and results, thereby promoting broader uptake.

We propose that the Swedish Social Insurance Agency and the Swedish Tax Agency should be tasked with testing secure multi-party computation. These agencies have the capacity to adopt new technologies and new ways of working efficiently. They also have a need to share data with each other in various contexts.

The inquiry further proposes that the National Board of Health and Welfare should be tasked with exploring the use of differential privacy within the healthcare sector. Increased use of differential privacy requires clear guidance, particularly regarding the choice of acceptable levels of privacy loss and how the technology can be combined with other methods, such as synthetic data. Early applications in privacy-sensitive areas may also provide valuable guidance for other areas.

We also propose that the Swedish eHealth Agency and the National Board of Health and Welfare should be tasked with exploring whether PETs can be used to support opt-out solutions within the context of the European Health Data Space (EHDS). The possibility for individuals to object to the use of their individual data is also relevant in other contexts within public administration, meaning that the agencies' findings can be reused.

1 Utredningens uppdrag och arbete

1.1 Uppdraget

Regeringen beslutade den 19 juni 2025 att ge en särskild utredare i uppdrag att analysera förutsättningarna för den offentliga förvaltningen att använda integritetsbevarande metoder vid datadelning och föreslå åtgärder som kan främja användningen av sådana metoder. Syftet är att öka den offentliga förvaltningens förmåga att dela data samtidigt som skyddet för uppgifterna upprätthålls.

Utredaren ska bland annat

- analysera förutsättningarna för myndigheter och andra aktörer i den offentliga förvaltningen att använda integritetsbevarande metoder vid datadelning och föreslå hur användningen kan förbättras,
- bedöma om det finns behov av att införa särskilda krav vid användning av integritetsbevarande metoder och i så fall lämna förslag på hur kraven bör regleras,
- analysera om en eller flera myndigheter bör ges i uppdrag att utveckla och tillhandahålla gemensamma tekniska tjänster, testmiljöer, testbäddar eller plattformar för integritetsbevarande metoder för datadelning,
- bedöma och lämna förslag på hur en funktion för rådgivning till den offentliga förvaltningen om datadelning och användning av integritetsbevarande metoder kan utformas och organiseras, och
- lämna nödvändiga författningsförslag.

1.2 Utredningens arbete

Utredningens arbete påbörjades den 4 augusti 2025. Utredningen har under arbetets gång, i enlighet med direktivet, inhämtat synpunkter och fört dialog med statliga myndigheter, kommuner, regioner, företag, universitet och högskolor. Vi har även inhämtat synpunkter från bland annat Myndigheten för digital förvaltning (Digg), Integritetsskyddsmyndigheten (IMY), Statistiska centralbyrån (SCB) och Nationellt cybersäkerhetscenter (NCSC) vid Försvarets Radioanstalt (FRA).

Utredningen har genomfört en enkätundersökning hos ett urval av statliga myndigheter, kommuner och regioner. Vi har också arrangerat två workshoppar där företrädare från statliga myndigheter, kommuner och regioner deltagit. Detta för att få en bild av hur integritetsfrämjande teknik används i den offentliga förvaltningen[1]. Därutöver har vi genomför en workshop med representanter från den privata sektorn i syfte att få deras syn på marknaden för integritetsfrämjande teknik.

Utredningen har även gett forskningsinstitutet RISE (Research Institutes of Sweden) i uppdrag att genomföra en samhällsekonomisk analys av de potentiella nyttor och kostnader som införandet av integritetsfrämjande teknik skulle innebära för offentlig förvaltning. Analysen har använts som underlag för våra bedömningar och förslag. Den återfinns även som bilaga[2] i betänkandet.

1.3 Närmare om utredningsuppdraget

1.3.1 Syfte och utgångspunkter

Utredningsuppdraget omfattar två huvudsakliga delar. Utredningen ska dels analysera de rättsliga förutsättningarna för att använda integritetsfrämjande teknik vid datadelning i den offentliga förvaltningen, dels föreslå organisatoriska och infrastrukturella lösningar för gemensamt stöd. Syftet med utredningen är enligt direktivet att öka den offentliga förvaltningens förmåga att dela data samtidigt som skyddet för uppgifterna upprätthålls. Utredningen uppfattar att det över-

[1] I betänkandet används fortsättningsvis begreppet integritetsfrämjande teknik i stället för integritetsbevarande metoder, se vidare avsnitt 1.5.1.
[2] Bilaga 2, *Samhällsekonomisk analys av potentialen för ökad användning av integritetsfrämjande teknik i offentlig förvaltning*.

gripande syftet med utredningen därmed är att genom en ökad användning av integritetsfrämjande teknik bidra till en utveckling som innebär att förvaltningen får tillgång till mer ändamålsenliga och heltäckande beslutsunderlag. Det kan i sin tur kan leda till en mer effektiv förvaltning, förbättrad service och mer ändamålsenliga tjänster till enskilda och företag. Därmed skapas bättre förutsättningar för innovation och förvaltningens möjligheter att främja samhällsutvecklingen.

Utgångspunkten för utredningen är *hur* integritetsfrämjande teknik kan användas som ett verktyg för att möjliggöra datadelning i den offentliga förvaltningen där det annars inte skulle vara möjligt på grund av sekretess- eller dataskyddsregelverket. Utredningens uppdrag är alltså att förbättra förutsättningarna för datadelning genom användning av integritetsfrämjande teknik. I uppdraget ingår inte att reglera nya skyldigheter att dela data inom den offentliga förvaltningen. Utredningen utgår därför från att delning av data ska ske i enlighet med befintliga rättsliga förutsättningar, vilket innebär att delning av data måste vara förenligt med dataskyddsförordningen[3] och kompletterande nationell reglering om skydd för personuppgifter. Datadelningen måste också vara förenlig med befintliga bestämmelser i offentlighets- och sekretesslagen (2009:400), OSL.

1.3.2 Ramar och avgränsningar

Utredningens uppdrag omfattar användning av integritetsfrämjande teknik vid datadelning inom offentlig förvaltning. Av direktiven framgår att statliga myndigheter och andra aktörer inom den offentliga förvaltningen, inklusive kommuner, regioner, privata utförare, kommunalförbund och kommunala bolag producerar, inhämtar och förvaltar stora mängder data.

Utredningen konstaterar att begreppet offentlig förvaltning bör tolkas utifrån uppdragets syfte. Det bör därför inte spela någon roll hur den offentliga förvaltningen har valt att utföra en viss verksamhet som åligger den. Det finns andra aktörer inom den offentliga förvaltningen som utför offentliga uppgifter. Som exempel kan nämnas att kommuner och regioner får överlåta skötseln av kom-

[3] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

munala angelägenheter till kommunala bolag, stiftelser, föreningar och privata utförare, under förutsättning att detta inte strider mot lag och att vissa villkor är uppfyllda.[4] Mot bakgrund av syftet med utredningens uppdrag innebär det att även bolag, privata utförare och andra som hanterar statliga eller kommunala angelägenheter kan komma att omfattas av utredningens uppdrag eftersom data rörande vissa angelägenheter kan förvaras även hos dem. Det hindrar dock inte att utredningens förslag och bedömningar i vissa avseenden kommer att begränsas till att endast beröra vissa aktörer inom den offentliga förvaltningen.

När det gäller forskningsverksamhet vid universitet och högskolor kan utredningen konstatera att statliga lärosäten är egna myndigheter och ingår i den offentliga förvaltningen. Av direktivet framgår dock att forskningsverksamhet vid universitet och högskolor inte ska omfattas av utredningen, eftersom denna verksamhet styrs av internationellt vägledande principer för öppna forskningsdata och datahantering, de så kallade FAIR-principerna. Enligt FAIR-principerna ska forskningsdata vara sökbara (Findable), tillgängliga (Accessible), interoperabla (Interoperable) och återanvändningsbara (Reusable).[5]

Integritetsfrämjande teknik förknippas ofta med datadelning, men teknikerna används även i syfte att stärka skyddet för den personliga integriteten internt inom en organisation. Eftersom utredningens uppdrag är avgränsat till att förbättra förutsättningarna för datadelning behandlas dock inte sådan intern användning av teknikerna inom ramen för detta betänkande. Detta utesluter dock inte att det finns bedömningar som är tillämpliga även på sådan intern användning.

1.4 Angränsande uppdrag av betydelse

Efter att regeringen fattat beslut om att tillsätta denna utredning har regeringen gett nya uppdrag till Skatteverket, Försäkringskassan, Myndigheten för digital förvaltning (Digg) och Statistiska centralbyrån (SCB) som i vissa avseenden angränsar till vår utredning. Det

[4] 3 kap. 11–12 §§ och 10 kap. 3–4 §§ kommunallagen (2017:725).
[5] https://www.vr.se/analys/rapporter/vara-rapporter/2021-10-28-vagledning-for-implementering-av-kriterier-for-fair-forskningsdata.html (hämtad 2026-03-26).

finns därför anledning att kort redogöra för och kommentera dessa uppdrag.

1.4.1 AI-verkstaden

Regeringen gav i juli 2025 Försäkringskassan och Skatteverket i uppdrag att utreda förutsättningarna för en AI-verkstad för den offentliga förvaltningen. Myndigheterna skulle även lämna förslag till hur AI-verkstaden skulle kunna utformas, etableras, förvaltas och finansieras.[6]

Myndigheternas redovisning av uppdraget pekar bland annat på ett omfattande behov när det gäller AI i offentlig förvaltning. Det gäller behov av miljöer för utforskande, utvecklingsstöd och stöd vid upphandling, men även tillgång till säkra AI-tjänster och behov av gemensamma lösningar, samt samverkan i rättsliga bedömningar.

För att möta dessa utmaningar och behov föreslog Försäkringskassan och Skatteverket att AI-verkstaden ska tillhandahålla

- stöd och rådgivning,
- kvalitetsgranskade AI-tjänster, samt
- en teknisk plattform bestående av en labbmiljö för experiment och innovation, utvecklingsmiljö och produktionsmiljö.

För att underlätta för användare föreslog Försäkringskassan och Skatteverket att det skapas en portal som fungerar som en väg in till AI-verkstaden. Denna portal kan också fungera som en samlad källa till vägledning i olika AI-relaterade frågor från flera myndigheter.[7]

I januari 2026 gav regeringen i uppdrag till Försäkringskassan och Skatteverket att etablera en AI-verkstad för offentlig förvaltning. Av uppdraget framgår att AI-verkstaden ska omfatta funktioner och tjänster som bedöms möjliga att erbjuda inom ramen för gällande rätt samt tekniska och organisatoriska förutsättningar. En AI-verkstad i begränsad skala ska tas i bruk senast den 1 juli 2026.[8]

---

[6] Finansdepartementet, Fi2025/01523, *Uppdrag till Försäkringskassan och Skatteverket att utreda förutsättningarna för en AI-verkstad för den offentliga förvaltningen*.
[7] Försäkringskassan och Skatteverket, FK 2025/016953 och SKV 8-8583-2026, *Svar på regeringsuppdraget att utreda förutsättningarna för en AI-verkstad för den offentliga förvaltningen*, s. 112–118.
[8] Finansdepartementet, Fi2026/00018, *Uppdrag till Försäkringskassan och Skatteverket att etablera en AI-verkstad för den offentliga förvaltningen*.

Integritetsfrämjande teknik i AI-verkstaden

Försäkringskassan och Skatteverket har i sin redovisning av uppdraget att utreda förutsättningarna för en AI-verkstad betonat vikten av integritetsfrämjande teknik för att analysera information och träna modeller utan att enskilda individers information röjs. Av redovisningen framgår att om vissa integritetsfrämjande tekniker integreras från början i AI-verkstadens ansvar, infrastruktur samt rådgivning och stöd, skapas förutsättningar för att den offentliga förvaltningen ska kunna dela och använda data enligt gällande reglering. Det skapar också förutsättningar för att utveckla AI-lösningar och att i övrigt kunna samverka på ett effektivt, säkert och robust sätt. Enligt redovisningen bidrar ett sådant arbetssätt även till att uppfylla kraven i dataskyddsförordningen vad gäller inbyggt dataskydd och dataskydd som standard. Det påpekas samtidigt att utvecklingen inom integritetsfrämjande teknik går mycket fort. Tillämpningen av teknikerna behöver därför löpande följas upp under AI-verkstadens etablering och förvaltning.[9]

1.4.2 Stärkt samverkan för tillgången till data och utvecklingen av AI

Regeringen gav i januari 2026 Digg i uppdrag att lämna förslag till en nationell samverkansstruktur för myndigheter och andra aktörer i syfte att stärka förmågan att kontinuerligt och över tid utveckla säkra och effektiva tjänster för data och AI.[10] Uppdraget ingår i handlingsplanen för AI-strategin[11]. Regeringen anger att samverkansstrukturen bland annat ska kunna utgöra ett stöd för den offentliga förvaltningen när tjänster för data eller AI tas fram eller vidareutvecklas. Den ska också kunna underlätta för svenska aktörer att ansöka om medel från fonder och program inom EU som rör data, AI, beräkningsförmåga, lagring och konnektivitet.

Inom ramen för uppdraget har Digg beaktat det arbete som bedrivs av denna utredning. Uppdraget slutredovisades den 29 maj 2026. I redovisningen lämnar Digg förslag på hur en nationell sam-

[9] Försäkringskassan och Skatteverket, *Svar på regeringsuppdraget att utreda förutsättningarna för en AI-verkstad för den offentliga förvaltningen*, s. 37 f.
[10] Finansdepartementet, Fi2026/00137, *Uppdrag till Myndigheten för digital förvaltning att föreslå en samverkansstruktur för utveckling av tjänster för data och artificiell intelligens.*
[11] Finansdepartementet, 2026, *Sveriges AI-strategi.*

verkansstruktur kan organiseras som en samordnande och stödjande funktion för utvecklingen av data och AI inom förvaltningen. Myndigheten lämnar även förslag på komponenter och system som bör utvecklas för att förbättra tillgången till data, särskilt i situationer där data behöver göras tillgängliga utan att överföras.[12] Digg konstaterar bland annat att användningen av integritetsfrämjande teknik i många fall är en förutsättning för att dela data. Digg bedömer vidare att integritetsfrämjande tekniker behöver synliggöras och stödjas inom de förmågor som myndigheten föreslår.[13]

1.4.3 Inrättandet av en funktion för främjande av datahantering

Regeringen gav i april 2026 Digg och SCB i uppdrag att förbereda inrättandet av en ny funktion vid SCB som ska främja god datahantering inom offentlig förvaltning. Funktionen ska kunna ge vägledning till aktörer inom förvaltningen för att skapa en god datahantering. I uppdraget ingår att utforma rutiner och arbetssätt, som bygger på aktuella ramverk och processer för datakvalitet, samt utgår från etablerade klassifikationer och tillämpliga standarder. Syftet med funktionen är att bidra till en mer säker och effektiv dataförvaltning, minskade administrativa kostnader och minskat uppgiftslämnande för olika aktörer.

SCB har i juni 2026 lämnat en delredovisning av uppdraget till Regeringskansliet. Senast den 29 januari 2027 ska Digg och SCB lämna en slutredovisning av uppdraget.[14]

1.5 Utredningens begreppsanvändning

I betänkandet används vissa begrepp som är centrala för utredningens uppdrag och förslag. Flera av dem förekommer i lagstiftning och i internationella sammanhang. I detta avsnitt beskrivs vad som avses när dessa begrepp används i betänkandet.

---

[12] Myndigheten för digital förvaltning (Digg), 2026-00634, *Förslag på samverkansstruktur och tjänster för data och AI*, s. 25 f.
[13] Digg, *Förslag på samverkansstruktur och tjänster för data och AI*, s. 53 f.
[14] Finansdepartementet, Fi2026/00909, *Uppdrag till Myndigheten för digital förvaltning och Statistiska centralbyrån att förbereda inrättandet av en funktion för främjande av datahantering*.

1.5.1 Integritetsfrämjande teknik

Begreppsanvändningen för tekniker som syftar till att skydda den personliga integriteten varierar i EU:s rättsakter. Olika engelska och svenska termer förekommer, vilket skapar en viss terminologisk oenhetlighet. I dataförvaltningsförordningen[15] används den engelska termen privacy-preserving methods och den svenska termen integritetsbevarande metoder.[16] I AI-förordningen[17] förekommer i stället privacy-enhancing techniques på engelska och integritetsbevarande teknik på svenska.[18] Vidare används i dataförordningen[19], förordningen om europeisk statistik[20] samt förordningen om europeisk statistik om befolkning och bostäder[21] det engelska begreppet privacy-enhancing technologies, vilket i de svenska språkversionerna översätts till integritetsfrämjande teknik.[22] Utredningens bedömning är att begreppen i allt väsentligt avser samma sak, även om olika termer används.

Internationellt går trenden mot att använda privacy-enhancing technologies som det mest etablerade engelska begreppet. Exempelvis använde Förenta nationerna (FN) tidigare termen privacy-preserving technologies (PPT), vilken har beskrivits som något snävare än privacy-enhancing technologies (PET).[23] Numera an-

[15] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[16] Artikel 7.4 c i dataförvaltningsförordningen.
[17] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).
[18] Skäl 67 i AI-förordningen.
[19] Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen).
[20] Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program.
[21] Europaparlamentets och rådets förordning (EU) 2025/2458 av den 26 november 2025 om europeisk statistik om befolkning och bostäder, om ändring av förordning (EG)nr 862/2007 och om upphävande av förordningarna (EG) nr 763/2008 och (EU) nr 1260/2013.
[22] Artikel 49.1 a i dataförordningen, artikel 12.3 b i förordningen om europeisk statistik om befolkning och bostäder och skäl 22 i Europaparlamentets och rådets förordning (EU) 2024/3018 av den 27 november 2024 om ändring av förordning (EG) nr 223/2009 om europeisk statistik.
[23] UNECE Input Privacy Preservation Project, 2023, *Final report version 28*, s. 5.

vänder FN det senare begreppet, bland annat inom arbetsgruppen för PET som är knuten till FN:s statistikkommission.[24] Utredningen anser därför att privacy-enhancing technologies bör betraktas som den mest vedertagna engelska termen.

I utredningens direktiv används den svenska termen integritetsbevarande metoder, medan IMY använder termen integritetshöjande teknik. I de EU-rättsakter där termen privacy-enhancing technologies används har den svenska översättningen konsekvent varit integritetsfrämjande teknik. Ordet främja betyder enligt Svensk ordbok att skapa gynnsamma förutsättningar och enligt Svenska Akademiens ordlista att hjälpa fram eller understödja. Teknik definieras som ett ändamålsenligt, praktiskt eller lämpligt tillvägagångssätt. Sammantaget tydliggör begreppet integritetsfrämjande teknik både syftet och användningsområdet för dessa tekniker. Utredningen har därför valt att använda termen integritetsfrämjande teknik, eftersom den bäst motsvarar den engelska termen och då det saknas skäl att använda en annan svensk term än den som använts mest frekvent i EU-rättsakter.

Begreppets innebörd och betydelse

Integritetsfrämjande teknik syftar till att göra det möjligt att dela data som innehåller personuppgifter och andra skyddsvärda uppgifter och samtidigt upprätthålla skyddet för den personliga integriteten. Privacy-enhancing technologies som begrepp tillkom 1995 och beskrevs då som en teknik som möjliggjorde anonyma transaktioner online.[25] Integritetsfrämjande teknik har sedan dess utvecklats och används inom flertalet områden. Det finns i dagsläget ingen enhetlig definition av begreppets innebörd och betydelse.

Europeiska unionens cybersäkerhetsbyrå (Enisa) har beskrivit privacy-enhancing technologies som programvaru- och hårdvarulösningar, det vill säga system som omfattar tekniska processer, metoder eller kunskap för att uppnå specifik integritets- eller data-

[24] https://unstats.un.org/bigdata/task-teams/privacy/index (hämtad 2026-05-19).
[25] The Royal Society, 2023, *From privacy to partnership*, s. 24.

skyddsfunktionalitet eller för att skydda mot risker för en individs eller en grupp av fysiska personers integritet.[26]

Internationella standardiseringsorganisationen (ISO) definierar privacy-enhancing technologies som en integritetskontroll, bestående av åtgärder för informations- och kommunikationsteknik (IKT), produkter eller tjänster som skyddar integriteten genom att eliminera eller minska personligt identifierbar information eller genom att förhindra onödig och/eller oönskad behandling utan att förlora IKT-systemets funktionalitet.[27]

IMY beskriver integritetsfrämjande teknik som ett samlingsbegrepp för tekniska lösningar som är utformade för att skydda individers personliga integritet.[28] Organisationen för ekonomiskt samarbete och utveckling (OECD) beskriver att integritetsfrämjande teknik möjliggör insamling, analys och delning av information samtidigt som integriteten skyddas.[29]

Användningen av integritetsfrämjande teknik kan dessutom bidra till en förändrad syn på datadelning. Genom att möjliggöra analys och samarbete utan att underliggande information exponeras minskar behovet av att överföra data mellan aktörer. Detta skapar förutsättningar för mer integritetsskyddande former av datadelning och främjar en modell där resultat och insikter delas snarare än de underliggande uppgifterna i sig.

Begreppets användning

En av svårigheterna med begreppet integritetsfrämjande teknik är att teknikerna är uppbyggda på helt olika sätt och har olika användningsområden. Även hur de olika teknikerna kategoriseras i olika sammanhang skiljer sig åt. Trots att de tekniker som omfattas av samlingsbegreppet integritetsfrämjande teknik skiljer sig åt i teknisk utformning eller kategoriseras på olika sätt har de i huvudsak ett gemensamt syfte. Det är att möjliggöra delning av data samtidigt

[26] Europeiska unionens cybersäkerhetsbyrå (Enisa), 2015, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies: Methodology, Pilot Assessment, and Continuity Plan*, s. 9.
[27] ISO/IEC 29100:2024, *Information technology – Security techniques – Privacy framework*, avsnitt 3.13.
[28] Integritetsskyddsmyndigheten (IMY), IMY-2026-5444, *Betrodda exekveringsmiljöer för uppkopplade fordon*, s. 8.
[29] https://www.oecd.org/en/topics/privacy-enhancing-technologies.html (hämtad 2026-05-12).

som skyddet för den personliga integriteten stärks. Det finns därför skäl att utgå från teknikernas syfte, i likhet med den beskrivning som används av IMY. Ett sådant angreppssätt ger en mer flexibel och teknikneutral utgångspunkt, vilket är av betydelse mot bakgrund av den snabba teknikutvecklingen och att nya tekniker kan tillkomma.

Mot denna bakgrund används integritetfrämjande teknik i detta betänkande som ett samlingsbegrepp för tekniker som bidrar till att stärka skyddet för den personliga integriteten.

1.5.2 Data

Data är ett centralt begrepp i en datadriven förvaltning. I lagen (2022:818) om den offentliga sektorns tillgängliggörande av data (öppna datalagen) definieras data som information i digitalt format oberoende av medium.[30] Lagen genomför EU:s öppna datadirektiv[31] och syftar till att främja användningen av öppna data och stimulera innovation inom produkter och tjänster genom vidareutnyttjande av information som tillgängliggörs av den offentliga sektorn. Vid genomförandet av direktivet valdes termen information i stället för handling, med motiveringen att information inte har samma tydliga koppling till fysiska dokument och att begreppet handling är starkt förknippat med handlingsbegreppet i 2 kap. tryckfrihetsförordningen. Enligt propositionen till lagen avses med data all information i digitalt format oberoende av medium, det vill säga allt informationsbärande innehåll och alla delar av ett informationsbärande innehåll, oberoende av i vilket digitalt format det innehas.[32]

Begreppet data definieras dock på ett annat sätt i dataförvaltningsförordningen. Där definieras data som varje digital återgivning av handlingar, fakta eller information och varje sammanställning av sådana handlingar, sådana fakta eller sådan information, däribland i form av ljudinspelningar, bildinspelningar eller audiovisuella inspelningar.[33] I promemorian med kompletterande bestämmelser till dataförvaltningsförordningen har bedömningen gjorts att de olika defini-

[30] 1 kap. 4 § lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.
[31] Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.
[32] Prop. 2021/22:225 *Den offentliga sektorns tillgängliggörande av data*, s. 17–19.
[33] Artikel 2.1 i dataförvaltningsförordningen.

tionerna i allt väsentligt har samma innebörd. Någon ändring av definitionen i öppna datalagen har därför inte ansetts nödvändig.[34]

Utredningen anser att det saknas skäl att använda en annan definition av data än någon av de som redan finns. Definitionen i dataförvaltningsförordningen innehåller begreppet handlingar, vilket även kan ge associationer till fysiska dokument och därmed riskerar att bli missvisande i detta sammanhang. Mot denna bakgrund har data samma innebörd i detta betänkande som i öppna datalagen, det vill säga information i digitalt format, oberoende av medium.

Ett begrepp som ofta används i samband med data är datamängd. Det används i detta betänkande som en generell term för en samling data, oavsett format. En datamängd kan både vara strukturerad och ostrukturerad.[35]

1.5.3 Datadelning

Datadelning utgör en grundläggande förutsättning för att den offentliga förvaltningen ska kunna utvecklas och bli mer datadriven. En utgångspunkt vid datadelning är att data kan delas av en eller flera avsändare till en eller flera mottagare. I enklare fall kan det vara data som delas mellan två aktörer vid ett enstaka tillfälle. I mer komplexa fall kan datadelningen vara kontinuerlig och automatiserad mellan flera aktörer.

I dataförvaltningsförordningen definieras datadelning som en registrerads eller datainnehavares tillhandahållande av data till en dataanvändare för gemensam eller individuell användning av dessa delade data, baserat på frivilliga avtal, unionsrätt eller nationell rätt, direkt eller via en förmedlare, till exempel inom ramen för öppna eller kommersiella licenser mot en avgift eller kostnadsfritt.[36] En datainnehavare kan vara en offentlig myndighet.[37] Definitionen i förordningen innehåller flera begrepp som kräver förklaring eller egna definitioner, så som registrerad, datainnehavare och dataanvändare. Utredningen har därför valt att använda en mer generell

[34] Ds 2023:24 *Genomförande av EU:s dataförvaltningsförordning*, s. 88 f.
[35] Det finns ingen avgörande betydelseskillnad mellan *datamängd* och dess engelska översättning *dataset*, som ibland förekommer i svensk text.
[36] Artikel 2.10 i dataförvaltningsförordningen.
[37] Artikel 2.8 i dataförvaltningsförordningen.

beskrivning av begreppet. Med datadelning avses i detta betänkande utbyte av digital information mellan olika aktörer.

1.5.4 Datadriven

Ett syfte med ökad användning av integritetsfrämjande teknik är, enligt utredningens direktiv, att den offentliga förvaltningen ska bli mer datadriven. Direktivet innehåller dock ingen definition av begreppet datadriven.

OECD har beskrivit en datadriven offentlig sektor (data-driven public sector) som en förvaltning som betraktar data som en tillgång och där data integreras i utformningen av policys, utformningen av tjänster, organisationsledning och innovation.[38]

Statskontoret beskriver en datadriven organisation som en organisation som använder data som en central källa för beslut och styrning av verksamheten. Detta innebär att data samlas in och analyseras på ett strukturerat sätt och att de insikter som analysen ger används för att förbättra verksamheten och nå uppsatta mål.[39]

Myndigheten för digital förvaltning framhåller att det inte är tillräckligt att enbart behandla data för att vara datadriven. Det krävs även att data analyseras och att de insikter som analysen ger används som underlag vid beslutsfattande. [40]

Mot denna bakgrund avses med begreppet datadriven i detta betänkande ett arbetssätt där relevanta data samlas in, analyseras och används som underlag för beslut och planering.

1.6 Betänkandets disposition

I kapitel 2 presenteras de rättsliga områden och politikområden där datadelning med integritetsfrämjande teknik är särskilt relevanta.

I kapitel 3 finns en beskrivning av teknikerna, deras utveckling och hur vi har kategoriserat dem.

---

[38] C. van Ooijen, B. Ubaldi & B. Welby, 2019, ”A data-driven public sector: Enabling the strategic use of data for productive, inclusive and trustworthy governance”, *OECD Working Papers on Public Governance*, no 33, s. 4.

[39] https://forum.statskontoret.se/verksamhetsutveckling/digitalisering-och-ai/Att-bli-en-datadriven-myndighet (hämtad 2026-02-10).

[40] Myndigheten för digital förvaltning (Digg), dnr 2024-7510, *Uppföljning av statliga myndigheters digitalisering 2024 – om data och AI. En enkätundersökning,* s. 54 f.

Kapitel 4 innehåller en redogörelse för resultatet av utredningens kartläggning av användningen av integritetsfrämjande teknik samt en beskrivning av nationella och internationella användningsfall.

I kapitel 5 beskrivs styrningen av integritetsfrämjande teknik och de tekniska standarder som finns på området.

I kapitel 6 presenteras utredningens bedömning av de möjligheter och hinder som finns vid datadelning med integritetsfrämjande teknik.

Kapital 7 innehåller utredningens analys av de rättsliga förutsättningarna för användningen av integritetfrämjande teknik.

I kapitel 8 finns våra förslag för att öka användningen av integritetsfrämjande teknik.

I kapitel 9 redovisar vi förslagens konsekvenser.

2 Integritetsfrämjande teknik och datadelning

2.1 Inledning

Integritetsfrämjande teknik och datadelning i offentlig förvaltning berör flera rättsliga områden och politikområden. Användningen av integritetsfrämjande teknik inom förvaltningen utgör en del av EU:s och regeringens digitaliseringspolitik. Teknikerna har också ett nära samband med utvecklingen av artificiell intelligens (AI). Vad gäller de rättsliga förutsättningarna för att använda teknikerna så styrs dessa bland annat av det dataskyddsrättsliga regelverket och bestämmelser om offentlighet och sekretess. När data delas är också reglerna om informationssäkerhet och cybersäkerhet aktuella.

I detta kapitel redogör utredningen översiktligt för en del av de områden och regelverk som är relevanta för att sätta integritetsfrämjande teknik i ett sammanhang. Syftet är också att ge vissa grundläggande rättsliga ramar för användningen av integritetsfrämjande teknik, som de ser ut just nu. I kapitel 7 kommer vissa rättsliga områden behandlas ytterligare.

Det kan dock noteras att det för närvarande pågår lagstiftningsarbeten, framför allt på EU-nivå, som kan komma att förändra den rättsliga bilden och dessa omnämns löpande i den mån utredningen har ansett det nödvändigt.

2.2 Digitaliseringspolitiken

Användningen av integritetsfrämjande teknik i offentlig förvaltning utgör en del av EU:s och regeringens digitaliseringspolitik, där digitaliseringen av den offentliga förvaltningen ingår. Mer specifikt är integritetsfrämjande teknik en del i arbetet med att stärka förutsätt-

ningarna för att öka datadelningen inom förvaltningen, utan att skyddet för den personliga integriteten eller annan skyddsvärd information äventyras. Integritetsfrämjande teknik har också ett nära samband med hur AI utvecklas i förvaltningen, till exempel när data behöver delas och användas för att träna och utveckla AI-modeller på ett säkert sätt.

2.2.1 EU:s digitala decennium och en europeisk dataunion

EU:s policyprogram för det digitala decenniet sätter den strategiska inriktningen och de övergripande målen för Europas digitala omställning fram till 2030.[1] Europeiska kommissionen har under en längre tid lyft fram data som en central resurs för innovation och tillväxt, bland annat genom insatser som syftar till att skapa en inre marknad för data.[2] Ett led i det arbetet har även varit inrättandet av gemensamma europeiska dataområden, där data från offentlig förvaltning och företag ska kunna utbytas inom EU. Först ut är införandet av det europeiska hälsodataområdet (EHDS), där EHDS-förordningen[3] trädde i kraft i mars 2025.

Under 2025 beslutade kommissionen om en ny strategi för en europeisk dataunion.[4] Strategin är en del av EU:s handlingsplan för AI som syftar till att göra Europa till en global ledare inom AI.[5] Strategin lyfter fram olika integritetsfrämjande tekniker som viktiga möjliggörande faktorer för att kunna träna AI-modeller och bidra till så kallad integritetsbevarande innovation. I den nya strategin för en europeisk dataunion betonas bland annat att AI-utvecklingen kräver fler insatser när det gäller att förbättra tillgången till stora mängder data av hög kvalitet. Ett av de prioriterade områdena är

[1] Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030.
[2] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *En EU-strategi för data*, COM/2020/66 final.
[3] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.
[4] Meddelande från kommissionen till Europaparlamentet och rådet, *Strategin för en europeisk dataunion: frigöra data för AI*, COM/2025/835 final.
[5] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *Handlingsplan för AI-kontinenten*, COM/2025/165 final.

att öka tillgången till data för AI-utveckling, bland annat genom datalaboratorier.[6]

2.2.2 Regeringens strategi för digitaliseringspolitiken

Regeringen har under 2025 och 2026 genomfört insatser för att tydliggöra den strategiska inriktningen för digitaliseringspolitiken, inklusive digitaliseringen av den offentliga förvaltningen. Det övergripande och riksdagsbundna målet för digitaliseringspolitiken är att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[7] Regeringens digitaliseringsstrategi för perioden 2025–2030 anger inriktningen för regeringens digitaliseringspolitik och ska fungera som ett komplement till de riksdagsbundna och EU-gemensamma målen för digitalisering.[8] Strategin innehåller målsättningar samt beslutade och planerade åtgärder som bland annat syftar till att stärka digitaliseringen av offentlig förvaltning och en datadriven utveckling. Målet för förvaltningens digitalisering anger att Sverige ska ha en offentlig förvaltning som förenklar och bidrar till minskad administration genom användarvänliga, säkra och trygga digitala tjänster som effektiviseras med hjälp av AI- och datadriven utveckling.

Strategin nämner inte specifikt integritetsfrämjande teknik, förutom i relation till två uppdrag till Myndigheten för digital förvaltning (Digg) om datadriven innovation och tillgängliggörandet av öppna data.[9] Dessa har regeringen aviserat men inte beslutat i dagsläget. I strategin finns också ett horisontellt mål för data som fastställer att Sverige ska ha en robust och säker nationell datainfrastruktur som möjliggör standardiserad, effektiv och hållbar delning och användning av data där den personliga integriteten värnas.

Digg och Post- och telestyrelsen (PTS) ska stödja genomförandet av digitaliseringsstrategin samt årligen följa upp målen i strategin.[10]

---

[6] COM/2025/835 final.
[7] Prop. 2011/12:1 *Budgetpropositionen för 2012* utg. omr. 22, bet. 2011/12:TU1, rskr. 2011/12:87.
[8] Finansdepartementet, 2025, *Sveriges digitaliseringsstrategi 2025–2030*.
[9] *Sveriges digitaliseringsstrategi 2025–2030*, s. 25.
[10] Finansdepartementet, Fi2025/01188, *Uppdrag till Myndigheten för digital förvaltning och Post- och telestyrelsen att stödja genomförandet av Sveriges digitaliseringsstrategi 2025–2030*.

2.3 Artificiell intelligens (AI)

Integritetsfrämjande teknik kan användas för att stärka skyddet för den personliga integriteten vid olika AI-tillämpningar, men är i sig inte AI. Utvecklingen av AI är beroende av stora datamängder för bland annat träning, testning och validering vilket kan utgöra integritetsproblem. Organisationen för ekonomiskt samarbete och utveckling (OECD) har lyft fram att integritetsfrämjande teknik spelar en avgörande roll för utvecklingen av AI då dessa kan användas som en lösning på integritetsproblemen. Ofta kombineras flera olika integritetsfrämjande tekniker för att skydda data och bibehålla kontrollen över dem i AI-tillämpningar.[11]

2.3.1 Regeringens strategi för AI

Regeringen har tagit fram en AI-strategi där det framgår att den offentliga förvaltningen behöver öka sin förmåga att arbeta datadrivet och dela data för att kunna utveckla och tillämpa AI på ett effektivt och säkert sätt. AI ska utvecklas och användas för att stärka och skydda demokratiska värden, rättssäkerhet och personlig integritet.[12] AI-strategin bygger bland annat på den färdplan och de förslag som AI-kommissionen lämnade i sitt slutbetänkande. AI-kommissionen framförde att integritetsfrämjande teknik är avgörande för att förena innovation och integritet eftersom teknikerna minskar risken för att personuppgifter exponeras.[13] I anslutning till att Digg och PTS följer upp målen i digitaliseringsstrategin ska myndigheterna också årligen följa upp AI-strategin.

[11] Organisationen för ekonomiskt samarbete och utveckling (OECD), *”Sharing trustworthy AI models with privacy-enhancing technologies”, OECD Artificial Intelligence Papers*, No. 38, s. 7 f.
[12] Finansdepartementet, 2026, *Sveriges AI-strategi*.
[13] SOU 2025:12 *AI-kommissionens Färdplan för Sverige,* s. 74.

2.3.2 Rättslig reglering av AI

Utvecklingen, tillhandahållandet och användningen av AI inom både privat och offentlig verksamhet regleras i AI-förordningen[14]. Syftet med AI-förordningen är att förbättra den inre marknadens funktion och att främja användningen av människocentrerad och tillförlitlig AI. AI-system som uteslutande används för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet är undantagna från förordningens bestämmelser. AI-förordningen trädde i kraft den 1 augusti 2024 och bestämmelserna börjar tillämpas successivt. AI-förordningen reglerar inte hur integritetsfrämjande teknik ska användas men det finns vissa krav i AI-förordningen på när sådan teknik ska användas (se avsnitt 5.2.1).

Utredningen om AI-förordningen har föreslagit kompletteringar och anpassningar i svensk rätt till AI-förordningen som för närvarande bereds inom Regeringskansliet.[15]

2.4 Dataskydd

2.4.1 Allmänt om regelverken

Integritetsfrämjande teknik är starkt förknippad med skyddet av personuppgifter vilket i huvudsak regleras i dataskyddsförordningen[16]. Förordningen är en generell dataskyddslagstiftning vid behandling av personuppgifter inom EU. Bestämmelserna är direkt tillämpliga och ska tillämpas precis som det vore en svensk författning. Dataskyddsförordningen kompletteras i svensk rätt generellt av lagen (2018:218) om kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Hur offentliga aktörer får behandla personuppgifter regleras dessutom ofta särskilt i olika registerförfattningar. Syftet med registerförfattningarna är att anpassa regleringen till de särskilda behov som myndigheterna har i sina re-

[14] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).
[15] SOU 2025:101 *Anpassningar till AI-förordningen.*
[16] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

spektive verksamheter samt att göra avvägningar mellan behovet av effektivitet i berörd verksamhet och behovet av skydd för den enskildes personliga integritet.[17] Det är därför vanligt att registerförfattningar innehåller begränsningar avseende vilka ändamål som personuppgifter får behandlas för eller andra begränsningar för hur personuppgifter får hanteras.

För brottsbekämpande myndigheter gäller brottsdatalagen (2018:1177) och brottsdataförordningen (2018:1202) i stället för dataskyddsförordningen och dataskyddslagen. Det finns även verksamheter, så som Försvarets Radioanstalt (FRA), där varken dataskyddsförordningen eller brottsdatalagen ska tillämpas. I stället regleras personuppgiftsbehandlingen i annan speciallagstiftning.[18] Generellt är det inte några större skillnader mellan dataskyddsförordningen och de andra regelverken. Vi har därför valt att fortsättningsvis endast nämna dessa speciallagstiftningar om tillämpningen av dessa påverkar användningen av integritetsfrämjande teknik på ett sätt som skiljer sig från möjligheterna att använda teknikerna enligt dataskyddsförordningen och dataskyddslagen.

2.4.2 Grundläggande regler om behandling av personuppgifter

I dataskyddsförordningen finns bestämmelser om skydd för fysiska personer med avseende på behandlingen av personuppgifter och om det fria flödet av personuppgifter. Ett av förordningens syften är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.[19] Den rätten är dock inte absolut utan måste vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.[20]

Dataskyddsförordningen är tillämplig på sådan behandling av personuppgifter som sker helt eller delvis på automatisk väg och på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.[21] Begreppen behandling och personuppgifter är därför centrala för att bedöma om dataskydds-

[17] Jfr bl.a. prop. 2015/16:65 *Utlänningsdatalag*, s. 21.
[18] Se t.ex. lag (2019:1182) om Säkerhetspolisens behandling av personuppgifter, lag (2021:1171) om behandling av personuppgifter vid Försvarsmakten och lag (2021:1172) om personuppgiftsbehandling vid Försvarets radioanstalt.
[19] Artikel 1.2 i dataskyddsförordningen.
[20] Skäl 4 i dataskyddsförordningen.
[21] Artikel 2 i dataskyddsförordningen.

förordningen är tillämplig vid användningen av integritetsfrämjande teknik.

Begreppet behandling definieras i artikel 4.2 i dataskyddsförordningen som en åtgärd eller en kombination av åtgärder beträffande personuppgifter, oberoende av om de utförs automatiserat eller inte. I artikeln exemplifieras begreppet behandling med insamling, registrering, organisering, lagring, ändring, läsning, användning, utlämning och radering av personuppgifter.

Begreppet personuppgifter definieras i artikel 4.1 i dataskyddsförordningen som varje upplysning som avser en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som till exempel ett namn, ett identifikationsnummer eller lokaliseringsuppgift. Det kan också avse en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska ekonomiska, kulturella eller sociala identitet. För att avgöra om en uppgift direkt eller indirekt kan identifiera en person bör alla hjälpmedel som rimligen kan användas beaktas.[22] Uppgifter som rör avlidna personer omfattas inte av dataskyddsförordningens bestämmelser.[23]

Rättslig grund och grundläggande principer

I dataskyddsförordningen finns det grunder för när behandling av personuppgifter är laglig (artikel 6–10) och principer för själva behandlingen (artikel 5). För att behandling av personuppgifter ska vara laglig krävs att något av de villkor som anges i artikel 6.1 i förordningen är uppfyllda. All behandling av personuppgifter måste också följa samtliga grundläggande principer som anges i artikel 5 i dataskyddsförordningen. Artiklarna 5 och 6 är alltså grundläggande och ska läsas tillsammans. Skillnaden mellan artiklarna är att artikel 6 reglerar *om* personuppgifterna får behandlas, medan artikel 5 handlar om *hur* de får behandlas.

Av principerna i artikel 5 framgår bland annat att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med

[22] Skäl 26 i dataskyddsförordningen.
[23] Skäl 27 i dataskyddsförordningen.

dessa ändamål (ändamålsbegränsning och finalitetsprincipen).[24] Uppgifterna ska också vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).[25] Detta innebär att all personuppgiftsbehandling, utöver att behandlingen måste ha en rättslig grund enligt artikel 6, bland annat ska ha samlats in för särskilda, uttryckligt angivna och berättigade ändamål och inte vara mer omfattande än nödvändigt.

Personuppgiftsansvar

Den som ensam eller tillsammans med andra bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till är personuppgiftsansvarig för behandlingen.[26] Med personuppgiftsansvaret följer ett ansvar att vidta de tekniska och organisatoriska åtgärder som krävs för att säkerställa att personuppgifterna behandlas i enlighet med dataskyddsregelverket.[27] Att bestämma ändamål tillsammans med andra innebär att det är fråga om gemensamma ändamål. Om två eller flera verksamheter gemensamt bestämmer ändamål och medel för en viss behandling är de personuppgiftsansvariga tillsammans.

När ett gemensamt personuppgiftsansvar föreligger ska de personuppgiftsansvariga fastställa sitt respektive ansvar genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av.[28] Ett sådan arrangemang kallas ofta ett datadelningsavtal. När ändamålen och medlen för behandlingen av personuppgifter bestäms på nationell nivå kan den personuppgiftsansvarige eller de särskilda kriterierna för att utse denne anges i nationell rätt.[29]

Den personuppgiftsansvariga kan ge en annan verksamhet i uppdrag att utföra personuppgiftsbehandlingen utan att det blir fråga om ett gemensamt personuppgiftsansvar. En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning

[24] Artikel 5.1 b i dataskyddsförordningen.
[25] Artikel 5.1 c i dataskyddsförordningen.
[26] Artikel 4.7 i dataskyddsförordningen.
[27] Kapitel IV i dataskyddsförordningen.
[28] Artikel 26 i dataskyddsförordningen.
[29] Artikel 4.7 i dataskyddsförordningen.

är då personuppgiftsbiträde.[30] Att en behandling av personuppgifter utförs av ett personuppgiftsbiträde innebär inte att personuppgiftsansvaret överlåts, utan det är alltid den personuppgiftsansvariga som måste säkerställa och kunna visa att behandlingen sker i enlighet med dataskyddsförordningen. Om det finns ett personuppgiftsbiträde krävs ett personuppgiftsbiträdesavtal. Personuppgiftsbiträdet får endast behandla personuppgifter enligt de instruktioner som biträdet har fått från den personuppgiftsansvariga.[31]

2.4.3 Inbyggt dataskydd och dataskydd som standard

Dataskyddsförordningen innehåller också bestämmelser om inbyggt dataskydd och dataskydd som standard. Genom bestämmelserna ställs krav på att datasystemen utformas på ett sådant sätt att det säkerställs att behandlingen sker med iakttagande av bland annat principen om uppgiftsminimering i artikel 5.1 c i dataskyddsförordningen. Av artikel 25.1 framgår att en personuppgiftsansvarig vid fastställandet av vilka medel som behandlingen utförs med och vid själva behandlingen ska genomföra lämpliga tekniska och organisatoriska åtgärder. Åtgärderna ska vara utformade för ett effektivt genomförande av dataskyddsrättsliga principer och för integrering av de nödvändiga skyddsåtgärderna vid behandlingen av personuppgifter, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Vilka åtgärder som är lämpliga ska avgöras med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna för fysiska personers rättigheter och friheter.

Av artikel 32 framgår det också att den personuppgiftsansvariga och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. I bedömningen av vad som är lämpliga åtgärder ska bland annat den senaste utvecklingen beaktas (se vidare avsnitt 7.3.2).

[30] Artikel 4.8 i dataskyddsförordningen.
[31] Artikel 28.3 i dataskyddsförordningen.

2.4.4 Anonymisering och pseudonymisering

Pseudonymisering omnämns i både artikel 25 och artikel 32 i dataskyddsförordningen som en lämplig teknisk åtgärd. Pseudonymisering definieras i artikel 4.5 i dataskyddsförordningen som behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används. Det krävs att de kompletterande uppgifterna förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. För att avgöra om en personuppgift är pseudonymiserad i rättslig mening behöver hänsyn tas till om en person kan identifieras utifrån både uppgiften och övriga uppgifter i datamängden. Det är också nödvändigt att ta hänsyn till vem som kan komma att ta del av uppgifterna och dennes möjligheter till identifiering utan tillgång till de kompletterande uppgifterna för att avgöra om en uppgift är pseudonymiserad i rättslig mening.[32]

Anonymisering saknar definition i dataskyddsförordningen men av skäl 26 framgår att personuppgifter kan anonymiseras på ett sådant sätt att den registrerade inte kan identifieras. I öppna datadirektivet definieras anonymisering som ett förfarande för att göra handlingar till anonyma handlingar, som inte avser en identifierad eller identifierbar fysisk person, eller förfarandet för att anonymisera personuppgifter på ett sådant sätt att den registrerade inte, eller inte längre, är identifierbar.[33]

När personuppgifter pseudonymiserats utgör de som huvudregel fortfarande personuppgifter, eftersom de med hjälp av en kompletterande uppgift (ofta i form av en översättningstabell eller nyckel) kan tillskrivas en fysisk person. Vid bedömningen av om en person rimligen kan identifieras bör samtliga objektiva faktorer, så som kostnader och tidsåtgång, tillgänglig teknik och den tekniska utvecklingen tas i beaktande. Om det inte rimligen längre går att identifiera en person som ingår i datamängden har personuppgifterna anony-

[32] Europeiska dataskyddsstyrelsen (EDBP), *Guidelines 01/2025 on pseudonymisation*, adopted version for public consultation, s. 8.
[33] Artikel 2.7 i Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

miserats och dataskyddsförordningens bestämmelser är då inte längre tillämpliga på den nya, anonymiserade datamängden.[34]

EU-domstolen har berört frågan om när en personuppgift kan anses identifiera en person i flera mål och senast i mål C-413/23.[35] Där har domstolen klargjort att pseudonymiserade personuppgifter inte alltid kan anses vara personuppgifter för en mottagare. Om mottagaren i det enskilda fallet inte kan identifiera personer i uppgiftsmängden är uppgifterna inte personuppgifter för mottagaren. Mot bakgrund av domstolens praxis har kommissionen föreslagit ett tillägg i definitionen av personuppgifter i artikel 4 i dataskyddsförordningen för att förtydliga när en person kan anses vara identifierbar i dataskyddsförordningens mening.[36] Vidare har kommissionen föreslagit att den ska få möjlighet att utfärda genomförandeakter för att specificera kriterier och medel för att avgöra när pseudonymiserade uppgifter inte längre är personuppgifter. För det ändamålet ska kommissionen enligt förslaget också bedöma den senaste utvecklingen av tillgängliga tekniker. Europeiska dataskyddsstyrelsen (EDPB) har tillsammans med Europeiska datatillsynsmannen (EDPS) avstyrkt kommissionens förslag eftersom de går utöver EU-domstolens praxis. Enligt EDPB och EDPS riskerar förslagen även att påverka dataskyddsförordningens tillämpningsområde och att skapa ökad rättslig osäkerhet.[37] EDPB har även hållit ett intressentmöte om anonymisering och pseudonymisering mot bakgrund av domstolens praxis.[38]

[34] Skäl 26 i dataskyddsförordningen.
[35] Domstolens dom av den 4 september 2025, Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden, C-413/23 P, EU:C:2025:645. Se även domstolens dom av den 19 oktober 2016, Patrick Breyer/Förbundsrepubliken Tyskland, C-582/14, EU:C:2016:779 och domstolens dom av den 9 november 2023, Gesamtverband Autoteile-Handel e.V. mot Scania CV AB, C-319/22, EU:C:2023:837.
[36] Kommissionens förslag till Europaparlamentets och rådets förordning om ändring av förordningarna (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 och direktiven 2002/58/EG, (EU) 2022/2555 och (EU) 2022/2557 vad gäller förenkling av lagstiftningsramen på det digitala området och om upphävande av förordningarna (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 och direktiv (EU) 2019/1024 (det digitala omnibuspaketet), COM/2025/837 final, artikel 3.
[37] Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS), Joint opinion 2/2026, *On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, s. 10 ff.
[38] https://www.edpb.europa.eu/system/files/2026-02/edpb-report-stakeholder-event-anonymisation-pseudonymisation_en.pdf (hämtad 2026-02-23).

2.5 Offentlighet och sekretess

Integritetsfrämjande teknik används främst till att skydda den personliga integriteten. Teknikerna kan också användas för att inte röja andra uppgifter som är känsliga, exempelvis uppgifter som omfattas av sekretess. Teknikerna kan till exempel möjliggöra analyser av data i samarbete med andra aktörer (samarbetsanalyser) utan att underliggande data delas. Reglerna om offentlighet och sekretess har därför stor betydelse för förutsättningarna när offentliga aktörer vill dela data.

2.5.1 Handlingsoffentlighet

Handlingsoffentligheten regleras i 2 kap. tryckfrihetsförordningen, TF. Av 2 kap. 3 § TF framgår att med handling avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt. Uttrycket handling i tryckfrihetsförordningen tar alltså sikte på såväl traditionella pappershandlingar som elektroniska handlingar.

En handling är allmän om den förvaras hos en myndighet och enligt särskilda bestämmelser är att anse som inkommen till eller upprättad där.[39] En handling som förvaras hos en myndighet endast som ett led i en teknisk bearbetning eller teknisk lagring för någon annans räkning anses dock inte som allmän handling hos den myndigheten.[40]

2.5.2 Sekretess och tystnadsplikt

I offentlighets- och sekretesslagen (2009:400), OSL, finns bestämmelser om sekretess som begränsar rätten att ta del av allmänna handlingar och som reglerar tystnadsplikt i det allmännas verksamhet. Lagen är tillämplig på myndigheter.[41] Med myndighet avses, på samma sätt som i regeringsformen och tryckfrihetsförordningen, organ som ingår i den offentligrättsliga statliga eller kommunala organisationen. Vid tillämpningen av offentlighets- och sekretesslagen jämställs med myndigheter också vissa andra organ.[42]

[39] 2 kap. 4 § TF.
[40] 2 kap. 13 § första stycket TF.
[41] 2 kap. 1 § OSL.
[42] 2 kap. 2–5 §§ OSL.

Med sekretess avses ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.[43] En sekretessbelagd uppgift som görs tillgänglig för någon annan anses dock inte vara röjd om den är krypterad på ett sätt som hindrar mottagaren från att ta del av dess innehåll. Om mottagaren däremot kan bryta krypteringen är uppgifterna röjda.[44]

En uppgift för vilken sekretess gäller får som utgångspunkt inte lämnas till en annan myndighet eller mellan olika verksamhetsgrenar inom samma myndighet, när de är att betrakta som självständiga i förhållande till varandra.[45]

2.5.3 Delning av data

Inom offentlig förvaltning finns det stora mängder uppgifter som inte kan delas eftersom de är sekretessbelagda. Sekretess kan därför utgöra ett hinder för datadelning. Möjligheten att dela data utgör en viktig förutsättning för att olika aktörer inom den offentliga förvaltningen ska kunna fullgöra sina uppdrag och för en fungerande samverkan mellan myndigheter i övrigt. Det har därför införts ett flertal sekretessbrytande bestämmelser i offentlighets- och sekretesslagen. Det finns också ett flertal uppgiftsskyldigheter i andra lagar och förordningar som har en sekretessbrytande verkan.

I 6 kap. 5 § OSL finns en generell bestämmelse om myndigheters informationsskyldighet gentemot varandra. Av den framgår att en myndighet på begäran av en annan myndighet ska lämna en uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Något krav på att uppgiften ska finnas i en allmän handling finns inte, varför bestämmelsen om informationsskyldighet mellan myndigheter har en större räckvidd än myndigheters skyldigheter gentemot enskilda.[46] Bestämmelsen anses vara en precisering av den allmänna samverkansskyldighet som gäller för myndigheter enligt 8 § förvaltningslagen (2017:900). Bestämmelsen i 6 kap. 5 § OSL har alltså ett annat syfte än bestäm-

[43] 3 kap. 1 § OSL.
[44] Prop. 2022/23:97 *Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter*, s. 7.
[45] 8 kap. 1–2 §§ OSL.
[46] Prop. 1979/80:2 *med förslag till sekretesslag m.m.*, Del A s. 361, jfr även 6 kap. 4 § OSL som reglerar utlämnande av uppgifter till enskilda.

melserna i 2 kap. TF och ska framför allt underlätta för myndigheter att fullgöra sin verksamhet.[47]

2.6 Informationssäkerhet och cybersäkerhet

När data delas är också reglerna om informationssäkerhet och cybersäkerhet aktuella. Informationssäkerhet avser skyddet av information så att den görs tillgänglig för rätt personer, vid rätt tid och så att den inte förstörs eller förvanskas.[48] Cybersäkerhet fokuserar på skyddet av digitala system och nätverk mot olika hot som obehörig åtkomst, skada eller stöld.[49] Datadelning med stöd av integritetsfrämjande teknik innebär inte enbart ett stärkt integritetsskydd utan möjliggör också en mer säker datadelning, exempelvis genom att minimera mängden känsliga uppgifter som delas, begränsa åtkomsten och på olika sätt skydda data. Det kan bidra till att stärka både informationssäkerheten och cybersäkerheten hos offentliga aktörer.

2.6.1 Informationssäkerhet

Statliga myndigheter omfattas av förordningen (2022:524) om statliga myndigheters beredskap. Enligt förordningen ska myndigheterna säkerställa att dess informationshanteringssystem uppfyller grundläggande och särskilda säkerhetskrav samt särskilt beakta behovet av säkra ledningssystem för informationssäkerhet[50]. Detta regelverk kompletteras av Myndigheten för civilt försvars föreskrifter. Föreskrifterna ställer ytterligare krav på utformningen av informationssystem och myndigheternas arbete med bland annat incident- och kontinuitetshantering.[51] Informationssäkerhet är inte begränsat

[47] Jfr prop. 1979/80:2 Del A s. 89–91, samt HFD 2021 ref. 10.
[48] https://www.sis.se/iso27001/informationssakerhet/ (hämtad 2026-05-07).
[49] termbank-informationssakerhet.msb.se/TermadoSearch.aspx?guid=86c49bc9-15ab-4b63-8588-838ada6794f5&name=cybersäkerhet&type=termpost (hämtad 2026-05-25).
[50] Ett ledningssystem för informationssäkerhet är en organisations processer för styrning och ledning av informationssäkerhetsarbetet. Läs mer hos Myndigheten för civilt försvar, https://www.mcf.se/sv/amnesomraden/informationssakerhet-och-cybersakerhet/arbeta-systematiskt-med-informationssakerhet-och-cybersakerhet/ledningssystem-for-informationssakerhet-lis/ (hämtad 2026-05-13).
[51] MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter och MSBFS 2020:8 föreskrifter om rapportering av it-incidenter för statliga myndigheter.

till enbart tekniska åtgärder utan inkluderar även bland annat rutiner och utbildning.

Kommuner och regioner omfattas inte av någon motsvarande specifik reglering för informationssäkerhet. Det finns dock vissa bestämmelser om åtgärder som kommuner och regioner ska vidta i krissituationer för att minska sårbarheten i sin verksamhet i lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap samt tillhörande förordning.

2.6.2 Cybersäkerhet

Den 15 januari 2026 trädde den nya cybersäkerhetslagen (2025:1506) i kraft. Lagen genomför NIS 2-direktivet[52] i svensk rätt. Lagen innebär skärpta krav på systematiskt cybersäkerhetsarbete, riskbaserade säkerhetsåtgärder och incidentrapportering för både offentliga och privata verksamhetsutövare. Bland de säkerhetsåtgärder som ska vidtas ingår bland annat att bedöma om kryptering krävs för att upprätthålla säkerheten.[53] Lagen omfattar fler sektorer än tidigare och tydliggör ledningens ansvar, samtidigt som tillsynen förstärks genom utpekade sektorsmyndigheter enligt den kompletterande cybersäkerhetsförordningen (2025:1507).

Regeringen beslutade 2025 om en nationell cybersäkerhetsstrategi som beskriver regeringens inriktning för arbetet med frågor av betydelse för Sveriges cybersäkerhet under perioden 2025–2029.[54] Strategin betonar vikten av ett förstärkt cybersäkerhetsarbete, bland annat mot bakgrund av de sårbarheter som uppstår vid en ökad utveckling och beroende av digital infrastruktur, digitala tjänster och AI.[55] Integritetsfrämjande teknik nämns inte specifikt i strategin men kan utgöra ett verktyg för att minska såväl individens som samhällets sårbarhet vid en ökad datadelning, vilket i förlängningen kan bidra till att stärka Sveriges cybersäkerhet.

[52] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).
[53] 2 kap. 3 § cybersäkerhetslagen (2025:1506).
[54] Försvarsdepartementet, *Nationell strategi för cybersäkerhet 2025–2029*.
[55] Regeringens skrivelse 2024/25:121, *Nationell strategi för cybersäkerhet 2025–2029*, s. 12 f.

2.6.3 Säkerhetsskydd

För vissa informationsmängder och i vissa verksamheter gäller ytterligare krav i form av säkerhetsskydd. Det kan också gälla när olika informationsmängder samlas och den totala, aggregerade informationsmängden blir skyddsvärd. Det kan också gälla om ett system är skyddsvärt ur tillgänglighets- eller riktighetsperspektiv. Säkerhetsskydd syftar till att i förebyggande syfte skydda säkerhetskänslig verksamhet och säkerhetsskyddsklassificerade uppgifter mot bland annat spionerі, sabotage och terroristbrott.

Säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955) anger de grundläggande krav som gäller för informationssäkerhet, fysisk säkerhet och personalsäkerhet. Både Säkerhetspolisen och Försvarsmakten utfärdar föreskrifter avseende säkerhetsskydd. Det kan till exempel innebära högre krav på säkerheten i systemen samt att vissa åtgärder måste vidtas för att skydda uppgifterna. En sådan åtgärd kan vara att krypteringen måste vara godkänd av Försvarsmakten vid hantering utanför den egna kontrollen vilket kan begränsa möjligheten att dela uppgifterna. Verksamheter som lyder under säkerhetsskyddslagstiftningen måste särskilt beakta dessa krav när data ska delas.

3 Beskrivning av integritetsfrämjande teknik

3.1 Inledning

För närvarande finns ingen gemensam eller vedertagen lista nationellt eller internationellt över tekniker som kan anses vara integritetsfrämjande. Utredningen har därför valt att beskriva de tekniker som ofta klassificeras som sådana i internationella rapporter och riktlinjer samt de tekniker som omnämns i vårt direktiv. Det finns således fler tekniker som kan anses vara integritetsfrämjade. Eftersom teknikerna i huvudsak beskrivs i internationella sammanhang saknas det ofta vedertagna svenska begrepp för teknikerna. I den mån det saknas har utredningen valt ett svenskt begrepp som vi anser vara lämpligt.

I detta kapitel redovisas hur teknikerna har utvecklats och hur vi kategoriserat dem (avsnitt 3.2–3.3). Vi beskriver även ett urval av de mest relevanta integritetsfrämjande teknikerna som både kan bidra till att skydda individers integritet vid datadelning och till att öka datadelningen (avsnitt 3.4–3.8). Syftet är att ge en grundläggande förståelse för de olika teknikerna och deras funktion. Avslutningsvis redovisas utredningens syn på den framtida utvecklingen av integritetsfrämjande teknik (avsnitt 3.9).

3.2 Utvecklingen av integritetsfrämjande teknik

Utvecklingen av integritetsfrämjande teknik följer samma typiska mönster som återkommer inom andra teknikområden. Inledningsvis utvecklas teknikerna huvudsakligen inom forskningen och det är osäkert vilka tekniker som kommer att få praktiskt genomslag.

Den mjukvara som krävs för att möjliggöra realistiska tillämpningar i större skala saknas ofta.

Efter denna inledande fas tas vissa tekniker upp av kommersiella aktörer och integreras i deras produkter. I övergången från potentiella till etablerade lösningar drivs standardiseringsarbetet i stor utsträckning av de kommersiella aktörerna själva, bland annat i syfte att vinna marknadsandelar. I vilken utsträckning integritetsfrämjande tekniker utvecklas vidare och implementeras i praktiken är i hög grad beroende av deras förväntade lönsamhet och den allmänna teknikutvecklingen. Detta påverkas till exempel av möjliga ökningar i beräkningskapacitet, minskade kostnader, ökad tillgänglighet till digital infrastruktur och förbättrade utvecklingsmetoder.

Utöver den allmänna teknikutvecklingen så spelar också den nationella ambitionsnivån roll för vilka tekniker som vidareutvecklas och etableras som standarder. Som exempel kan nämnas att i USA bidrar offentliga aktörer till utvecklingen genom tidig efterfrågan. De bidrar även till utvecklingen genom finansiering av forskning och genom att stödja standardiseringsarbete (se även avsnitt 5.5.1).

3.3 Kategorisering av teknikerna

Integritetsfrämjande teknik delas ofta in i olika kategorier, men det saknas en vedertagen kategorisering. Utredningen har valt att inledningsvis göra en uppdelning mellan etablerade respektive moderna integritetsfrämjande tekniker. Med etablerade tekniker avses välkända tekniker med utbredd användning inom offentlig förvaltning och där kunskapsnivån generellt är hög. Dessa tekniker ingår inte alltid i internationella rapporter och riktlinjer om integritetsfrämjande teknik. Med moderna integritetsfrämjande tekniker avses tekniker som ännu inte har fått ett brett genomslag inom offentlig förvaltning och som i olika grad är tekniskt mogna för användning. Kunskapen om dessa tekniker är i regel mer begränsad och användningen är låg.

Tabell 3.1 Kategorisering av integritetsfrämjande teknik

Kategori	Underkategori	Teknik som ingår
Etablerade tekniker	Avidentifieringstekniker	Anonymisering Pseudonymisering Undertryckande Generalisering Randomisering
Moderna tekniker	Avidentifieringstekniker	Differentiell integritet Syntetiska data
	Uppgiftsminimerande tekniker	Federerad inlärning Nollkunskapsbevis
	Tekniker för skyddad bearbetning	Betrodda exekveringsmiljöer Säker flerpartsberäkning Homomorf kryptering

De integritetsfrämjande teknikerna delas vidare in i tre underkategorier. Den första underkategorin är avidentifieringstekniker, vilka kännetecknas av att personuppgifter ändras, avlägsnas eller döljs. Inom denna kategori finns det både moderna tekniker och etablerade tekniker. En skillnad mellan dessa är att de etablerade avidentifieringsteknikerna främst används vid datadelning mellan två aktörer, medan moderna avidentifieringstekniker även kan vara lämpliga för situationer där data delas med flera mottagare eller ska offentliggöras. Den andra underkategorin utgörs av uppgiftsminimerande tekniker, där syftet är att säkerställa att endast en begränsad mängd data delas. Den tredje och sista underkategorin omfattar tekniker för skyddad bearbetning, vilka karakteriseras av att data skyddas under själva bearbetningsprocessen. Det sker exempelvis genom kryptering eller genom att bearbetningen sker i en särskilt avgränsad och skyddad miljö. Inom underkategorierna uppgiftsminimerande tekniker och tekniker för skyddad bearbetning saknas det etablerade, välkända tekniker på det sätt som det finns för avidentifieringstekniker.

I internationella rapporter används andra kategoriseringar. Exempelvis delar Organisationen för ekonomiskt samarbete och utveckling (OECD) in integritetsfrämjande teknik i fyra andra grupper. Den första är verktyg för att göra data svårtolkad (data obfuscation tools) som karaktäriseras av att teknikerna tar bort eller döljer personuppgifter. Den andra kategorin är verktyg för krypterad data-

behandling (encrypted data processing tools) som används för bearbetning av krypterade data. Den tredje kategori är federerad och distribuerad analys (federated and distributed analytics) som gör det möjligt att träna modeller på data för att identifiera mönster. Ett exempel på detta är federerad inlärning. Den fjärde kategorin är verktyg för dataansvar (data accountability tools) som ger kontroll över data och möjlighet att sätta upp regler för tillgång, exempelvis personliga informationshanteringssystem. Verktygen i denna kategori utgör dock inte integritetsfrämjande teknik enligt OECD.[1] FN har en annan, enklare kategorisering av de integritetsfrämjande teknikerna. Den första kategorin är inmatningsintegritet (input privacy) där teknikerna möjliggör att flera parter lämnar in data för bearbetning utan att få tillgång till data. Den andra kategorin är utdataintegritet (output privacy) där teknikerna syftar till att förhindra identifiering.[2]

3.4 Etablerade avidentifieringstekniker

3.4.1 Anonymisering och pseudonymisering

Anonymisering och pseudonymisering används ofta som samlingsbegrepp för olika tekniker vilka gör det svårare att identifiera fysiska personer. Exempel på sådana tekniker är undertryckande, generalisering och randomisering. Ur ett rättsligt perspektiv används begreppen anonymisering och pseudonymisering snarare för att beskriva vilket resultat som användningen av avidentifieringstekniker har lett till än för att beskriva hur avidentifieringen har gått till. Tekniker för anonymisering kan rättsligt skapa pseudonymiserad data.[3]

Vanligtvis används anonymisering som begrepp för att förändra identifierande uppgifter på ett oåterkalleligt sätt medan pseudonymisering används när identifierande uppgifter ersätts med andra uppgifter, en pseudonym.[4] Kopplingen mellan pseudonymen och

[1] Organisationen för ekonomiskt samarbete och utveckling (OECD), ”Emerging privacy-enhancing technologies: Current regulatory and policy approaches”, *OECD Digital Economy Papers*, No. 351, s. 14 f.
[2] Förenta nationerna (FN), 2023, *United Nations Guide on Privacy-Enhancing Technologies for Official Statistics (PET-Guide)*, s. 19.
[3] Europeiska dataskyddsstyrelsen (EDPB), *Guidelines 01/2025 on pseudonymisation*, adopted version for public consultation, s. 8. Se också avsnitt 2.4.4. angående den rättsliga definitionen.
[4] https://tietosuoja.fi/sv/pseudonymiserade-och-anonymiserade-uppgifter (hämtad 2026-04-17).

den ursprungliga uppgiften kan till exempel vara en översättningstabell, kodnyckel eller krypteringsnyckel.[5]

3.4.2 Undertryckande

En vanlig avidentifieringsteknik är undertryckande (suppression). Tekniken innebär att uppgifter som direkt eller indirekt kan användas för att identifiera en fysisk person tas bort eller maskeras.[6] Det kan exempelvis röra sig om att specifika värden, så som namn och personnummer, eller att hela poster, kopplat till en person, i en datamängd tas bort. Undertryckande av hela poster i datamängden kan vara nödvändigt i de fall där andra avidentifieringstekniker har tillämpats, men där det fortfarande är möjligt att identifiera den enskilda individen bakom en viss post.[7]

3.4.3 Generalisering

Generalisering är en teknik för avidentifiering som syftar till att minska risken för identifiering av enskilda individer genom att reducera detaljeringsgraden i uppgifter som fungerar som kvasi-identifierare, det vill säga uppgifter som indirekt kan användas för att identifiera en person. Exempel på generalisering är att ersätta en exakt ålder med ett åldersintervall eller att ersätta en specifik ort med en större geografisk enhet så som kommun eller län.[8]

3.4.4 Randomisering

Randomisering är ett samlingsbegrepp för tekniker som används för att minska möjligheten att koppla data till enskilda individer. Detta sker genom att sanningshalten i uppgifterna påverkas på ett kontrollerat sätt. Teknikerna kan exempelvis innebära att uppgifter som indirekt kan användas för att identifiera en person byts ut eller för-

[5] eSam, *Vägledning ES2022-01 Pseudonymisering av personuppgifter,* s. 9.
[6] Rådet för den officiella statistiken, 2015, *Handbok i statisk röjandekontroll*, s. 55.
[7] Personal Data Protection Commission Singapore (PDPC), 2022, *Guide to basic anonymisation,* s. 22.
[8] Artikel 29-arbetsgruppen för skydd av personuppgifter, 0829/14/EN WP216, *Yttrande 05/2014 om avidentifieringsmetoder*, s. 16 f.

ändras. Syftet är att bevara datamängdens analytiska värde samtidigt som risken för identifiering av enskilda individer minimeras.[9]

Brustillägg

En vanlig randomiseringsteknik är att tillföra så kallat brus (noise), vilket innebär att värden i datamängden förändras så att de blir mindre exakta. Samtidigt som brus tillförs bibehålls den övergripande fördelningen av värdena. Brustillägg kan genomföras på olika sätt, till exempel genom att en persons ålder justeras med ett slumpmässigt antal år inom ett begränsat intervall eller genom att numeriska uppgifter multipliceras med ett slumpmässigt tal. [10]

Permutation

En variant av randomisering är permutation, som innebär att värden i en post byts ut mot värden från en annan post i samma datamängd. På detta sätt bevaras uppgifterna i sig, men kopplingen mellan uppgift och individ bryts.[11] Vid användning av permutation bevaras den exakta fördelningen av värdena i datamängden.[12]

3.5 Moderna avidentifieringstekniker

3.5.1 Differentiell integritet

Med differentiell integritet (differential privacy) bestäms en skyddsnivå som en algoritm behöver uppfylla för att säkerställa integriteten hos individer i en datamängd.[13] Till skillnad från etablerade avidentifieringstekniker, där det är svårt att avgöra om åtgärderna är tillräckliga för att förhindra identifiering så ger differentiell integritet ett matematiskt bevis för sannolikenheten att en person inte kan identifieras.

[9] Artikel 29-arbetsgruppen, *WP216*, s. 12.
[10] https://www.fsd.tuni.fi/en/services/data-management-guidelines/anonymisation-and-identifiers/ Avsnitt Anonymisation of quantative data, Noise addition (hämtad 2026-04-16).
[11] https://researchdata.se/sv/hantera-data/data-med-personuppgifter/handbok-data-med-personuppgifter/metoder/metoder-kvantitativa (hämtad 2026-02-11).
[12] Artikel 29-arbetsgruppen, *WP216,* s. 14.
[13] FN, *PET-Guide*, s. 36.

Det finns flera olika tillvägagångssätt för att uppnå differentiell integritet, men samtliga bygger på att ett slumpmässigt (randomiserat) brus tillförs datamängden.[14] Bruset kalibreras för att överstiga den påverkan på utfallet som en enskild individs uppgifter har. Detta medför att det inte är möjligt att avgöra om en specifik individ ingår i datamängden. För att resultaten ska vara tillförlitliga krävs i regel omfattande datamängder.[15]

Differentiell integritet kan även tillämpas vid framställning av syntetiska data (se vidare i avsnitt 3.5.2). Sådana datamängder kallas på engelska differentially private synthetic datasets och framställs med mekanismer som uppfyller de krav som ställs för differentiell integritet.[16]

Tillåten nivå av integritetsförlust

Vid användning av differentiell integritet behöver den som bearbetar data bestämma den tillåtna nivån av integritetsförlust (*privacy loss parameter)*, så kallad epsilon (ε). En låg nivå av integritetsförlust innebär att mer slumpmässigt brus adderas, vilket stärker integritetsskyddet men minskar datamängdens precision och tillförlitlighet. En hög nivå av integritetsförlust innebär att mindre brus tillförs, vilket ger mer användbara data men ett svagare integritetsskydd. Valet av integritetsnivå bör föregås av en noggrann avvägning mellan integritet och datakvalitet, där hänsyn tas till datamängdens känslighet och syftet med databehandlingen.[17] Det finns ett samarbete, OpenDP, vid Harvard University som har skapat ett frivilligt register för användningen av differentiell integritet och vilken tillåten nivå som valts för integritetsförlust.[18]

Vid upprepade analyser av samma datamängd används ofta en så kallad integritetsbudget (privacy budget). Denna anger en övre gräns för den totala tillåtna integritetsförlusten. Varje analys som genomförs medför då en viss förbrukning av budgeten. När bud-

[14] FN, *PET-Guide*, s. 36.
[15] https://researchdata.se/sv/hantera-data/data-med-personuppgifter/handbok-data-med-personuppgifter/metoder/metoder-kvantitativa (hämtad 2026-02-11).
[16] National Institute of Standards and Technology, *NIST SP800-226 Guidelines for Evaluating Differential Privacy Guarantees*, s. 46 och 72.
[17] NIST, *SP800-226*, s. 13 f.
[18] https://registry.opendp.org/deployments-registry/(hämtad 2026-03-16).

geten är förbrukad kan ytterligare analyser inte utföras utan att integritetsskyddet försvagas.[19]

Tekniken kan användas vid datainsamling

Till skillnad från traditionella avidentifieringstekniker kan differentiell integritet tillämpas redan vid själva datainsamlingen, i stället för i den efterföljande bearbetningen. Denna datainsamlingsteknik kallas randomiserat svar (randomized response) och innebär att endast en förvanskad, brusad version av de faktiska uppgifterna samlas in. Det innebär att integritetsskyddet stärks redan vid insamlingstillfället.[20]

3.5.2 Syntetiska data

Syntetiska data är fiktiva uppgifter som baseras på verkliga data och har därmed liknande statistiska egenskaper och mönster som verkliga data. Syntetiska data kan genereras både från strukturerade och ostrukturerade datakällor. Det finns också flera tekniker för att framställa dem och dessa kan ofta kombineras. Exempelvis kan statistiska tekniker användas för enklare datamängder med kända attribut och korrelationer, medan avancerade modeller så som transformatormodeller kan användas för generering av syntetiska data från text.[21]

Syntetiska data kan användas för att möjliggöra datadelning i situationer där delning av verkliga data begränsas av integritetsskäl.[22] De kan också användas som substitut i situationer där insamling av verkliga data är inte är möjlig eller etiskt problematisk.[23]

[19] NIST, *SP800-226*, s. 15.
[20] B. Steephenson, 2017, *Implementing Differential Privacy Using Randomized Response Algorithms*, s. 1, 4 och 6.
[21] https://www.ibm.com/think/insights/synthetic-data-generation (hämtad 2026-04-23).
[22] FN, *PET-Guide*, s. 40.
[23] Europeiska unionens cybersäkerhetsbyrå (Enisa), 2022, *Data Protection Engineering – From Theory to Practice*, s. 18.

Typer av syntetiska data

Det finns tre typer av syntetiska data:

- *Helt syntetiska data* innebär att alla delar av datan är fiktiv men relationen mellan olika värden baseras fortfarande på verkliga data.
- *Delvis syntetiska data* avser data där endast vissa delar ersätts med fiktiva uppgifter. Ofta ersätts de känsligaste delarna medan övriga delar består av verkliga data. Denna typ används exempelvis inom klinisk forskning när verkliga data är avgörande för analysen men personlig information behöver skyddas.
- Hybriddata innebär att värden från verkliga data slumpmässigt ersätts med motsvarande värden från helt syntetiska data, vilket skapar en slumpmässig kombination av verkliga och syntetiska uppgifter.[24]

Kvalitet och utmaningar vid träning av AI-modeller

Syntetiska data återspeglar mönster och egenskaper i verkliga data. Extremvärden eller avvikelser i den verkliga datamängden är ofta svåra att korrekt representera i syntetiska data utan att risk för identifiering uppstår. För att minska denna risk döljs ofta extremvärden, vilket medför att sådana värden kan vara underrepresenterade i syntetiska datamängder.[25]

Syntetiska data används ofta för att träna AI-modeller. Det finns dock risker med att enbart använda syntetiska data vid träning av AI-modeller eftersom detta kan leda till en försämrad prestanda i AI-modellen, så kallad modellkollaps. Problemet uppstår eftersom syntetiska data ofta är mindre komplexa än verkliga data. Detta medför att modellerna tenderar att imitera mönster i syntetiska data snarare än att utveckla en förmåga att dra slutsatser utifrån den. Det kan i sin tur bland annat ge upphov till att modellen genererar ett svar eller resultat som är felaktigt, så kallade AI-hallucinationer. För att säkerställa robusthet och korrekthet i modellen är det där-

[24] https://www.ibm.com/think/topics/synthetic-data#1003835707 (hämtad 2026-04-23).
[25] J. Jordon, L. Szpruch, F. Houssiau, M. Bottarelli, G. Cherubin, C. Maple, S. N. Cohen & A. Weller, 2022, *Synthetic Data – what, why and how?*, s. 25 f.

för viktigt att syntetiska data kompletteras med verkliga data vid träning av AI-modeller.[26]

3.6 Utmaningar med avidentifieringstekniker

De största utmaningarna med avidentifieringstekniker är att balansera integritet med dataanvändbarhet samt att säkerställa att vidtagna åtgärder är tillräckliga för att individer inte ska kunna identifieras. När data förändras för att minska risken för identifiering av enskilda individer påverkas ofta även dess användbarhet, eftersom relevant information eller samband kan gå förlorade.[27] Det kan dessutom vara svårt att säkerställa att till exempel brustillägg genomförs konsekvent eller att utbytet av värden sker på ett sätt som inte bryter logiska relationer mellan data.[28]

3.6.1 Utvärdering av vidtagna avidentifieringsåtgärder

Europeiska dataskyddsstyrelsen (EDPB) har gjort vissa uttalanden om risken för att enskilda individer identifieras i AI-modeller som är relevanta för anonymisering generellt. De har bland annat uttalat att den personuppgiftsansvarige behöver kunna visa att AI-modellerna är anonyma, det vill säga att det inte är möjligt att utvinna personuppgifter från modellen. Det framhålls också att olika tester bör övervägas för att bedöma motståndskraften mot återidentifieringsförsök.[29] I en rapport framtagen på uppdrag av EDPB nämns bristfällig anonymisering som en risk och behovet av robusta test- och valideringsprocesser lyfts fram.[30] Det finns dock inga generella riktlinjer för test av motståndskraft vid återidentifieringsförsök, vilket skapar osäkerhet om anonymiseringsåtgärderna är tillräckliga. Denna osäkerhet kan leda till att fler åtgärder vidtas än nödvändigt, med konsekvensen att återstående data blir mindre användbar. Det kan också leda till att data inte delas alls. Ett sätt att bedöma åtgär-

[26] https://www.ibm.com/think/topics/model-collapse (hämtad 2026-04-23).
[27] PDPC, *Guide to basic anonymisation*, s. 10.
[28] Artikel 29-arbetsgruppen, *WP216*, s. 14.
[29] Europeiska dataskyddsstyrelsen (EDBP), *Yttrande 28/2024 om vissa dataskyddsaspekter vid behandling av personuppgifter i samband med AI-modeller*, s. 2 och 55.
[30] I. Barberá, 2025, *AI Privacy Risks & Mitigations - Large Language Models (LLMs)*, s. 31 f. och 68.

dernas effekt är testet motiverad angripare (motivated-intruder test). I detta test får en person, med rimlig kompetens men utan specialistkunskaper om återidentifiering, i uppgift att försöka identifiera individer i anonymiserade data. Personen får använda allmänt tillgängliga informationskällor, så som internet, bibliotek och information från myndigheter.[31] Testet beaktar däremot inte möjligheten till identifiering genom dataintrång eller andra brottsliga gärningar. Om identifieringsförsöken misslyckas bedöms anonymiseringsåtgärderna som tillräckliga. Testet har sin grund i skäl 26 i dataskyddsförordningen[32], som anger att alla rimliga hjälpmedel som kan användas för identifiering ska beaktas vid bedömningen av om en fysisk person är identifierbar.

3.6.2 Särskilt om pseudonymisering och kompletterande information

Det som utmärker pseudonymiserade data är att de uppgifter som kan användas för identifiering har ersatts med ett pseudonym. Kopplingen mellan pseudonymen och den ursprungliga uppgiften (kompletterande information) måste förvaras separat och på ett säkert sätt. Det kräver att de tekniska och organisatoriska åtgärder som väljs är hållbara över tid. Offentliga aktörer måste också bedöma om den kompletterande informationen kan utgöra en allmän handling enligt 2 kap. tryckfrihetsförordningen, samt om någon sekretessbestämmelse är tillämplig på informationen. Regler om bevarande och gallring behöver också beaktas.[33]

3.7 Uppgiftsminimerande tekniker

3.7.1 Federerad inlärning

Federerad inlärning (federated learning) är en teknik för träning av AI-modeller. Tekniken innebär att själva träningsprocessen sker lokalt hos datakällan i stället för att all träningsdata samlas in hos

[31] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/how-do-we-ensure-anonymisation-is-effective/ (hämtad 2026-04-27).
[32] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[33] eSam, *Vägledning ES2022-01*, s. 14 f. och 43 f.

en central part. Därefter tränas en gemensam (central) AI-modell på resultaten från varje lokal träning. Exempelvis kan en AI-modell för att bedöma röntgenbilder tränas lokalt på varje sjukhus i stället för att alla röntgenbilder samlas centralt för att träna AI-modellen. Resultatet av den lokala träningen utgörs av parametrar som representerar den kunskap som erhållits genom träningen. Det är dessa parametrar som används för att uppdatera den centrala modellen.

I jämförelse med vanlig träning av AI-modeller är integritetsskyddet högre eftersom all träningsdata inte samlas på samma ställe och ingen träningsdata behöver delas med andra parter. Eftersom endast träningsresultatet delas innebär det en uppgiftsminimering och en ökad kontroll över personuppgiftsbehandlingen.[34]

Utmaningar med integritet, säkerhet och kvalitet

En utmaning med federerad inlärning är att det är svårt att utesluta att AI-modeller inte minns de personuppgifter som de tränats på. Det gäller dock generellt för AI-modeller och inte enbart vid federerad inlärning. När AI-modeller delas kan det innebära att även personuppgifter delas om personer går att identifiera i modellen.[35] Det finns därför behov av att kombinera federerad inlärning med andra integritetsfrämjande tekniker.[36]

På grund av sin distribuerade karaktär är federerad inlärning sårbar för olika typer av attacker, särskilt om säkerheten brister vid överföringen mellan parterna. Det kan därför vara nödvändigt att till exempel använda avidentifieringstekniker på den data som används vid träning av AI-modellen.[37]

Med fler parter involverade i träningen av AI-modellen finns det även en större risk för att det uppstår fel i träningen. Det kan bero på att det kan vara svårt att upptäcka om den träningsdata som används lokalt skiljer sig i kvalitet, kvantitet och mångfald från annan träningsdata som används. Om träningsdata skiljer sig för mycket

[34] https://www.edps.europa.eu/press-publications/publications/techsonar/federated-learning_en (hämtad 2026-04-27).
[35] Integritetsskyddsmyndigheten (IMY), IMY-2023-2602, *Federerad maskininlärning mellan två vårdgivare*, s. 19 f.
[36] https://www.edps.europa.eu/press-publications/publications/techsonar/federated-learning_en (hämtad 2026-04-27).
[37] FN, *PET-Guide*, s. 45 f.

åt kan det skapa negativa konsekvenserna och det är svårt att vidta lämpliga åtgärder för att minska detta.[38]

3.7.2 Nollkunskapsbevis

Nollkunskapsbevis (zero-knowledge proof) är en kryptografisk teknik som möjliggör verifiering av ett påstående utan att ytterligare information om den underliggande datan behöver avslöjas. Den information som ligger till grund för beviset förblir därmed dold för den part som tar emot beviset. Nollkunskapsbevis kan till exempel användas för att verifiera att en person är myndig utan att födelsedatumet eller personnumret delas. Ur ett integritetsperspektiv leder nollkunskapsbevis till att färre uppgifter delas.[39]

Nollkunskapsbevis är för närvarande endast användbart vid enklare bevispåståenden och är inte användbart vid mer komplexa påståenden. Det kan också uppstå problem med tillförlitlighet när flera körningar sker samtidigt och nollkunskapsbevis ska utfärdas parallellt.[40]

3.8 Tekniker för skyddad bearbetning

3.8.1 Betrodda exekveringsmiljöer

En betrodd exekveringsmiljö (trusted execution environment) utgör ett avskilt och skyddat område i en datorprocessors hårdvara. Miljön är isolerad från det ordinarie operativsystemet och andra delar av systemet. Inom detta avskilda område kan känslig information lagras och bearbetas genom att enbart säker, verifierad kod kan köras (exekveras). Eftersom miljön är isolerad från övriga delar av systemet skyddas informationen i miljön även om operativsystemet eller andra delar av systemet skulle komprometteras.[41] Miljön är också väl skyddad mot externa angrepp och påverkas inte av attacker riktade mot andra delar av systemet. Däremot kan skadlig kod som införts

[38] https://www.edps.europa.eu/press-publications/publications/techsonar/federated-learning_en (hämtad 2026-04-27).
[39] OECD, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, s. 17.
[40] FN, *PET-Guide*, s. 49 f.
[41] Integritetsskyddsmyndigheten (IMY), IMY-2025-5444, *Betrodda exekveringsmiljöer för uppkopplade fordon*, s. 8.

i den betrodda miljön inifrån orsaka skada, eftersom isoleringen inte förhindrar interna angrepp.[42]

En betrodd exekveringsmiljö kan tillhandahållas som en avgränsad del i en molnlösning, vilket i sådana sammanhang ofta benämns som en säker enklav (secure enclave).[43] En säker enklav i molnmiljö möjliggör isolering och skydd av känsliga data under bearbetning i enklaven. Genom isoleringen förhindras obehörig åtkomst, inklusive åtkomst från molntjänstleverantören. Det skydd som en säker enklav ger för data under bearbetning kan kombineras med kryptering under överföring och lagring för att uppnå end-to-end-säkerhet i molnlösningar.[44]

Betrodda exekveringsmiljöer kan bidra till ett förbättrat dataskydd genom att säkerställa att data förblir skyddade både under bearbetning och lagring.[45] Vid datadelning kan betrodda exekveringsmiljöer användas av flera parter som skickar krypterade data till en gemensam miljö där datan dekrypteras, analyseras och bearbetas. Det är även möjligt för parterna att verifiera att miljön inte manipulerats eller kompromitterats och att miljön faktiskt är en betrodd exekveringsmiljö. Det görs genom en teknisk och kryptografisk process kallad attestering, där miljön skapar ett bevis på tillstånd som kan kontrolleras av en särskild kontrollfunktion.[46] Attesteringen gör att betrodda exekveringsmiljöer kan användas för att skapa tillit mellan parter som inte har fullt förtroende för varandra.[47]

Den avgränsade miljön innebär att all programvara och alla resurser som krävs för bearbetningen måste finnas inom den betrodda miljön. Detta kan medföra begränsningar i minneskapacitet.[48] Bearbetningar av data i en betrodd exekveringsmiljö kan dock genomföras effektivt, eftersom datamängden bearbetas i klartext och inte under kryptering. Vidare behålls datamängden intakt.[49]

Betrodda exekveringsmiljöer kan ibland förväxlas med begreppet *säker behandlingsmiljö*. Det senare är ett begrepp som ofta förekommer i EU-lagstiftning i samband med att en part ska få tillgång

[42] https://learn.microsoft.com/en-us/azure/confidential-computing/trusted-execution-environment (hämtad 2026-04-15).
[43] FN, *PET-Guide*, s. 51 f.
[44] https://www.ibm.com/think/topics/confidential-computing (hämtad 2026-03-27).
[45] OECD, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, s. 21.
[46] IMY, *Betrodda exekveringsmiljöer för uppkopplade fordon*, s. 11.
[47] IMY, *Betrodda exekveringsmiljöer för uppkopplade fordon*, s. 8 f.
[48] FN, *PET-Guide*, s. 51 f.
[49] The Royal Society, 2023, *From privacy to partnership,* s. 16.

till data för vidareutnyttjande, till exempel i EHDS-förordningen[50]. Begreppet definieras i dataförvaltningsförordningen.[51] Säkra behandlingsmiljöer är inte samma sak som betrodda exekveringsmiljöer, även om de skulle kunna baseras på betrodda exekveringsmiljöer som en del av sin tekniska lösning.

3.8.2 Säker flerpartsberäkning

Säker flerpartsberäkning (secure multi-party computation) utgör en samling kryptografiska tekniker som möjliggör att data förblir krypterad även under bearbetning.[52] Genom denna teknik kan flera aktörer genomföra gemensamma bearbetningar på sina respektive datamängder utan att dela underliggande data med varandra. Endast resultatet av den gemensamma bearbetningen görs tillgängligt för de deltagande parterna.[53] Tekniken innebär att data och personuppgifter inte delas i onödan, vilket stödjer principen om uppgiftsminimering[54].

Säker flerpartsberäkning kan även tillämpas på sekretessbelagda uppgifter, eftersom dessa inte anses röjda när de är krypterade på ett sätt som förhindrar tillgång till innehållet.[55] Tekniken möjliggör dessutom att bearbetningar kan utföras av en tredje part som inte behöver vara betrodd, eftersom underliggande data förblir krypterad under bearbetning.[56]

En utmaning med att göra bearbetningar av krypterade data är att det medför högre kostnader jämfört med bearbetning av data i klartext. Detta beror på att det är mer komplext att bearbeta krypterade data och det därför krävs mer datorkapacitet. En annan utmaning är att förbehandla data inför en säker flerpartsberäkning. Vid traditionell dataanalys kan den aktör som samlat in data för-

[50] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.
[51] Artikel 2.20 Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[52] OECD, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, s. 20.
[53] FN, *PET-Guide*, s. 28.
[54] Artikel 5.1 c i dataskyddsförordningen.
[55] Prop. 2022/23:97 *Sekretessbrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter*, s. 7.
[56] The Royal Society, *From privacy to partnership*, s. 16.

behandla och rensa den innan analysen genomförs. Detta är inte möjligt vid säker flerpartsberäkning, eftersom data inte delas mellan aktörerna. Varje deltagande part behöver därför förbereda och kvalitetssäkra sina egna data för att säkerställa att den gemensamma bearbetningen ger ett korrekt resultat.[57]

Protokoll och algoritmer

Vid användning av säker flerpartsberäkning tillämpas särskilda protokoll och algoritmer som kommer från standardiseringsorganisationerna[58]. Protokollen beskriver steg för steg hur processen ska genomföras för att säkerställa att den sker på ett korrekt och säkert sätt.

De algoritmer som används vid säker flerpartsberäkning utgör den underliggande beräkningslogiken, det vill säga en specificerad beskrivning av vilka beräkningar som ska utföras och hur dessa ska genomföras. Förekomsten av en tydligt definierad algoritm innebär att det i efterhand är möjligt att redogöra för och förstå hur ett visst resultat har beräknats, trots att den data som används i beräkningen är krypterade och inte exponeras för de deltagande parterna.

Algoritmerna är normalt anpassade och optimerade för den aktuella typen av beräkning och det sammanhang där de används. Nedan redovisas några förenklade exempel på algoritmer för säker flerpartsberäkning.

Integritetsfrämjad mängdskärning

Integritetsfrämjad mängdskärning (private set intersection) gör det möjligt att identifiera gemensamma värden i olika aktörers datamängder utan att data delas mellan dem.[59] Ett exempel på användningsområde är om flera myndigheter vill fastställa vilka personer som förekommer i samtliga deltagande myndigheters register. En sådan analys kan då göras utan att uppgifter om andra personer

[57] OECD, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, s. 21 f.
[58] De relevanta standardiseringsorganisationerna beskrivs i avsnitt 5.5.1.
[59] OECD, *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, s. 20.

som enbart förekommer hos någon eller några myndigheter, men inte hos alla, delas.

Integritetsfrämjad jämförelse

Med integritetsfrämjad jämförelse (privacy preserving comparison) kan parter avgöra vilken part som har det minsta eller största värdet utan att avslöja sina värden för varandra.[60] Detta kan exempelvis användas för att avgöra vem som lagt det lägsta anbudet i ett anbudsförfarande eller för att avgöra vilket lager som har mest av en vara i beredskapstid.

Integritetsfrämjad aggregering av statistik

Med integritetsfrämjad aggregering av statistik (privacy-preserving aggregation of statistics) möjliggörs beräkning av statistik på krypterade data. Detta innebär att enskilda värden inte delas med den som ska ta fram statistiken.[61]

3.8.3 Homomorf kryptering

Homomorf kryptering utgör en generell teknik för databehandling under kryptering. Tekniken innebär att behandlingen av data sker under skydd av kryptering oberoende av vad algoritmen har för specifika egenskaper. Detta skiljer sig från säker flerpartsberäkning, där den kryptografiska konstruktionen behöver utformas specifikt för varje typ av algoritm. Homomorf kryptering erbjuder således ett generellt skydd medan säkra flerpartsberäkningar förutsätter ett skräddarsytt skydd för varje typ av bearbetning.

Homomorf kryptering möjliggör bearbetningar av sekretessbelagd information utan att informationen röjs.[62] Tekniken möjliggör även att bearbetning sker hos en annan part utan att den parten kan tillgängliggöra sig något från processen eftersom den data

[60] Den första kryptografiska algoritmen för integritetsfrämjad jämförelse gällde två parter och introducerades av Yao 1982 och den generaliserades till flera parter av Goldreich 1987. Se O. Goldreich, 2021, *Foundations of Cryptography Volume II Basic Applications*.
[61] Y. Lindell, "Secure multiparty computation", *Communications of the ACM*, Volume 64 Issue 1.
[62] Prop. 2022/23:97, s. 7.

som bearbetas är skyddad av kryptering under hela processen.[63] Homomorf kryptering möjliggör därför att bearbetningen även sker i en miljö som i vanliga fall inte skulle bedömts lämplig för att behandla personuppgifter, till exempel i vissa molntjänster.[64]

Tekniken har fördelen att den kan tillämpas för bearbetning av i princip alla typer av data och att den inte medför någon förlust av information.[65] Trots betydande tekniska framsteg är homomorf kryptering fortfarande förenad med flera praktiska begränsningar. Den främsta utmaningen är att bearbetningarna är avsevärt långsammare än på data som inte är krypterad. Detta bidrog till att FN år 2023 bedömde att kostnaden för praktisk tillämpning var hög.[66] Även om homomorf kryptering i dagsläget fortfarande är opraktiskt förutom i specialfall, så går utvecklingen snabbare framåt än vad man tidigare förväntade sig.[67] Det är exempelvis möjligt att med hjälp av AI, som skyddas av fullständig homomorf kryptering, identifiera ett ansikte på mindre än en sekund.[68]

Typer av homomorf kryptering

Det finns tre typer av homomorf kryptering:

- *Partiell homomorf kryptering* (partially homomorphic encryption) tillåter obegränsade beräkningar av samma typ (exempelvis endast additioner eller multiplikationer), men klarar inte att kombinera olika typer av beräkningar.
- *Delvis homomorf kryptering* (somewhat homomorphic encryption) möjliggör flera olika typer av beräkningar, men endast under en begränsad tid eller omfattning. Detta beror på att det brus som byggs upp under processen till slut gör att krypteringsschemat inte kan genomföras lika effektivt.

[63] FN, *PET-Guide*, s. 32.
[64] K. Potter, D. Stilinki & S. Adablanu, 2024, *Homomorphic Encryption for Secure Cloud Computing,* s. 2 och 8.
[65] The Royal Society, *From privacy to partnership,* s. 16.
[66] FN, *PET-Guide*, s. 35.
[67] https://datatracker.ietf.org/meeting/125/materials/slides-125-cfrg-recent-advances-in-fully-homomorphic-encryption-01 (hämtad 2026-03-18).
[68] K. Lam, X. Lu, L. Zhang, X. Wang, H. Wang, S. Q. Goh, 2024, „Efficient FHE-based privacy-enhanced neural network for trustworthy AI-as-a-service", *IEEE Transactions on Dependable and Secure Computing*, s. 3.

- *Fullständig homomorf kryptering* (fully homomorphic encryption) tillåter obegränsade beräkningar av valfri typ utan de begränsningar som finns i de två andra varianterna. Tekniken är dock mycket resurskrävande och kräver omfattande beräkningskapacitet. Fullständig homomorf kryptering bedöms även ha motståndskraft mot kvantdatorattacker.[69]

Utöver dessa finns även hybridvarianter som kombinerar homomorf kryptering med annan kryptografi i syfte att förbättra prestanda och användbarhet. Sådana lösningar befinner sig dock i dagsläget huvudsakligen på forskningsstadiet.[70]

Dold informationshämtning

Ett tillämpningsområde för homomorf kryptering är så kallad dold informationshämtning (private information retrieval). Med hjälp av denna teknik kan sökning och hämtning av information från en databas ske utan att det avslöjas vilken specifik informationspost som efterfrågats.[71] Själva sökförfrågan hålls därmed konfidentiell, samtidigt som tillgången begränsas till den efterfrågade informationen.

Integritetsfrämjande beslutsträdsutvärdering

Homomorf kryptering kan användas för integritetsfrämjande beslutsträdsutvärdering (private decision tree evaluation).[72] Ett beslutsträd är en modell som, likt ett flödesschema, stegvis leder fram till ett beslut eller utfall genom att ange olika alternativ utifrån givna kriterier. Beslutsträd används vid automatiserat beslutsfattande, men förutsätter att all den data som beslutet grundar sig på samlas på ett ställe. Dessa beslutsträd kan både vara en datalogisk formalisering av ett existerande regelverk eller resultatet av AI-träning.[73]

[69] https://digitalprivacy.ieee.org/publications/topics/types-of-homomorphic-encryption/ (hämtad 2026-04-24).
[70] H. Abdinasibfar, C. Nuoskala & A. Michalas, 2025, *The HHE Land: Exploring the Landscape of Hybrid Homomorphic Encryption,* s. 1 f. och 10.
[71] J. Kim, J. Park & H. Sung, 2025, *Private Information Retrieval based on Homomorphic Encryption, Revisited,* s. 1.
[72] Se t.ex. K. Cong, J. Kang, G. Nicolas, J. Park, 2024, *Faster Private Decision Tree Evaluation for Batched Input from Homomorphic Encryption.*
[73] H. Blockeel, L. Devos, B. Frénay, G. Nanfack & S. Nijssen, 2023, "Decision trees: from efficient prediction to responsible AI", *Frontiers in Artificial Intelligence*, avsnitt 2.

Integritetsfrämjande beslutsträdsutvärdering möjliggör att den data som ett beslut grundar sig på inte behöver samlas på ett ställe eller delas mellan dem som bidrar med den.

3.9 Framtiden för integritetsfrämjande teknik

3.9.1 Den kommande utvecklingen

Att förutse utvecklingen av integritetsfrämjande teknik under de närmaste 10–15-årsperioden är förenat med betydande osäkerhet, vilket är kännetecknande för prognoser inom teknologisk innovation. Utredningen har dock identifierat fyra framträdande utvecklingslinjer som vi tror kommer att löpa parallellt med varandra.

Den första utvecklingslinjen avser framsteg inom kryptografi, särskilt avseende möjligheten att bearbeta krypterade data på olika sätt.[74] Denna utveckling visar sig redan i form av

- Krypterad databehandling (encrypted computation), där bearbetningar utförs direkt på krypterade data. Det kan exempelvis ske med homomorf kryptering. Detta möjliggör analys och bearbetning utan att data behöver exponeras i klartext.
- Integritetsbevarande maskininlärning (privacy-preserving machine learning), där träning av AI-modeller kan ske på krypterade eller på annat sätt skyddade data. Detta minskar behovet av att tillgängliggöra data i klartext.
- Konfidentiell databehandling (confidential computing), där data hålls krypterad under hela sin livscykel men tillfälligt kan dekrypteras inom betrodda exekveringsmiljöer i samband med bearbetning.

En grundläggande utmaning med bearbetning av krypterade data är att det är avsevärt mer resurskrävande och tidskrävande än motsvarande bearbetning av okrypterad data. Utvecklingen inom kryptografi samt den underliggande hård- och mjukvaran har återkommande dock överträffat branschens egna prognoser. Det talar för

[74] E.N. Kucur, T. Buyuktanir, M. Ugurelli & K. Yildiz, 2026, ”Privacy-Preserving Machine Learning Techniques: Cryptographic Approaches, Challenges, and Future Directions”, *Applied Sciences*, Vol. 16 Issue 1.

att kryptering kommer att användas i allt större utsträckning framöver (se även avsnitt 3.9.2).

Den andra utvecklingslinjen rör användningen av artificiell intelligens vid utvecklingen av integritetsfrämjande teknik. Redan i dag finns exempel på mjukvaruutveckling där en betydande del av koden genereras med stöd av AI utifrån funktionsbeskrivningar på en högre abstraktionsnivå.[75] Avståndet mellan användare och programkod bedöms minska ytterligare, vilket kan möjliggöra att verksamheter i högre grad själva kan utveckla eller anpassa sina systemstöd. Detta kan i sin tur bidra till att införandet av integritetsfrämjande teknik sker närmare den operativa verksamheten och med mindre behov av it-resurser, särskilt i situationer där flera tekniker behöver kombineras.

Den tredje utvecklingslinjen avser just samspelet mellan olika tekniker. Utvecklingen bedöms gå mot ett mer systematiskt och metodiskt arbete med hur tekniker kombineras, snarare än ett fokus på enskilda lösningar. Olika kombinationer av tekniker kan ge upphov till data med skilda analytiska egenskaper. Det är därför sannolikt att metoder för att finjustera teknikerna kommer att utvecklas i syfte att upprätthålla ett tillräckligt integritetsskydd samtidigt som kvaliteten i analyser och resultat förbättras.[76]

Den fjärde utvecklingslinjen rör integritetsfrämjande tekniker som är användbara inom statistik, särskilt differentiell integritet. Inom statistiken används ofta asymptotiska approximationer[77] vid stora datamängder. Det beror bland annat på att exakta beräkningar traditionellt varit beräkningsmässigt mycket krävande. Sådana approximationer kan dock leda till att mer brus än nödvändigt tillförs, vilket försämrar analysresultatens kvalitet. Utvecklingen inom exempelvis algebraisk statistik, i kombination med ökad beräkningskapacitet och hårdvara som utvecklats för AI-ändamål, bedöms kunna

[75] Se t.ex. https://fortune.com/2026/01/29/100-percent-of-code-at-anthropic-and-openai-is-now-ai-written-boris-cherny-roon/ (2026-05-25).
[76] V. S. Naresh & D. Ayyappa, 2026, ”Privacy-preserving federated credit risk models: evaluating differential privacy and homomorphic encryption techniques”, *Nature Scientific Reports*, 16:4379.
[77] Med asymptotiska approximationer avses förenklade beräkningssätt där exakta värden ersätts av uttryck som ger allt bättre precision ju större datamängden eller problemets storlek är, och som används för att möjliggöra praktiskt hanterbara analyser i situationer där exakta beräkningar är för resurskrävande.

möjliggöra mer exakta metoder.[78] Detta kan på sikt bidra till att uppnå en bättre balans mellan integritetsskydd och analytisk precision.

3.9.2 Kryptering som regel

I dag är kryptering etablerad som standard vid överföring av data och används i ökad utsträckning även vid lagring. Bearbetning av data sker alltjämt i huvudsak i klartext. Mot bakgrund av den tekniska utvecklingen och ökade krav på skydd för personuppgifter och andra känsliga uppgifter bedömer utredningen att en utveckling där kryptering i allt högre grad genomsyrar hela samhällets informationshantering är sannolik på längre sikt. En sådan utveckling innebär att data inte endast är krypterad vid överföring och lagring utan även vid själva bearbetningen, vilket möjliggör att ett högt skydd upprätthålls genom datans hela livscykel. Sammantaget framstår det därför som sannolikt att kryptering successivt utvecklas från att utgöra en kompletterande skyddsåtgärd till att bli till regel i all datahantering, där dekryptering endast sker i särskilt motiverade fall.

Vid ett införande av kryptering som regel bör data hanteras genom ett sammanhållet krypterat flöde, där uppgifter krypteras vid införsel i system och endast dekrypteras när det är nödvändigt. För att säkerställa en rättssäker hantering kan det krävas att uppgifterna kompletteras med standardiserade metadata, som till exempel kan omfatta uppgift om rättslig grund, ansvarig aktör och gallringstid. Vidare bör samtliga relevanta åtgärder loggas. Dekryptering bör endast få ske när det finns rättsligt stöd och sådana åtgärder ska dokumenteras. En sådan ordning innebär att endast den information som är nödvändig exponeras i klartext, vilket bidrar till ett stärkt integritetsskydd.

En konsekvens av en sådan modell är att de rättsliga avvägningarna i högre grad kan knytas till tidpunkten för dekryptering snarare än till själva datadelningen. Det kan möjliggöra ett utökat utbyte av krypterad information samtidigt som den faktiska exponeringen av personuppgifter begränsas. Sammantaget innebär modellen att mer data kan delas, men att mindre data görs tillgänglig i läsbar form.

[78] G. Pistone, E. Riccomagno & H.P. Wynn, 2001, *Algebraic statistics Computational commutative algebra in statistics* och M. Drton, B. Sturmfels & S. Sullivant, 2008, *Lectures on Algebraic Statistics*.

En ordning med kryptering som regel ligger nära den moderna cybersäkerhetsmodellen Zero Trust. Det är en modell där tillit inte utgår från systemgränser eller organisatoriska avgränsningar. I stället baseras säkerheten på tekniska kontrollmekanismer, så som autentisering och kryptering. Zero trust utgår från att ingen användare, enhet eller tjänst automatiskt ska betraktas som betrodd. All åtkomst ska därför fortlöpande verifieras utifrån identitet, behörighet och aktuell säkerhetsstatus i syfte att minimera risken för intrång och obehörig åtkomst. Syftet med en sådan modell är att minska risken för obehörig åtkomst samt att begränsa konsekvenserna av intrång. Modellen innebär således att fasta säkerhetsgränser ersätts av en mer dynamisk och situationsanpassad säkerhetsnivå, där verksamhetens behov ges ett ökat genomslag. Forskning visar att cybersäkerhetsincidenter minskar med Zero Trust och att det finns stora verksamhetsnyttor.[79]

Kryptering som regel kan få liknande effekter som Zero Trust inom en myndighet. Om data genomgående är krypterad minskar betydelsen av dess fysiska lagringsplats och åtkomsten till dekrypterade data kan i stället styras. Detta möjliggör en mer differentierad informationsåtkomst beroende på sammanhang, exempelvis utifrån var och hur arbetet bedrivs. En ytterligare fördel är att säkerhetsnivån kan anpassas vid förändrade hotbilder. Genom styrning av nyckelhantering och åtkomstpolicyer kan möjligheten att ta del av data i klartext begränsas eller tillfälligt upphöra, samtidigt som den underliggande bearbetningen kan fortgå i krypterad form. Därigenom kan verksamhetskontinuiteten upprätthållas även vid förhöjd riskexponering.

[79] Z. Adahman, A. W. Malik & Z. Anwar, 2022, ”An analysis of zero-trust architecture and its cost-effectiveness for organizational security”, *Computers & Security*, Volume 122.

Drivkrafter framåt

Inledningsvis förväntas en ökad användning av kryptering främst efterfrågas av aktörer med höga krav på integritet, även till en högre kostnad. Med tiden bedöms dock krypterad databehandling utvecklas till en allmänt tillgänglig standard.

Det finns en risk att offentlig förvaltning halkar efter denna utveckling. Om privatpersoner och företag möter en högre nivå av integritetsskydd på marknaden än i sina kontakter med myndigheter kan förtroendet för myndigheternas datahantering påverkas negativt. Detta talar för att myndigheter bör inta en mer aktiv roll i att utveckla och tillämpa sådana lösningar.

Utvecklingen mot kryptering som regel drivs i hög grad av marknadsförväntningar. Myndigheter med säkerhetskänslig verksamhet har i många fall redan påbörjat eller etablerat den kompetens som krävs, vilket indikerar att en bredare tillämpning inte är enbart en fråga för framtiden.

4 Användningen av integritetsfrämjande teknik

4.1 Inledning

För att kunna bedöma förutsättningarna för en ökad användning av integritetsfrämjande teknik vid datadelning i offentlig förvaltning har utredningen behövt få en bild av hur den nuvarande användningen ser ut. För att göra detta har vi genomfört en kartläggning av hur teknikerna används i förvaltningen. Vi har även undersökt den privata marknaden för att få en uppfattning om i vilken utsträckning och på vilket sätt privata aktörer kan bidra till en ökad användning av teknikerna. En annan viktig aspekt för bedömningen har varit att utforska vad teknikerna kan ha för användningsområden.

I detta kapitel redovisas resultatet av vår kartläggning (avsnitt 4.2). Vidare redogör vi för undersökningen av den privata marknaden (avsnitt 4.3). Vi redovisar också nationella och internationella exempel där integritetsfrämjande teknik har använts inom olika områden (avsnitt 4.4).

4.2 Nuvarande användning i offentlig förvaltning

Under hösten 2025 genomförde utredningen en enkätundersökning om användningen av integritetsfrämjande teknik[1]. Enkätundersökningen riktade sig till ett urval av statliga myndigheter (inklusive länsstyrelser), kommuner och regioner som hanterar stora mängder data. Enkäten skickades till sammanlagt 38 offentliga aktörer varav 23 av dessa besvarade enkäten. I enkäten frågade utredningen om aktören använder integritetsfrämjande teknik i dag och i så fall vilka

[1] I enkäten användes begreppet *integritetsbevarande metoder*.

tekniker som används och inom vilka användningsområden. Vi frågade också om potentiella användningsområden och vilka de största hindren mot att använda teknikerna är.

Resultaten från enkäten har bekräftats under de workshoppar som har genomförts med myndigheter, regioner och kommuner.

4.2.1 Användningen av moderna tekniker är begränsad

Av de offentliga aktörer som besvarat enkäten har de flesta erfarenhet av olika avidentifieringstekniker, framför allt de etablerade teknikerna så som anonymisering och pseudonymisering. Många av de som svarat har även uppgett att de har erfarenhet av betrodda exekveringsmiljöer[2]. Användningen av andra moderna tekniker för skyddad bearbetning och uppgiftsminimerande tekniker är dock låg.

Tabell 4.1 Antal användare av respektive teknik

Teknik	Antal användare
Anonymisering	20
Pseudonymisering	18
Generalisering	11
Syntetiska data	10
Betrodda exekveringsmiljöer	9
Randomisering	4
Differentiell integritet	2
Federerad inlärning	2
Säker flerpartsberäkning	1
Nollkunskapsbevis	1
Homomorf kryptering	0

Källa: Utredningens enkät hösten 2025. Dnr Komm2025/00491.

Vissa försvarsmyndigheter och brottsbekämpande myndigheter har inte bevarat enkäten med hänvisning till sekretess. Användningen av vissa integritetsfrämjande tekniker inom offentlig förvaltning kan därför vara vanligare än vad enkätresultaten visar.

[2] I enkäten användes begreppet *säkra exekveringsmiljöer*.

4.2.2 Användningsområden

Av enkäten framgår att integritetsfrämjande teknik ofta används internt av offentliga aktörer. Det är främst avidentifieringstekniker som används vid sammanställning av statistik för internt bruk och för framtagande av testdata. Integritetsfrämjande teknik används också inom AI och maskininlärning, av exempelvis Kronofogdemyndigheten. Teknikerna används även vid sammanställning av statistik för publicering eller forskningsverksamhet samt vid delning av data och vid utlämnande av allmän handling. E-hälsomyndigheten har uppgett att de bland annat använder teknikerna vid delning av sekretessbelagda uppgifter mellan myndigheter och regioner.

Majoriteten av de offentliga aktörer som besvarat enkäten anser att integritetsfrämjande teknik kan användas inom fler områden i deras respektive verksamheter. Ett potentiellt användningsområde är samkörning av pseudonymiserade uppgifter mellan förvaltningar inom kommuner, till exempel mellan skolförvaltning och socialförvaltning för att identifiera barn i riskzon som är i behov av stödinsatser. Andra potentiella användningsområden som nämnts är datadelning generellt, träning av AI-modeller och att pseudonymisering kan möjliggöra överföring av uppgifter till tredjeland vid användning av externa AI-verktyg.

4.2.3 Hinder mot användning

Enligt enkätsvaren är de största hindren mot användning av integritetsfrämjande teknik inom offentlig förvaltning att teknikerna är tekniskt komplicerade och att man saknar kunskap om dem. Ett annat hinder är att de rättsliga förutsättningarna för användningen av teknikerna inte är utredda, och det kan därför uppfattas som att teknikerna inte får användas. Några andra hinder som förts fram är att det finns gamla it-system som inte är anpassade för integritetsfrämjande teknik, att användbarheten av data blir låg efter användning av teknikerna, att sekretess kan hindra delning av data och att det saknas standarder vilket försvårar datadelning mellan olika system.

I workshopparna som genomförts med myndigheter, regioner och kommuner har bilden av hindren förtydligats. En insikt från dessa är att det inte bara är kunskap om teknikerna som saknas utan också kunskap om vilka nyttor som skulle kunna åstadkommas om

integritetsfrämjande teknik användes i större utsträckning. Detta gäller särskilt för kommuner och regioner. Det har också framkommit att de rättsliga förutsättningarna för att använda etablerade avidentifieringstekniker i regel är klara men att hindret består av en osäkerhet om när teknikerna har använts i tillräckligt stor utsträckning. Vad gäller olika tekniker som involverar kryptering har det också lyfts fram att man är osäker på vilka krav som ställs på kryptering och risken för att krypteringen bryts längre fram.

4.3 Undersökning av den privata marknaden

4.3.1 Om undersökningen

För att få en bättre bild av hur tekniskt mogna teknikerna är för användning har utredningen undersökt den privata marknaden och vilket utbud som finns tillgängligt hos potentiella leverantörer.[3] Eftersom etablerade avidentifieringstekniker redan används i stor utsträckning har dessa inte inkluderats i undersökningen. Fokus har i första hand varit på den svenska och den europeiska marknaden. I de fall det funnits få leverantörer har även marknaden utanför EU undersökts. Det kan finnas rättsliga, strategiska och säkerhetsmässiga skäl till att en offentlig aktör inte väljer en leverantör utanför EU. Vi har dock inte tagit ställning till sådana överväganden, utan har bara undersökt tillgången.

Ett alternativ till att köpa in färdiga lösningar är att utveckla egna lösningar med hjälp av konsulter. Därför har utredningen också undersökt vilka möjligheter det finns att anlita företag verksamma i Sverige som har kunskap om de olika teknikerna.

Undersökningen har inte haft ambitionen att vara heltäckande. Den har endast syftat till att ge utredningen en uppfattning om vad en offentlig aktör har för möjligheter att upphandla lösningar och att ta hjälp för att komma i gång med användningen av olika integritetsfrämjande tekniker. Informationen har hämtats från företagens egna webbplatser samt från olika rapporter, tidningsartiklar och liknande. Resultatet är därför beroende av hur mycket företagen själva marknadsför sina produkter och hur väl de finns beskrivna.

[3] Dnr Komm2025/00605.

Den workshop som utredningen har genomfört med representanter från den privata sektorn har bekräftat bilden av hur marknaden ser ut.[4] En viktig insikt från workshoppen är att det finns expertkunskap om teknikerna i Sverige men att kunskapen inte är särskilt utbredd.

4.3.2 Undersökningens resultat

Det finns några svenska företag som erbjuder software-as-a-service-lösningar för syntetiska data. När det gäller federerad inlärning, differentiell integritet och betrodda exekveringsmiljöer finns det enstaka svenska företag som tillhandahåller plattformar för teknikerna. Det finns också flera företag som på olika sätt arbetar med eller har kunskap om syntetiska data, federerad inlärning och differentiell integritet. Så vitt utredningen har kunnat utröna finns det inget svenskt företag som erbjuder färdiga lösningar för homomorf kryptering, nollkunskapsbevis eller säker flerpartsberäkning men det finns ett fåtal svenska företag med kunskap om teknikerna.

För samtliga tekniker finns det aktörer inom EU som erbjuder olika produkter. I en kartläggning över europeiska företag inom cybersäkerhet listas 145 företag i kategorin moln och dataskydd.[5] I den kategorin ingår företag som arbetar med syntetiska data och differentiell integritet men även andra lösningar som inte avser integritetsfrämjande teknik. I kategorin kryptering, som kan innefatta homomorf kryptering, säker flerpartsberäkning och nollkunskapsbevis återfinns 21 företag.

För homomorf kryptering har utredningen endast kunnat finna ett företag inom EU som är specialiserat på tekniken. På den internationella marknaden finns det dock både open source-lösningar och specialister att få stöd av, men utbudet är även där begränsat.

[4] Se anteckningar och enkätsvar från workshoppen, dnr Komm2026/00105.
[5] https://european-champions.org/wp-content/uploads/2025/01/ECA_European_Cybersecurity_Mapping_2025_Startups_and_Scaleups_Edition.pdf (hämtad 2026-03-26).

4.4 Exempel på användning av integritetsfrämjande teknik

I dagsläget används moderna integritetsfrämjande tekniker endast i begränsad utsträckning i offentlig förvaltning. Det finns dock ett växande intresse för moderna tekniker inom flera områden. I detta avsnitt redovisas en sammanställning av relevanta användningsområden där dessa tekniker har använts eller prövats i pilotprojekt och regulatoriska sandlådor. Beskrivningarna utgår från rapporter och liknande vilka beskriver den aktuella användningen, nyttor som teknikanvändningen har medfört och eventuella begränsningar eller problem som uppmärksammats. Det saknas i regel information om huruvida användningen har fortsatt efter projekten har avslutats.

4.4.1 Hälso- och sjukvård

Inom hälso- och sjukvård behandlas ett stort antal känsliga personuppgifter som omfattas av både dataskyddsregelverk och sekretess. En ökad delning och användning av denna data har stor potential när det gäller att skapa nyttor inom flera verksamhetsområden. Genom användning av integritetsfrämjande teknik kan riskerna för identifiering av patienter eller otillbörlig användning av uppgifter minskas, samtidigt som data fortsatt kan användas för vård, samverkan och forskning. Till exempel kan federerad inlärning och syntetiska data användas för att skydda integriteten vid användning av integritetskänsliga uppgifter. Även säker flerpartsberäkning kan användas för att möjliggöra datadelning som annars inte varit tillåten.

Utveckling och träning av AI-modeller

AI Sweden har tillsammans med Region Västerbotten, Örebro universitet och SynData utforskat möjligheten att skapa syntetiska data för utveckling och träning av AI-modeller inom sjukvården.[6] I det aktuella projektet var målet att kunna förutsäga vårdtider. I februari 2022 presenterades rapporten från den första projektfasen där fokus var att utforska hur användbara syntetiska data inom vården är och hur träffsäkerheten för prediktionsmodeller skiljer sig åt beroende

[6] Läs mer i rapporten från AI Sweden, 2022, *Syntetiska data inom intensivvård*.

på om träningen skett på syntetiska data eller ursprungsdata. I projektet tränades sju olika modeller för att skapa syntetiska data som därefter tränat modeller för att förutsäga vårdtid på respektive datamängd. I en av modellerna användes också differentiell integritet vid syntetiseringen. Denna modell visade sig ge bäst skydd för integriteten även om samtliga modeller generellt visade en hög nivå av integritetsskydd.[7]

Pilotprojekt om AI-träning

IMY har tillsammans med Region Halland, Sahlgrenska Universitetssjukhuset och AI Sweden utforskat användningen av federerad maskininlärning mellan två vårdgivare.[8] Projektet genomfördes som ett pilotprojekt med regulatorisk testverksamhet. Numera bedrivs denna typ av projekt inom ramen för IMY:s innovationssandlåda för dataskydd.

Hypotesen för pilotprojektet var att träna varsin lokal maskininlärningsmodell, därefter kombinera lärdomarna till en gemensam maskininlärningsmodell och sedan upprepa träningen på den lokala datan i syfte att inte överföra några personuppgifter mellan parterna. Av IMY:s rapport framgår att det i det aktuella fallet inte kunde uteslutas att det gick att få fram personuppgifter från den andra parten genom användning av olika attacker även om det hade varit komplicerat. Några andra integritetsfrämjande tekniker testades dock inte i kombination med federerad inlärning för att minska den risken. Det hade möjligen kunnat påverka slutsatserna.

Avancerad medicinsk forskning över nationsgränser

Forskningsprojektet Federated Secure Computing startade 2019 för att analysera data om cancerpatienter över nationsgränser med hjälp av säker flerpartsberäkning.[9] Resultatet från projektet presenterades under 2024 och visade att avancerad medicinsk forskning

[7] AI Sweden, *Syntetiska data inom intensivvård*, Bilaga 2 ”Evaluation of Syntethic Data” s. 4.
[8] Läs mer i rapporten från Integritetsskyddsmyndigheten (IMY), IMY-2023-2602, *Federerad maskininlärning mellan två vårdgivare*.
[9] Läs mer på https://www.med.lmu.de/en/latest-news/news-overview/news/data-security-breakthrough-in-research-with-health-data-a8ac0a4e.html (hämtad 2026-02-26) och https://cyber.ee/resources/news/federated-secure-computing-2024/ (hämtad 2026-02-13).

kan genomföras över nationsgränser utan att rådata behöver delas mellan parterna.[10] I projektet deltog ett tyskt och ett italienskt sjukhus som testade tekniken i en internationell klinisk studie för att analysera och förbättra behandlingen av patienter med binjuremetastaser. De två sjukhusen krypterade sin patientdata och bearbetningarna utfördes sedan på tre olika säkra servrar, som var och en bara hanterade en del av informationen. Efter beräkningarna presenterades aggregerade resultat i form av statistik och medelvärden. Forskarna upplevde att metoden ökade säkerheten och möjliggjorde samarbeten som annars inte hade varit möjliga på grund av sekretess. En erfarenhet från projektet var att tekniken kräver viss expertkunskap vid installation och drift. En annan erfarenhet var att vissa administrativa processer, så som etikgodkännanden och avtal, blev omfattande eftersom tekniken är ny.

4.4.2 Brottsförebyggande och brottsbekämpning

I den brottsförebyggande och brottsbekämpande verksamheten krävs ofta omfattande datainsamling och analys, vilket kan innebära behandling av särskilt skyddsvärda personuppgifter om lagöverträdelser. Insamlingen kan också inkludera överskottsinformation. Användning av integritetsfrämjande teknik kan bidra till att säkerställa att enbart den information som är nödvändig för ändamålet behandlas, att åtkomsten begränsas samt att uppgifterna skyddas mot obehörig användning. Genom att använda integritetsfrämjande tekniker så som federerad inlärning och homomorf kryptering kan myndigheter minska intrånget i den personliga integriteten samtidigt som de behåller möjligheten att effektivt förebygga och utreda brott.

Regulatorisk sandlåda om penningtvätt

I Norge har Datatilsynets regulatoriska sandlåda för ansvarsfull AI under 2022 utforskat möjligheten för banker att träna en gemensam AI-modell för att motverka penningtvätt och finansiering av terrorism. AI-modellerna ska bland annat hjälpa bankerna att identifiera misstankar om ekonomisk brottslighet. Ofta sker den lokala

[10] H. Ballhausen, S. Corradini, C. Belka et al., 2024, "Privacy-friendly evaluation of patient data with secure multiparty computation in a European pilot study", *npj Digit. Med. 7*.

träningen parallellt hos respektive deltagare men i det här fallet har man utforskat möjligheten att träna modellen hos en deltagande part i taget. Efter varje träningstillfälle har kvalitetssäkring och kontroll av dataläckage genomförts. Från sandlådan har Datatilsynet bland annat dragit slutsatsen att risken för att personuppgifter kan återskapas ur modellerna är låg men att risken är svår att bedöma eftersom tekniken är ny och kunskapen begränsad.[11]

Regulatorisk sandlåda om underrättelser mellan olika jurisdiktioner

Singapores digitaliseringsmyndighet (Infocomm Media Development Authority) har genomfört ett sandlådeprojekt om homomorf kryptering tillsammans med Mastercard. Projektets syfte var att undersöka möjligheterna för säker delning av underrättelser om ekonomisk brottslighet mellan olika jurisdiktioner (Singapore, Indien, USA och Förenade kungariket). Målet var att förebygga bedrägerier som sker över nationsgränser genom att möjliggöra informationsutbyte mellan olika länder utan att försämra skyddet för den personliga integriteten.

Slutsatserna från projektet var att homomorf kryptering är en teknik med betydande potential och att den kan bidra positivt både till dataskydd och till möjligheterna att dela information över nationsgränser. Samtidigt identifierades vissa utmaningar, bland annat kopplat till administration av krypteringsnycklar och användarupplevelsen. Vidare konstaterades att det fanns vissa regulatoriska frågor avseende banksekretess som behövde utredas ytterligare. Samtidigt bedömde myndigheten att identifierade risker borde kunna hanteras genom förstärkta styrningsmekanismer, exempelvis användning av förhandsgodkända typer av förfrågningar eller genom att resultat aggregeras innan dekryptering.[12]

[11] Datatilsynet, 2022, *Maskinlæring uten datadeling: Bruk av føderert læring for antihvitvasking* s. 3 och 21 f.
[12] Infocomm Media Development Authority, *Preventing financial fraud across different jurisdictions with secure collaborations IMDA PET sandbox – Mastercard case study*.

4.4.3 Socialförsäkring

Inom socialförsäkringen behandlas stora mängder känsliga personuppgifter om individers hälsa, ekonomi och livssituation. Integritetsfrämjande tekniker som skyddar uppgifter under bearbetning kan bland annat användas för att skydda den personliga integriteten samtidigt som myndigheter kan fatta korrekta beslut och samverka effektivt.

I Nederländerna har man använt säker flerpartsberäkning och homomorf kryptering i ett pilotprojekt för att identifiera personer som har rätt till ett visst bidrag.[13] Det aktuella bidraget riktar sig till pensionärer med en samlad hushållsinkomst under en fastställd miniminivå och som bara cirka hälften av de berättigade personerna har ansökt om. För att identifiera personerna behövdes uppgifter både om hushållens sammansättning och deras inkomster, vilket fanns hos två olika nederländska myndigheter. Att dela uppgifterna direkt mellan myndigheterna bedömdes innebära höga risker för enskildas personliga integritet varför ett pilotprojekt inleddes för att utforska ett alternativt sätt att dela uppgifterna.

I projektet gjordes beräkningarna i flera steg, där myndigheten som ansvarar för bidraget och har uppgift om hushållens sammansättning inledningsvis levererade en lista över hushållen till den andra myndigheten. Den myndigheten tog därefter fram bruttoinkomstdata, krypterade uppgifterna och skickade tillbaka dessa. Därefter beräknades nettoinkomster per individ och hushåll under kryptering och sedan jämfördes de krypterade inkomsterna med tröskelvärdet för bidraget med hjälp av ett framtaget jämförelseprotokoll. När beräkningarna var klara hade den första myndigheten en lista över personer vars hushållsinkomst låg under tröskelvärdet utan att myndigheten hade fått reda på den faktiska inkomsten.[14] Lösningen används nu för att nå personer som kan ha rätt till bidraget.[15]

[13] Läs en sammanfattning av pilotprojektet på https://ercim-news.ercim.eu/en126/special/increasing-access-to-social-welfare-programmes-with-proportional-data-usage (hämtad 2026-02-23).
[14] https://www.tno.nl/en/technology-science/technologies/secure-multi-party-computation/#:~:text=By%20combining%20data%2C%20the%20government%20can%20improve,without%20gaining%20access%20to%20their%20income%20data (hämtad 2026-02-23).
[15] https://www.svb.nl/nl/innovatie/experimenten/mpc-oplossing-voor-het-terugdringen-van-niet-gebruik-aio (hämtad 2026-02-23).

4.4.4 Cybersäkerhet

Inom cybersäkerhetsområdet behandlas ofta omfattande datamängder som kan innehålla personuppgifter så som loggar och uppgifter om användarbeteenden. Genom att använda flera olika integritetsfrämjande tekniker kan organisationer stärka sin motståndskraft mot cyberhot samtidigt som analyser kan genomföras utan att data exponeras i onödan. Användningen av integritetsfrämjande teknik kan även bidra till att uppfylla krav på dataminimering och inbyggt dataskydd.

HARPOCRATES var ett EU-finansierat forskningsprojekt som avslutades i september 2025.[16] Projektet kombinerade användningen av federerad inlärning, betrodda exekveringsmiljöer och homomorf kryptering för att utveckla lösningar där analyser och maskininlärning kan ske utan att någon part ser de faktiska uppgifterna. Tekniken testades i två pilotprojekt, ett inom hälsa och ett inom cybersäkerhet. I det senare byggdes en modell för att upptäcka cyberhot, där regionala myndigheter först tränar lokala modeller för att sedan träna en gemensam modell på resultaten från de lokala modellerna. För att skydda modellinformationen som skickas mellan de lokala modellerna och den centrala användes homomorf kryptering. Även beräkningarna gjordes i en betrodd exekveringsmiljö för att garantera att de utfördes korrekt och skyddat. Lösningen har visat sig kunna hjälpa organisationer att upptäcka avancerade cyberhot utan att försämra effektiviteten och visade god prestanda i fråga om hastighet, minnesanvändning och lagringskrav. De främsta utmaningarna för lösningen var i träningsfasen då det krävdes att varje lokal modell hade tillräcklig mängd data samt att denna hade likartad struktur och kvalitet som övriga data. Användningen av homomorf kryptering medförde även att träningstiden ökade.

4.4.5 Digitala tjänster och service till medborgare

Utveckling av avancerade digitala tjänster och service kan vara beroende av data om användares beteenden, preferenser och ärenden, vilket i vissa fall kan omfatta integritetskänsliga uppgifter. Genom att använda integritetsfrämjande teknik så som federerad inlärning

[16] Läs mer om projektet på https://harpocrates-project.eu/ (hämtad 2026-02-13) och https://cordis.europa.eu/project/id/101069535 (hämtad 2026-02-13).

kan träning av AI-modeller genomföras utan att personuppgifter behöver delas. Användningen av exempelvis nollkunskapsbevis och betrodda exekveringsmiljöer kan även bidra till att tjänster utformas så att endast den data som är nödvändig för ändamålet behandlas, samtidigt som risken för obehörig åtkomst eller otillbörlig användning av uppgifter minskar.

Digitala val

I Estland infördes digitala val redan 2005 och sedan dess kan röstning ske digitalt både i nationella och europeiska val efter elektronisk identifiering.[17] Den lösning som används för val har flera lager säkerhet och rösterna krypteras och anonymiseras innan de dekrypteras för att räknas. En brist i systemet är dock att det inte går att kontrollera att varje krypterad röst är en giltig röst och under valet till Europaparlamentet 2024 tog sig en ogiltig röst fram till dekrypteringen. Problemet med att sortera bort ogiltiga röster är att det inte går att bevisa att valmyndigheten bara har tagit bort ogiltiga röster. En studie har därför undersökt om problemet kan lösas med hjälp av nollkunskapsbevis. Studien visar att användningen av nollkunskapsbevis skulle kunna visa att rösten är giltig utan att röstsedeln behöver dekrypteras och avslöja vilken kandidat som rösten har lagts på. Vidare visar studien att lösningen är tekniskt genomförbar, att den fungerar med Estlands befintliga digitala infrastruktur och att den kan skalas upp till stora val. Det betonas dock att nollkunskapsbevis är tekniskt komplicerade och att även om de fungerar bra så är de svåra att förklara för allmänheten.

Gemensam AI-assistent för offentlig sektor

Estland har lanserat en gemensam AI-assistent för offentlig sektor som kallas för Bürokratt[18]. Genom att chatta med Bürokratt ska medborgare kunna få svar på frågor från olika myndigheter och utföra olika myndighetsärenden med hjälp av samma assistent. Målet är att Bürokratt ska fungera som spindeln i nätet och koppla ihop

[17] Läs mer på https://www.nature.com/articles/s41598-025-16764-1 (hämtad 2026-02-24).
[18] Läs mer om Bürokratt på https://www.ria.ee/en/state-information-system/personal-services/burokratt (hämtad 2026-02-20).

olika myndighetstjänster. Den underliggande informationen, och beslutsunderlagen, ligger dock fortfarande kvar hos respektive myndighet. I AI-assistenten pseudonymiseras direkta identifierare och i en rapport från 2023 framgår det att användningen av federerad inlärning och syntetiska data kan bli aktuellt att använda för att träna Bürokratt.[19]

Plattform för säker delning och analys av känsliga data

TITAN är ett EU-finansierat forskningsprojekt som syftar till att göra det praktiskt möjligt att dela och analysera känsliga data med hjälp av betrodda exekveringsmiljöer, avidentifieringstekniker och nollkunskapsbevis. Vidare möjliggör TITAN träning av AI-modeller med federerad inlärning och beräkningar i betrodda exekveringsmiljöer. Projektet startade 2024 och ska avslutas i januari 2027.[20]

Ett av testfallen för TITAN rör offentlig sektor där vinodlare i vissa delar av Spanien och Italien ska få bättre beslutsunderlag för åtgärder som bevattning, gödsling och skadedjursbekämpning genom en AI-modell. För att bygga sådana AI-modeller krävs detaljerade data om bland annat enskilda vingårdars odlingsmetoder och skadedjurslägen. Även vissa ekonomiska uppgifter kan behövas. Av konkurrensskäl är detta uppgifter som vinodlarna inte vill dela. Därför skapas en decentraliserad och säker infrastruktur där deltagarna själva kan styra hur deras data får användas. Datamängderna samlas in både från vinodlarna och lokala myndigheter och kombineras med offentlig information så som väderprognoser, klimatdata och satellitbilder.

Att använda avidentifieringstekniker är en viktig del av projektet eftersom all data som kan kopplas till en specifik vingård måste anonymiseras. Projektet ska också testa olika sätt att bygga AI-modeller för olika scenarion beroende på hur känslig den data som ska hanteras och delas är.

[19] https://www.kratid.ee/en/analuusid-ja-uuringud (hämtad 2026-02-25).
[20] Läs mer om projektet på https://cordis.europa.eu/project/id/101129822 (hämtad 2026-02-13) och https://titan-eosc.eu/ (hämtad 2026-02-13).

Förvaltningsgemensam tjänst för testdata

Norge har skapat en förvaltningsgemensam tjänst för testdata, Tenor testdatasök.[21] Tjänsten är en söktjänst för syntetiska testdata och används som ett arbetsverktyg för systemutveckling och integrationstester mellan offentlig och privat sektor i Norge. Det finns syntetiska testdata från Folkeregisteret, Brønnøysundregisteret, Skatteetaten, NAV, Digitaliseringsdirektoratet och Statens vegvesen.

Målet med Tenor testdatasök är att förenkla integrationstester mellan olika verksamheter. Tjänsten ger tillgång till testdata för runt 1,1 miljoner fiktiva personer och nästan 600 000 fiktiva företag. De fiktiva personerna i testdatan skapas av Folkeregisteret och har ingen koppling till verkliga personer. Andra myndigheter kan i tjänsten tillföra ytterligare attribut till dessa fiktiva personer.

Genom att samla sökbara testdata på ett ställe kan användare exempelvis hitta en syntetisk person som både är gift (data från Folkeregisteret) och har ett anställningsförhållande (data från NAV), för att därefter använda denna person i tester mot ett specifikt system. Det finns ingen exakt statistik över hur mycket tjänsten används men över hundra verksamheter är anslutna till tjänstens API[22].

4.4.6 Statistik

Statistik baseras på stora mängder data om individer som i vissa fall kan vara integritetskänsliga. Genom att använda integritetsfrämjande tekniker som differentiell integritet och säker flerpartsberäkning kan data bearbetas och sammanställas på ett sätt som förhindrar att enskilda individer identifieras, samtidigt som statistikens kvalitet och användbarhet bevaras.

Publicering av uppgifter ur födelseregister

I Israel har differentiell integritet och syntetiska data använts för att tillgängliggöra data ur det nationella födelseregistret. Registret innehåller både uppgifter om modern och barnet och är en av landets mest heltäckande källor till kunskap om befolkningen, familjer och

[21] Läs mer på https://www.skatteetaten.no/testdata/ (hämtad 2026-04-07).
[22] Application Programming Interface är ett standardiserat gränssnitt för kommunikation mellan olika system.

hälsa. Målen med att tillgängliggöra uppgifter ur registret var att hjälpa forskare och beslutsfattare att följa födelsetrender, för att se mönster som påverkar hälsan hos barn och mödrar för att skapa bättre politik i framtiden. I februari 2024 lanserades en första, begränsad datamängd ur registret för att testa konceptet.[23]

Den begränsade datamängd som tillgängliggjordes innehåller sex olika variabler med data, bland annat födelsevikt och kön, presenterade som mikrodata. För att kunna presentera data på mikronivå var det inte möjligt att endast använda differentiell integritet eftersom det var svårt att hitta en nivå av brus som både skyddade individerna och skapade användbara data. Lösningen blev därför att skapa syntetiska data genom att träna en modell på uppgifterna i födelseregistret och att använda differentiell integritet för uppgifterna under träningen. För tillförseln av brus sattes den tillåtna nivån av integritetsförlust (epsilon, ε) till 9,98 vilket bedömdes ge tillräckligt starkt skydd mot realistiska angripare samtidigt som det gav syntetiska data av hög kvalitet. Det sattes också upp acceptanskriterier som den syntetiska datamängden behövde klara så att den inte avvek allt för mycket för de ursprungliga uppgifterna.

Testet visar att det är möjligt att publicera känsliga födelsedata som bevarar individernas integritet samtidigt som informationen blir användbar. Ytterligare en slutsats från projektet är att det finns behov av mer utvecklade metoder för att bestämma den tillåtna nivån för integritetsförlust på ett systematiskt och transparent sätt.

Publicering av folkräkningsuppgifter

Ett välkänt exempel på när differentiell integritet använts i stor skala är när US Census Bureau använde tekniken för att offentliggöra stora delar av statistiken för 2020 års folkräkning i USA. Tekniken valdes efter att en stor del av befolkningen hade identifierats ur data

[23] Läs mer om testet i artikel från S. Hod & R. Canettis, 2025, *Differentially Private Release of Israel's National Registry of Live Births*.

från folkräkningen 2010.[24] Den valda nivån av integritetsförlust (epsilon, ε)[25] sattes till 19,61.[26]

Gemensam plattform för statistikmyndigheter

Den europeiska statistikmyndigheten Eurostat driver projektet JOCONDE tillsammans med ett estniskt företag.[27] Syftet är att främja användningen av integritetsfrämjande teknik inom det europeiska statistiksystemet med målet att utveckla en gemensam europeisk plattform (Multi-Party Secure Private Computing-as-a-service[28]) som kan användas av statistikmyndigheterna. En sådan plattform ska minska behovet för respektive statistikmyndighet att själva ha specialistkompetens inom exempelvis kryptografi.

I projektet testas användningen av säker flerpartsberäkning i en betrodd exekveringsmiljö för att skapa en lösning där flera organisationer kan göra beräkningar på känsliga data utan att dela dem med varandra. Ett fall som testats handlar om att två länder inom EU ville ta reda på hur många personer som är registrerade som boende i båda länder. Genom att jämföra invånaruppgifter med stöd av teknikerna kan länderna få fram uppgifter om hur många som är registrerade som boende i båda länderna utan att det framkommer vilka personerna är.

Projektet avslutades i mars 2026. Inom projektet har också de rättsliga förutsättningarna analyserats och förslag på avtal och annan nödvändig dokumentation tagits fram.

[24] Exemplet beskrivs i artikeln från M. Christ, S. Radway & S. M. Bellovin, ”Differential Privacy and Swapping: Examining De-Identification’s Impact on Minority Representation and Privacy Preservation in the U.S. Census,” *2022 IEEE Symposium on Security and Privacy (SP)*, s. 457–472.
[25] Ju högre ε är, desto svagare är integritetsskyddet. Läs mer i avsnitt 3.5.1.
[26] https://www.census.gov/newsroom/press-releases/2021/2020-census-key-parameters.html (hämtad 2026-02-25) och Förenta nationerna (FN), 2023, United Nations *Guide on Privacy-Enhancing Technologies for Official Statistics (PET-Guide)*, s. 105.
[27] Läs mer på https://cros.ec.europa.eu/joconde (hämtad 2026-02-13).
[28] FN har beskrivit konceptet i UNECE Input Privacy Preservation Project, 2023, *Final report version 28*, s. 35 f.

5 Styrning och standarder för integritetsfrämjande teknik

5.1 Inledning

Styrningen av integritetsfrämjande teknik kan ske genom bindande författningsreglerade krav i nationell rätt eller EU-rätt eller genom icke-bindande styrning i form av exempelvis vägledningar, rekommendationer och riktlinjer. Styrningen kan också ske genom att myndigheter får regeringsuppdrag eller uppgifter i sin instruktion. Vidare kan styrningen ske genom olika typer av finansiering. Styrningen kan vara sektorsspecifik eller gälla generellt för offentlig förvaltning.

I detta kapitel redogör vi för befintlig styrning av integritetsfrämjande teknik, både vad gäller styrningen på EU-nivå (avsnitt 5.2) och på nationell nivå (avsnitt 5.3). Redogörelsen syftar till att ge en samlad bild av hur styrningen av integritetsfrämjande teknik ser ut, för att i sin tur kunna identifiera eventuella utvecklingsbehov när det gäller styrningen. Vi redovisar även vissa exempel på styrning av integritetsfrämjande teknik från andra länder, bland annat från våra nordiska grannländer (avsnitt 5.4). Detta för att ge en inblick i olika åtgärder som kan öka användningen av teknikerna.

Det finns även ett flertal standarder som rör integritetsfrämjande teknik. Standarder kan utgöra en form av icke-bindande styrning, om det inte finns ett uttryckligt krav i författning att de ska tillämpas. I kapitlet redogör vi därför även särskilt för de standarder som är relevanta för integritetsfrämjande teknik (avsnitt 5.5).

5.2 Styrningen på EU-nivå

Styrningen av integritetsfrämjande teknik på EU-nivå sker i huvudsak genom förordningar som avser dataskydd, dataförvaltning, AI och europeisk statistik. En EU-förordning är direkt tillämplig i varje medlemsstat, vilket innebär att de bestämmelser som finns i en EU-förordning ska tillämpas i Sverige som om de vore i en svensk lag.

Det har också på EU-nivå tagits fram vägledningar och riktlinjer som rör vissa integritetsfrämjande tekniker. Vidare har det i omgångar funnits möjlighet att ansöka om bidrag från EU:s finansieringsprogram för projekt som avser användningen av teknikerna.

5.2.1 Förordningsreglerad styrning

Inom EU regleras skyddet för den personliga integriteten i huvudsak genom dataskyddsförordningen[1] (se även avsnitt 2.4). Förordningen innehåller bestämmelser om pseudonymisering och kryptering men det finns inga uttryckliga bestämmelser om användning av integritetsfrämjande teknik som ett samlat begrepp eller om tillämpningen av fler sådana tekniker. Under senare år har emellertid kraven på användning av integritetsfrämjande teknik blivit ett allt vanligare inslag i EU. I flera rättsakter har såväl offentliga som privata aktörer ålagts att i vissa situationer tillämpa integritetsfrämjande teknik i syfte att stärka skyddet för den personliga integriteten. Nedan följer exempel på EU-förordningar som styr mot användning av integritetsfrämjande teknik.

Dataförvaltningsförordningen

Dataförvaltningsförordningen[2] är den första EU-förordningen som har sin grund i EU:s datastrategi[3]. I dataförvaltningsförordningen regleras bland annat vidareutnyttjande av vissa typer av skyddade data från offentliga myndigheter. Förordningen innebär inte en

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).
[3] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén, *En EU-strategi för data*, COM/2020/66 final.

skyldighet för myndigheter att tillgängliggöra skyddade data för vidareutnyttjande.[4] I förordningen finns dock villkor som behöver efterlevas om skyddade data ska tillgängliggöras för vidareutnyttjande. En grundförutsättning för att skyddade data ska få tillgängliggöras för vidareutnyttjande är att uppgifternas skyddade karaktär kan bevaras.[5] Det kan bland annat ske genom att personuppgifter anonymiseras eller att affärs- och företagshemligheter aggregeras.[6]

Förordningen föreskriver också att ett eller flera behöriga organ ska utses för att bland annat bistå myndigheter med tekniskt stöd vid tillgängliggörande av skyddade data för vidareutnyttjade. Stödet ska bland annat omfatta pseudonymisering, anonymisering, generalisering, undertryckande, randomisering och ”andra toppmoderna integritetsbevarande metoder”.[7] Med tekniskt stöd avses rådgivning och kunskapsöverföring, inte tillhandahållande av tekniska lösningar eller support. Statistiska centralbyrån (SCB) och Myndigheten för digital förvaltning (Digg) är utsedda till behöriga organ för att tillhandahålla tekniskt stöd. Digg har även en samordnande roll.[8]

Dataförvaltningsförordningen tillämpas sedan den 24 september 2023.[9] I Sverige har kompletterande bestämmelser till den del av förordningen som handlar om vidareutnyttjande av skyddade data förts in i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data.

Dataförordningen

Dataförordningen[10] syftar till att skapa ett enhetligt och rättvist regelverk inom EU för att underlätta och reglera tillgången till och användningen av data. Förordningen reglerar i huvudsak tillgången till data inom EU för fysiska och juridiska personer. Förordningen innehåller även bestämmelser som ger den offentliga sektorn möj-

[4] Artikel 1.2 i dataförvaltningsförordningen.
[5] Ds 2023:24, Genomförande av EU:s dataförvaltningsförordning, s. 74 och 78.
[6] Artikel 5.3 i dataförvaltningsförordningen.
[7] Artikel 7.4 c i dataförvaltningsförordningen.
[8] 2 § 11 p. förordningen (2016:822) med instruktion för Statistiska centralbyrån och 1 c § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[9] Artikel 38 i dataförvaltningsförordningen.
[10] Europaparlamentet och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen).

lighet att få tillgång till data från den privata sektorn vid hantering av krissituationer.

Om ett exceptionellt behov föreligger, exempelvis vid ett allmänt nödläge, kan ett offentligt organ, Europeiska kommissionen, Europeiska centralbanken eller ett unionsorgan som behöver en viss datamängd för att fullgöra en lagstadgad skyldighet av allmänt intresse, begära att juridiska personer tillgängliggör data. Om begäran avser data innehållande personuppgifter ska den som framställer begäran bland annat specificera vilka skyddsåtgärder som ska vidtas, exempelvis pseudonymisering, samt informera om datan kan anonymiseras innan den görs tillgänglig.[11]

Utredningen om kompletterande bestämmelser till EU:s dataförordning har föreslagit att Myndigheten för civilt försvar (MCF) ska ge stöd till offentliga organ i deras förberedelser för att vid behov begära, ta emot och använda data för att hantera allmänna nödlägen enligt förordningen. Det föreslagna uppdraget är tidsbegränsat till ett år, men i uppdraget ingår även att utreda om uppdraget bör bli permanent. MCF ska utföra sitt uppdrag i samråd med Integritetsskyddsmyndigheten (IMY) och Post- och telestyrelsen (PTS).[12]

Dataförordningen tillämpas sedan den 12 september 2025. Vissa krav i förordningen ska dock börja tillämpas senare.[13] Förslag till lag och förordning med kompletterande bestämmelser till EU:s dataförordning bereds för närvarande inom Regeringskansliet.

AI-förordningen

AI-förordningen[14] reglerar utvecklingen, tillhandahållandet och användningen av AI (se avsnitt 2.3.2). Förordningen innehåller särskilda regler för AI-system med hög risk. Leverantörer av sådana system får undantagsvis behandla särskilda kategorier av personuppgifter om det är absolut nödvändigt för att säkerställa upptäckt och korrigering av partiskhet (bias) som kan påverka människors

[11] Artikel 14–15 och 17.1 g i dataförordningen.
[12] SOU 2025:118 *Ökad och rättvis tillgång till data – kompletterande bestämmelser till EU:s dataförordning*, s. 213 f.
[13] Artikel 50 i dataförordningen.
[14] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

hälsa och säkerhet, inverka negativt på grundläggande rättigheter eller leda till diskriminering som är förbjuden enligt unionsrätten.[15]

Som huvudregel är behandling av känsliga personuppgifter förbjuden enligt dataskyddsförordningen, men de får behandlas under förutsättning att något av undantagen i artikel 9 i dataskyddsförordningen är tillämpligt. I AI-förordningen ställs ytterligare krav som också måste vara uppfyllda för att känsliga personuppgifter ska få behandlas. Ett krav är att det inte är tillräckligt att använda syntetiska eller anonymiserade data. Ett annat krav är att de känsliga personuppgifterna ska omfattas av säkerhetsåtgärder och integritetsbevarande åtgärder på en nivå som motsvarar den senaste utvecklingen, inbegripet pseudonymisering.[16]

Kraven som rör behandling av känsliga personuppgifter i AI-system med hög risk skulle börja tillämpas från och med den 2 augusti 2026.[17] Enligt en preliminär överenskommelse[18] mellan Europaparlamentet och rådet kommer tillämpningsdatumet skjutas fram till den 2 december 2027 för AI-system med hög risk inom vissa användningsområden[19] och till den 2 augusti 2028 för AI-system med hög risk som är säkerhetskomponenter inbyggda i produkter eller som i sig är produkter[20]. De förslag som Utredningen om AI-förordningen lämnat bereds för närvarande inom Regeringskansliet.[21]

[15] Artikel 6 och 10.5 i AI-förordningen.
[16] Artikel 10.5 a-b i AI-förordningen.
[17] Tidpunkten för tillämpning och innehållet i bestämmelserna om behandling av känsliga personuppgifter kan komma att påverkas av de förslag som kommissionen lämnat avseende förändringar i AI-förordningen. Se kommissionens förslag till Europaparlamentets och rådets förordning om ändring av förordningarna (EU) 2024/1689 och (EU) 2018/1139 vad gäller förenkling av genomförandet av de harmoniserade reglerna om artificiell intelligens (digital omnibusförordning om AI), COM/2025/836 final, artikel 1.
[18] https://www.consilium.europa.eu/sv/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/ (hämtad 2026-05-12).
[19] Se bilaga III till AI-förordningen.
[20] Se avsnitt A i bilaga I till AI-förordningen.
[21] Se SOU 2025:101 *Anpassningar till AI-förordningen*.

Förordningen om europeisk statistik

Förordningen om europeisk statistik[22] innehåller den rättsliga ramen för utveckling, framställning och spridning av europeisk statistik. Enligt artikel 1 är europeisk statistik relevant statistik som behövs för gemenskapens verksamhet och som följer subsidiaritetsprincipen och bestämmelserna om medlemsstaternas och gemenskapens myndigheters oberoende, integritet och ansvar.

Om en uppgiftsdelning enligt förordningen medför en personuppgiftsbehandling ska särskilda skyddsåtgärder tillämpas. Detta omfattar tekniska och organisatoriska åtgärder så som integritetsfrämjande teknik. De integritetsfrämjande tekniker som används när uppgifter delas ska vara utformade för att efterleva de grundläggande principerna om ändamålsbegränsning, uppgiftsminimering, lagringsbegränsning, integritet och konfidentialitet i dataskyddsförordningen.[23]

Förordningen om europeisk statistik om befolkning och bostäder

Förordningen om europeisk statistik om befolkning och bostäder[24] innehåller den rättsliga ramen för utveckling, framställning och spridning av europeisk statistik över befolkning och bostäder. Enligt förordningen får delning av konfidentiella uppgifter eller personuppgifter mellan olika statistikaktörer ske frivilligt under vissa förutsättningar. En av förutsättningarna är att uppgiftsdelningen sker med hjälp av integritetsfrämjande tekniker som säkerställer efterlevnad av de grundläggande principerna om dataskydd i dataskyddsförordningen.[25] Vidare ska EU:s officiella statistikmyndighet (Eurostat) och medlemsstaterna utföra pilotstudier för att bland annat

[22] Europaparlamentets och rådets förordning (EG) nr 223/2009 av den 11 mars 2009 om europeisk statistik och om upphävande av Europaparlamentets och rådets förordning (EG, Euratom) nr 1101/2008 om utlämnande av insynsskyddade statistiska uppgifter till Europeiska gemenskapernas statistikkontor, rådets förordning (EG) nr 322/97 om gemenskapsstatistik och rådets beslut 89/382/EEG, Euratom om inrättande av en kommitté för Europeiska gemenskapernas statistiska program.
[23] Skäl 22 i Europaparlamentets och rådets förordning (EU) 2024/3018 av den 27 november 2024 om ändring av förordning (EG) nr 223/2009 om europeisk statistik.
[24] Europaparlamentets och rådets förordning (EU) 2025/2458 av den 26 november 2025 om europeisk statistik om befolkning och bostäder, om ändring av förordning (EG)nr 862/2007 och om upphävande av förordningarna (EG) nr 763/2008 och (EU) nr 1260/2013.
[25] Artikel 12.3 i förordningen om europeisk statistik om befolkning och bostäder.

testa ändamålsenligheten hos relevant integritetsfrämjande teknik för datadelning.[26]

Förordningen trädde i kraft den 1 januari 2026 och ska tillämpas från och med den 1 januari 2028.

5.2.2 Vägledningar och riktlinjer

För vissa integritetsfrämjande tekniker har organ på EU-nivå tagit fram vägledningar och riktlinjer. Det gäller främst för de etablerade teknikerna och sällan för de moderna. Användning av pseudonymisering har behandlats i en riktlinje[27] från Europeiska dataskyddsstyrelsen (EDPB). Riktlinjerna avser att klargöra användningen och fördelarna med pseudonymisering för personuppgiftsansvariga och personuppgiftsbiträden. Pseudonymisering behandlas också i en rapport från Europeiska unionens cybersäkerhetsbyrå (Enisa).[28]

Vidare arbetar EDPB för närvarande med att ta fram en vägledning som bland annat omfattar anonymiseringstekniker. Inom ramen för förberedelserna inför det europeiska hälsodataområdet (EHDS) och tillgängliggörande av hälsodata för sekundäranvändning har det också tagits fram en vägledning för anonymisering, pseudonymisering och skapande av syntetiska data.[29]

5.2.3 Finansiering

Under några år har det inom EU:s ramprogram för forskning och innovation, Horisont Europa, tilldelats bidrag för projekt som utforskar utvecklingen och användningen av integritetsfrämjande teknik.

Europeiska kompetenscentret för cybersäkerhet (ECCC) utlyste under slutet av 2025 medel för projekt som på olika sätt och för olika syften utforskar utvecklingen av integritetsfrämjande teknik

[26] Artikel 12.5 och 13.1 g i förordningen om europeisk statistik om befolkning och bostäder.
[27] Europeiska dataskyddsstyrelsen (EDBP), *Guidelines 01/2025 on pseudonymisation, adopted version for public consultation*.
[28] Europeiska unionens cybersäkerhetsbyrå (Enisa), 2021, *Data pseudonymisation: Advanced techniques & use cases - Technical analysis of cybersecurity measures in data protection and privacy*.
[29] TEHDAS2 – Second Joint Action Towards the European Health Data Space, 2025, *M7.2 Draft guideline on data minimisation, pseudonymisation, anonymisation and synthetic data*.

med det övergripande syftet att öka cybersäkerheten.[30] Utlysningen omfattade totalt 11 miljoner euro. I mars 2026 inledde ECCC, inom ramen för arbetsprogrammet Civil säkerhet för samhället, en ny ansökningsomgång för finansiering av projekt som bland annat utforskar användningen av integritetsfrämjande teknik i olika sammanhang. Arbetsprogrammet omfattar totalt 56,2 miljoner euro.[31]

Det har även inom ramen för EU:s finansieringsprogram DIGITAL, Programmet för ett digitalt Europa, funnits finansieringsmöjligheter för projekt som berör användningen av integritetsfrämjande teknik, till exempel avseende datahantering inom hälso- och sjukvård.[32]

5.3 Styrningen på nationell nivå

Utredningen konstaterar att styrningen av integritetsfrämjande teknik på nationell nivå är relativt begränsad. Förutom de EU-förordningar som redogjorts för i avsnitt 5.2.1 saknas det uttryckliga bestämmelser om användningen av integritetsfrämjande teknik i nationell lagstiftning. Regeringen har inte heller styrt användningen av integritetfrämjande teknik, exempelvis genom regeringsuppdrag. En del myndigheter har dock inom ramen för sina nuvarande ansvarsområden tagit fram vägledningar som avser användningen av vissa av de etablerade integritetsfrämjande teknikerna.

5.3.1 Statliga myndigheters författningsreglerade uppgifter och regeringsuppdrag

Integritetsfrämjande teknik är relevant för vissa myndigheters nuvarande uppdrag och ansvarsområden. Det gäller främst Digg och IMY. Det finns också sektorspecifik styrning för hälsodata och genomförandet av EHDS-förordningen[33] som berör vissa integritetsfrämjande tekniker.

[30] https://cybersecurity-centre.europa.eu/funding-opportunities/calls-proposals/increased-cybersecurity-horizon-cl3-2025-02-cs-eccc_en (hämtad 2026-03-04).
[31] https://cybersecurity-centre.europa.eu/news/new-eccc-call-proposals-under-horizon-europe-programme-open-applications-2026-03-13 (hämtad 2026-04-15).
[32] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/DIGITAL-2026-AI-09-DS-HEALTH-TOOL (hämtad 2026-04-21).
[33] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.

Diggs uppdrag inom den förvaltningsgemensamma digitaliseringen

Digg har olika instruktionsenliga uppgifter och regeringsuppdrag som angränsar till integritetsfrämjande teknik. Det gäller till exempel inom ramen för den förvaltningsgemensamma digitaliseringen samt tillgängliggörandet och vidareutnyttjandet av data. Integritetsfrämjande teknik finns dock i dagsläget inte specifikt utpekat som en del av myndighetens uppgifter eller uppdrag.

Diggs övergripande uppgift är att samordna och stödja den förvaltningsgemensamma digitaliseringen, vilket inkluderar nästan samtliga statliga myndigheter[34] samt även kommuner och regioner.[35] I det ingår att ansvara för den förvaltningsgemensamma digitala infrastrukturen, kallad Ena.[36] Syftet med Ena är att underlätta för den offentliga förvaltningen att dela data och bygga digitala lösningar som fungerar bättre för invånare och företag. Ena består av olika digitala lösningar så som digitala system och tjänster, men även andra lösningar som möjliggör digitalisering. Det gäller till exempel standarder, ramverk och specifikationer.[37] Digg ansvarar för ledningen och samordningen av infrastrukturen, samt för merparten av de gemensamma lösningar som ingår i Ena. Exempel på befintliga lösningar som i dagsläget ingår i Ena är Digital post, Mina ombud, Sveriges dataportal, E-legitimering och Säker digital kommunikation (SDK).[38]

Digg ska också främja öppen och datadriven innovation samt tillgängliggörande och vidareutnyttjande av data från den offentliga förvaltningen.[39] Det innebär bland annat att Digg tillhandahåller vägledningar, metodstöd och rekommendationer, till exempel när det gäller att tillgängliggöra, dela och skydda data i offentlig sektor. Här finns bland annat vägledning som berör vissa integritetsfrämjande tekniker (se vidare i avsnitt 5.3.2). Digg har även haft regeringsuppdrag som har viss relevans för användningen av integritetsfrämjande teknik, till exempel när det gäller att föreslå en sam-

[34] Med undantag för Regeringskansliet, Säkerhetspolisen, Fortifikationsverket, Försvarshögskolan och myndigheter som hör till Försvarsdepartementet.
[35] 1 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[36] 1 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[37] Myndigheten för digital förvaltning (Digg), dnr 2024–4511, *Förslag till långsiktig utveckling och förvaltning av Ena,* s. 7 f.
[38] Digg, *Förslag till långsiktig utveckling och förvaltning av Ena* och bilagan *Lösningar i Ena.*
[39] 6 § 2 punkten (2018:1486) med instruktion för Myndigheten för digital förvaltning.

verkansstruktur för utveckling av tjänster för data och AI (se avsnitt 1.4.2).[40]

Regeringen har beslutat om en sammanslagning av Digg och PTS, vilket innebär att Diggs uppgifter överförs och inordnas i PTS från och med den 1 januari 2027.[41] Sammanslagningen syftar till att skapa bättre förutsättningar för att stärka arbetet med den digitala infrastrukturen samt att öka takten i digitaliseringen av den offentliga förvaltningen. Regeringen har aviserat att myndigheten kommer att heta Digitaliseringsmyndigheten.[42]

IMY:s uppdrag inom integritet och ny teknik

Även IMY har instruktionsenliga uppgifter som angränsar till integritetsfrämjande teknik, till exempel inom integritetsskydds- och dataskyddsområdet. IMY har i uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter. Myndigheten ska också följa, analysera och beskriva utvecklingen på it-området när det gäller frågor som rör integritet och ny teknik.[43] I den senaste redovisningen från 2025 lyfter IMY fram att Sverige bör främja integritetsvänlig teknikutveckling genom att satsa på utveckling av integritetsstärkande tekniker. IMY anser också att det bör finnas tydlig vägledning för att minska den regulatoriska osäkerheten.[44] Myndigheten har dock inget specifikt uppdrag som rör användningen av integritetsfrämjande teknik.

Förberedelser inför EHDS och sekundäranvändning av hälsodata

Införandet av EHDS och genomförandet av EHDS-förordningen medför styrning på nationell nivå som berör vissa integritetsfrämjande tekniker. Det gäller främst uppdrag till myndigheter som avser användningen av hälsodata för så kallad sekundäranvändning,

[40] Finansdepartementet, 2026, *Uppdrag till Myndigheten för digital förvaltning att föreslå en samverkansstruktur för utveckling av tjänster för data och artificiell intelligens.*
[41] Finansdepartementet, Fi2025/00654 Fi2025/02303, *Uppdrag till Post- och telestyrelsen att förbereda ett inordnande av Myndigheten för digital förvaltnings uppgifter* och Finansdepartementet, Fi2025/02297, *Uppdrag till Myndigheten för digital förvaltning att förbereda en överföring av uppgifter till Post- och telestyrelsen och avveckling av myndigheten.*
[42] https://regeringen.se/pressmeddelanden/2026/05/digg-och-pts-blir-digitaliseringsmyndigheten/ (hämtad 2026-05-19).
[43] 1 § förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten.
[44] Integritetsskyddsmyndigheten (IMY), IMY-2024-2570, *Integritet och ny teknik 2020–2024*, s. 3.

exempelvis för forskning, beslutsfattande och innovation. För att uppnå samhällsvinsterna med sekundäranvändningen betonas i skälen till EHDS-förordningen att de datamängder som tillgängliggörs behöver vara så fullständiga som möjligt. Pseudonymiserade och anonymiserade data är några av de skyddsåtgärder som förordningen nämner för att begränsa riskerna med detta.[45]

Enligt EHDS-förordningen ska medlemsstaterna ha utsett ett eller flera organ för tillgång till hälsodata (Health Data Access Body). Socialstyrelsen har fått i uppdrag att förbereda sig för att bli Sveriges organ för tillgång till hälsodata och lämnade i februari 2025 en delredovisning av uppdraget. Socialstyrelsen konstaterar bland annat att en betydande del av organets ansvar är att säkerställa att data hanteras med hög skyddsnivå och att integritetsrisker reduceras redan innan data tillgängliggörs för sekundäranvändning. För detta behövs bland annat rutiner för hur pseudonymisering och anonymisering ska utföras. Organet för tillgång till hälsodata ska bland annat kunna avgöra när hälsodata bör lämnas ut som aggregerad statistik, som anonymiserad data, eller i vilka fall pseudonymiserade uppgifter kan motiveras.[46] Socialstyrelsen ska senast den 15 juni 2026 lämna en slutredovisning av uppdraget.

Påtalade brister avseende styrningen av den förvaltningsgemensamma digitaliseringen

Flera utredningar har påtalat brister inom regeringens styrning av digitaliseringen av den offentliga förvaltningen. Styrningen beskrivs bland annat som alltför decentraliserad och inte tillräckligt samordnad, vilket bland annat har försvårat den förvaltningsgemensamma digitaliseringen. Det har bland annat resulterat i att Sverige har tappat i internationella jämförelser när det gäller digitaliseringen av offentlig sektor.[47]

Flera utredningar har lyft fram behovet av såväl tydligare uppgifter och uppdrag till statliga myndigheter inom den förvaltningsgemensamma digitaliseringen som en långsiktig finansiering för arbetet. Tydliga roller och ansvar anses särskilt relevant inom den

[45] Skäl 53 i EHDS-förordningen.
[46] Socialdepartementet, S2025/00977 (delvis), *Uppdrag till Socialstyrelsen att förbereda för att bli ansvarigt organ för tillgång till hälsodata enligt EHDS.*
[47] Se till exempel Myndigheten för digital förvaltning (Digg), dnr 2024-1332, *Ett samhälle i förändring – underlag till regeringens strategiska prioriteringar*, s. 25–35.

förvaltningsgemensamma digitaliseringen, eftersom ansvaret och genomförandet ofta behöver delas mellan flera myndigheter.[48] Det gäller till exempel Ena, där arbetet med infrastrukturen har försvårats efter att de ursprungliga regeringsuppdragen har avslutats.[49]

Statskontoret har också påtalat att enskilda myndigheter kan ha låga incitament för att utveckla förvaltningsgemensamma digitala lösningar, eftersom nyttorna ofta är indirekta. Det innebär att nyttorna ofta tillfaller den offentliga förvaltningen eller samhället som helhet, snarare än enskilda myndigheter.[50] Det ställer därför andra krav på finansieringen av förvaltningsgemensamma lösningar, till exempel behöver det finnas en tydlig och långsiktig finansiering.[51] Digg har bland annat lyft fram att det behövs en långsiktig finansieringslösning och förvaltningsmodell som tydligare definierar ansvarsfördelningen mellan regeringen, Digg och andra statliga myndigheter som tillhandahåller gemensamma lösningar inom Ena.[52]

5.3.2 Vägledningar

Det finns ett fåtal vägledningar på nationell nivå som avser integritetsfrämjande teknik och dessa berör främst etablerade avidentifieringstekniker. Pseudonymisering behandlas i en vägledning från samverkansprogrammet eSam.[53] Syftet med vägledningen är att lyfta fram olika scenarier där pseudonymisering är lämpligt att använda och att generellt beskriva de rättsliga förutsättningarna samt ge exempel på hur olika organisationer har etablerat lösningar för de olika scenarierna. SCB har en handbok i statistisk röjandekontroll som kan vara användbar vid avidentifiering i andra sammanhang än statistiska.[54]

Digg och SCB har, i egenskap av behöriga organ enligt dataförvaltningsförordningen, tagit fram information om anonymisering

[48] SOU 2025:96 *Flera möjligheter till ökat välstånd* och Digg, *Förslag till långsiktig utveckling och förvaltning av Ena.*
[49] Statskontoret, 2023:18, *Myndighetsanalys av Myndigheten för digital förvaltning.*
[50] Ekonomistyrningsverket, ESV 2020:23, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, Statskontoret, Dnr 2020/40-5, *Styrning av digitala investeringar*, Delrapport och SOU 2025:96.
[51] SOU 2025:96.
[52] Digg, *Förslag till långsiktig utveckling och förvaltning av Ena*.
[53] eSam, *Vägledning ES2022-01 Pseudonymisering av personuppgifter*.
[54] Rådet för den officiella statistiken, 2015, *Handbok i statisk röjandekontroll.*

och pseudonymisering som har publicerats i en vägledning om skyddade data.[55]

Regulatoriska sandlådor

IMY bedriver sedan 2022 en innovationssandlåda för dataskydd som ett arbetssätt för fördjupad vägledning i rättsligt oklara dataskyddsfrågor som rör ny teknik och innovation. I denna sandlåda kan olika integritetsfrämjande tekniker utforskas. Hittills har IMY publicerat tre rapporter som berör integritetsfrämjande teknik. De tekniker som utforskats är federerad inlärning[56], syntetiska data[57] och betrodda exekveringsmiljöer[58].

Integritetsfrämjande teknik kan även användas för att hantera utmaningar vid träning av AI-modeller. Regeringen har även i vårändringsbudgeten för 2026 aviserat att PTS ska få i uppdrag att inrätta en regulatorisk sandlåda för AI i enlighet med de krav som finns i AI-förordningen.[59] Den regulatoriska sandlådan för AI ska främja AI-innovation genom en kontrollerad experiment- och testmiljö vid utveckling av AI-system innan dessa system släpps ut på marknaden. I sandlådan ska tillsyn och vägledning ske för att säkerställa att de innovativa AI-systemen är förenliga med AI-förordningen och annan relevant EU-rätt och nationell rätt.

5.4 Exempel på styrning från andra länder

5.4.1 Integritetsfrämjande teknik i våra grannländer

Det finns flera exempel på olika typer av styrning av integritetsfrämjande teknik från andra länder. Vi har i avsnittet valt att fokusera på Norge, Finland och Danmark eftersom dessa länders förvaltningsmodeller har likheter med den svenska. Sverige har dock en mer decentraliserad förvaltningsmodell, med mer fristående stat-

[55] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/vagledning-om-skyddade-data (hämtad 2026-03-12).
[56] Integritetsskyddsmyndigheten, IMY-2023-2602, *Federerad maskininlärning mellan två vårdgivare*.
[57] Integritetsskyddsmyndigheten, IMY-2025-23536, *Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell.*
[58] Integritetsskyddsmyndigheten, IMY-2026-5444, *Betrodda exekveringsmiljöer för uppkopplade fordon*.
[59] Prop. 2025/26:99 *Vårändringsbudget för 2026,* utgiftsområde 22, s. 62. Se även SOU 2025:101.

liga myndigheter och ett mer långtgående kommunalt och regionalt självstyre.[60] Det gör att erfarenheterna från dessa länder inte alltid är direkt överförbara.

Norge

Användningen av integritetsfrämjande teknik omnämns inte i Norges digitaliseringsstrategi[61]. Däremot har Datatilsynet i Norge publicerat en vägledning om integritetsfrämjande teknik.[62] Vägledningen är till sin karaktär mer av information och ger inte stöd i juridiska eller tekniska frågor. Datatilsynet genomför också regulatoriska sandlådor där vissa integritetsfrämjande tekniker behandlats. Ett sådant sandlådeprojekt som genomförts avser federerad inlärning för att förbättra bankers förmåga att identifiera transaktioner som kan utgöra penningtvätt eller finansiering av terrorism (se närmare i avsnitt 4.4.2).[63] Ett annat sådant projekt avser elektronisk identifiering med biometri där uppgifterna skyddas med homomorf kryptering.[64]

I Norge finns det även en förvaltningsgemensam tjänst för testdata, Tenor testdatasök. Tjänsten tillhandahåller syntetiska testdata från flera myndigheter som kan användas vid systemutveckling och integrationstester mellan den privata och offentliga sektorn (se närmare i avsnitt 4.4.5).

Finland

I Finland saknas i dag nationell styrning och vägledning avseende användningen av integritetfrämjande teknik. Finland har dock en lag om sekundär användning av personuppgifter inom social- och hälsovården (2019/552). Enligt denna lag har Findata, som är tillståndsmyndighet för social- och hälsovårdsdata, befogenhet att på begäran samla in personuppgifter från olika aktör för att samman-

[60] Statskontoret, *Styrning av digitala investeringar*, s. 55 f.
[61] Norwegian Ministry of Digitalisation and Public Governance, *The Digital Norway of the Future National – Digitalisation Strategy 2024–2030.*
[62] https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/personvernfremmende-teknologi/ (hämtad 2026-03-10).
[63] Datatilsynet, 2022, *Maskinlæring uten datadeling: Bruk av føderert læring for antihvitvasking.*
[64] Datatilsynet, 2025, *Sikring av digitale identiteter - Biometriske opplysninger og beskyttede maler i eID løsninger*.

ställa anonymiserade data åt den som framställt begäran. Findata kan även säkerställa att data som andra aktörer har sammanställt är anonymiserad.[65] Vidare kan myndigheten genomföra verifiering av anonymitet i AI-modeller.[66] Bedömningen av om en AI-modell kan anses vara anonym grundas i huvudsak på den beskrivning som modellinnehavaren lämnat om modellen och dess egenskaper, den process som använts för att träna modellen samt egenskaperna hos de data som har använts vid träningen. Det innebär att Findata inte gör någon närmare granskning av hur AI-modellerna verkligen fungerar eller vilka resultat de ger.

Findata undersöker för närvarande möjligheterna att använda andra integritetfrämjande tekniker, främst differentiell integritet. Arbetet befinner sig dock ännu i ett utforskande skede och några slutsatser har ännu inte presenterats.

Danmark

I Danmark finns ingen nationell satsning på användning av integritetsfrämjande teknik vid datadelning inom den offentliga förvaltningen. Integritetsfrämjande teknik har dock lyfts fram i några sammanhang.

Den danska dataskyddsmyndigheten, Datatilsynet, har lyft fram integritetsfrämjande teknik som en del av dataskyddsförordningens krav på inbyggt dataskydd.[67] Dataskyddsmyndigheten har också en strategi för data- och riskbaserat arbete som indirekt stödjer användningen av integritetsfrämjande teknik i offentliga it-system. Strategin handlar bland annat om avancerad och mer målriktad användning av dataskyddsverktyg och tekniska säkerhetsåtgärder.[68]

Den danska digitaliseringsmyndigheten, Digitaliseringsstyrelsen, har en strategi[69] och vägledning för användningen av AI[70] som sätter fokus på säkert datautbyte, dataminimering och kontroll över åt-

[65] 2 kap. 5 § och 5 kap. 52 § lagen om sekundär användning av personuppgifter inom social- och hälsovården (2019/552).
[66] https://findata.fi/en/services-and-instructions/producing-anonymous-results/ (hämtad 2026-04-27).
[67] https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/databeskyttelse-gennem-design-og-standardindstillinger (hämtad 2026-05-07).
[68] Datatilsynet, 2024, *Tilsyn med effekt: Datatilsynets strategi for en data- og risikobaseret indsats, 2024–2026*.
[69] Digitaliseringsministeriet, 2025, *Den fællesoffentlige digitaliseringsstrategi 2026–2029.*
[70] https://digst.dk/kunstig-intelligens/guides-til-brug-af-kunstig-intelligens/guide-til-virksomheder/#accordion-persondatabeskyttelse (hämtad 2026-05-07).

komsten till känsliga data genom åtgärder som anonymisering, syntetiska data och åtkomstkontroll.

5.4.2 Styrning och specialreglering i övriga länder

I detta avsnitt lyfter vi fram några exempel från andra länder för att illustrera hur andra länder har främjat användningen av integritetsfrämjande teknik. Vissa av dessa länder har dock andra förvaltningsmodeller och lagstiftningstraditioner, vilket gör att erfarenheterna inte alltid går att tillämpa i Sverige.

Specialregleringar för teknikerna

Olika nivåer av anonymisering i tysk statistiklagstiftning

Den tyska statistiklagstiftningen innehåller tre olika varianter på anonymisering.[71] Enskilda uppgifter som är *absolut anonymiserade* omfattas inte av den sekretess som normalt gäller för officiella statistikuppgifter. Om de enskilda uppgifterna enbart ska användas för forskning räcker det att uppgifterna är *faktiskt anonymiserade*. Med det menas att det ska krävas en orimlig kostnad, tidsåtgång och arbetsinsats för att koppla ihop uppgifterna med en enskild person. Inom särskilt avgränsade delar av statistikmyndigheterna får också *formellt anonymiserade* uppgifter användas för forskning, under förutsättning att det finns effektiva säkerhetsåtgärder för att skydda sekretessen. Uppgifter är formellt anonymiserade när direkt identifierande uppgifter, så som namn, har tagits bort från datamängden.[72] För uppgifter som är faktiskt eller formellt anonymiserade gäller också särskilda bestämmelser avseende tystnadsplikt, ändamålsbegräsning och radering.

[71] § 16 Gesetz über die Statistik für Bundeszwecke (BStatG).
[72] https://www.forschungsdatenzentrum.de/en/anonymity (hämtad 2026-04-22).

Anonymiserad och syntetiska data i delstaten Utah

I delstaten Utah i USA finns en lag som utgör en policy om artificiell intelligens. I lagen definieras begreppet avidentifierade data. Med avidentifierade data avses där information som inte rimligen kan hänföras till en identifierad eller identifierbar individ. Den som behandlar sådan data ska vidta rimliga åtgärder för att förhindra att uppgifterna kan hänföras till en individ, åta sig att endast använda och underhålla datan i avidentifierad form utan att försöka återidentifiera individer samt säkerställa att mottagare av datan kontraktsmässigt förbinder sig att följa samma krav. Lagen fastslår även att syntetiska data omfattas av definitionen av avidentifierade data. Med syntetiska data avses data som genererats med hjälp av datoralgoritmer eller statistiska modeller och som inte innehåller personuppgifter.[73]

Styrning av myndigheters användning av teknikerna

I oktober 2023 utfärdade USA:s president en exekutiv order om säker, trygg och pålitlig utveckling och användning av artificiell intelligens. Där framgår det att federala myndigheter ska använda tillgängliga policyer och tekniska lösningar för att skydda individers integritet vid användning av AI. Detta omfattar även integritetsfrämjande teknik.[74] En exekutiv order från presidenten kan betraktas som bindande direktiv till federala myndigheter.

Nationella riktlinjer, vägledningar och strategier

Dataskyddsmyndigheten (Information Commissioner's Office) i Storbritannien har publicerat en vägledning om integritetsfrämjande teknik som även innehåller illustrativa användarfall.[75] Mer detaljerad vägledning om teknikerna ges av landets expertmyndigheter, så som det nationella cybersäkerhetscentret (National Cyber Security Center) som ger råd om integritetsfrämjande tekniker som bygger

[73] Utah Artificial Intelligence Amendents, S.B. 149, 2024.
[74] Executive Order 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Section 1f.
[75] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/ (hämtad 2026-04-15).

på kryptografi sedan april 2025.[76] Dessa råd pekar ännu inte på standarder, vilket är ett vanligt nästa steg för cybersäkerhetscentret.[77] Centret arbetar även med att påverka internationell standardisering.[78] Storbritanniens statistikmyndighet (Office for National Statistics) publicerar precis som SCB vägledning om statistisk röjandekontroll.[79] De har identifierat differentiell integritet som en central ny teknik att inkludera i kommande vägledningar.[80]

Även Israels dataskyddsmyndighet (the Privacy Protection Authority) har en vägledning om teknikerna.[81]

Det amerikanska nationella vetenskaps- och teknikrådet (The National Science and Technology Council) publicerade 2023 en nationell strategi för att främja integritetskyddad datadelning och dataanalys som bland annat behandlar användningen av integritetsfrämjande teknik. Strategin anger fem prioriterade områden för såväl offentlig som privat sektor i syfte att utveckla ett framtida ”ekosystem för data”. Dessa områden avser styrning och ansvarsfull användning, forskning, kompetensuppbyggnad, internationellt samarbete samt åtgärder för att påskynda överföringen från forskning till praktisk tillämpning.[82]

Singapores dataskyddsmyndighet (Personal Data Protection Commission) presenterade i juli 2024 ett förslag till vägledning om användning av syntetiska data. Vägledningen omfattar bland annat olika tekniker för generering av syntetiska data, användarfall samt risker för återidentifiering och metoder för att utvärdera dessa risker.[83]

[76] https://www.ncsc.gov.uk/whitepaper/advanced-cryptography (hämtad 2026-02-27).
[77] https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography#section_3 (hämtad 2026-02-27).
[78] https://www.ncsc.gov.uk/blog-post/new-standard-for-post-quantum-terminology (hämtad 2026-02-27).
[79] https://www.ons.gov.uk/methodology/methodologytopicsandstatisticalconcepts/disclosurecontrol (hämtad 2026-03-19).
[80] Office for National Statistics, 2021, *Applying differential privacy protection to ONS mortality data, pilot study*.
[81] The Privacy Protection Authority, 2025, *Guide to Privacy Enhancing Technologies*.
[82] The National Science and Technology Council, 2023, *National strategy to advance privacy-preserving data sharing and analytics*.
[83] Personal Data Protection Commission Singapore (PDPC), 2024, *Privacy Enhancing Technology (PET): Proposed guide on synthetic data generation*.

Regulatoriska sandlådor

Singapores digitaliseringsmyndighet (Infocomm Media Development Authority) har genomfört ett sandlådeprojekt om homomorf kryptering tillsammans med Mastercard (se närmare avsnitt 4.4.2). Myndigheten har även genomfört ett sandlådeprojekt om generering av syntetiska data för analys av hur en fastighet används och rörelsemönster hos de personer som bor i eller besöker fastigheten i syfte att förbättra tjänsterna för boende i fastigheten.[84]

Innovationstävlingar

Storbritannien och USA anordnade under 2023 en gemensam innovationstävling med fokus på integritetsfrämjande teknik. Tävlingen syftade till att främja innovation och metodutveckling. Det inkluderade att ta fram lösningar som är motståndskraftiga mot angrepp genom att kombinera olika tekniker samt att utveckla maskininlärningsmodeller med hög samhällsnytta inom två prioriterade områden: förebyggande av ekonomisk brottslighet och förbättrade prognoser för att stärka beredskapen vid pandemier. Tävlingen omfattade både deltagare som utvecklade lösningar och deltagare som hade i uppgift att testa lösningarnas motståndskraft genom att försöka avslöja den data som använts för att träna modellerna.[85]

5.5 Standarder

En standard utgör en gemensamt framtagen och överenskommen lösning på ett återkommande problem. Syftet är att etablera enhetliga och tydliga arbetssätt som kan bidra till att höja kvaliteten, minska risken för missförstånd och skapa bättre förutsättningar för samverkan mellan olika aktörer.[86]

Standarder spelar en betydande roll i arbetet med att säkerställa säkerhet, kvalitet och effektivitet inom olika samhällssektorer. Genom att fastställa gemensamma riktlinjer skapas förutsättningar för interoperabilitet mellan system och produkter, vilket underlättar både

[84] Infocomm Media Development Authority, *Preventing financial fraud across different jurisdictions with secure collaborations IMDA PET sandbox – Mastercard case study*.
[85] https://petsprizechallenges.com/ (hämtad 2026-04-16).
[86] https://www.sis.se/standarder/vad-ar-en-standard/ (hämtad 2026-03-12).

användning och samordning. Vidare medverkar standarder till ökad tillförlitlighet och kan leda till kostnadsbesparingar genom att effektivisera produktion, utveckling och förvaltning av tjänster och tekniska lösningar. Standarder har även betydelse för utvecklingen och användningen av integritetsfrämjande teknik. Standarder kan bidra till att sådana tekniker utformas och implementeras på ett tillförlitligt sätt. Detta underlättar samverkan och informationsutbyte utan att integritetsskyddet äventyras.

I regeringens strategi för standardisering från 2019 betonas att användningen av standarder både driver och är en förutsättning för ökad digitalisering och teknikutveckling.[87] Där framhålls även vikten av att utveckla återanvändbara lösningar på europeisk nivå och att digitala tjänster i så stor utsträckning som möjligt ska bygga på öppna standarder. Regeringens utrikeshandelsstrategi från 2023 betonar också att internationell, regelbaserad handel och globalt accepterade standarder gynnar Sverige och svenska företag.[88] Ett av de 78 delmålen i strategin är att Sverige ska få genomslag för sina prioriteringar i utvecklingen av framtidens gröna och digitala standarder.[89]

5.5.1 Standardiseringsorganisationer

Standardisering som rör användningen av integritetsfrämjande teknik bedrivs inom flera olika organisationer, som arbetar på skilda sätt och med varierande finansieringsmodeller. Nedan redovisas de standardiseringsorganisationer som har en central betydelse för utvecklingen av tekniska standarder som rör integritetsfrämjande teknik. Vidare redovisas en översiktlig beskrivning av deras respektive arbetssätt för att ge en förståelse för hur standarderna utvecklas och beslutas.

[87] Regeringens strategi för standardisering, 2019, s. 28.
[88] Regeringens strategi för Sveriges utrikeshandel, investeringar och globala konkurrenskraft, UD2023/01758, s. 13.
[89] Regeringens strategi för Sveriges utrikeshandel, investeringar och globala konkurrenskraft, s. 16.

SIS

Svenska institutet för standarder (SIS) är Sveriges nationella standardiseringsorgan och deltar i de internationella samarbetena inom Internationella standardiseringsorganisationen och Europeiska kommitteen för standardisering. Organisationen samverkar med aktörer från industri, akademi, offentlig sektor och civilsamhälle för att utveckla standarder inom olika områden. SIS projektleder det svenska standardiseringsarbetet och arbetar för att standarder ska spridas samt tillämpas.[90]

SIS finansierar sin verksamhet genom försäljning av standarder, medlemsavgifter och statliga anslag. Det statliga anslaget för budgetåret 2026 uppgår till 33 miljoner kronor, varav 3,3 miljoner kronor är avsatt för digitalisering och cybersäkerhet.[91] Försäljningen av standarder görs både separat och som prenumeration.[92] Vissa standarder görs även tillgängliga utan kostnad genom särskilda avtal mellan SIS och olika myndigheter eller organisationer. Sådana förköpta standarder kan laddas ner eller läsas online av företag och i vissa fall privatpersoner verksamma i Sverige.

CEN

Europeiska kommitteen för standardisering (CEN) är en europeisk standardiseringsorganisation vars medlemmar utgörs av nationella standardiseringsorgan från samtliga EU-länder samt ytterligare ett antal europeiska länder. Organisationens uppdrag är att utveckla och anta europeiska standarder i syfte att stödja den inre marknaden, undanröja handelshinder och främja säkerhet, interoperabilitet och konsumentskydd. CEN är officiellt erkänt av EU som ett av de europeiska standardiseringsorganen.[93] CEN finansieras genom medlemsavgifter, försäljning av standarder och EU-bidrag.

[90] https://www.sis.se/om-sis/ (hämtad 2026-03-12).
[91] Regeringsbeslut II:23, 2025-12-18, *Riktlinjer för budgetåret 2026 avseende avseende Svenska instituet för standarder (SIS), Standardiseringens Konsument- och Arbetstagarråd (SKA-rådet), Svensk Elstandard (SEK) och Svenska Informations- och Telekommunikationsstandardiseringen (ITS)*.
[92] https://www.sis.se/standarder/kpenstandard/ (hämtad 2026-03-12).
[93] https://www.cencenelec.eu/european-standardization/ (hämtad 2026-03-12).

ISO

Internationella standardiseringsorganisationen (ISO) är en global standardiseringsorganisation bestående av 175 nationella standardiseringsorgan, där det svenska SIS är en av medlemmarna. ISO utvecklar internationella standarder inom ett stort antal områden och samarbetar nära med europeiska CEN genom det så kallade Wienavtalet för att undvika dubbelarbete och möjliggöra gemensamma standarder.[94]

De flesta tekniska standarder inom cybersäkerhet och integritetsfrämjande tekniker som antagits av ISO (och sedan av CEN/SIS) bygger på kodifiering av redan etablerade standarder från mer specialiserade standardiseringsorgan, så som IETF och NIST.

ETSI

European Telecommunications Standards Institute (ETSI) är ett europeiskt standardiseringsorgan som arbetar med att utveckla globalt tillämpbara standarder för informations- och kommunikationsteknik. ETSI är också officiellt erkänt av EU som ett av de europeiska standardiseringsorganen.[95] Det nationella standardiseringsorganet som representerar Sverige i ETSI är Svenska Informations- och Telekommunikationsstandardiseringen (ITS). De erhåller för budgetåret 2026 totalt 2,5 miljoner kronor i statligt anslag för uppgiften.[96] ETSI finansieras bland annat av medlemsavgifter från organisationerna som deltar och EU-bidrag.[97]

IETF

Internet Engineering Task Force (IETF) är ett globalt standardiseringsorgan som utvecklar öppna standarder genom transparanta processer med målet att få internet att fungera bättre. Finansieringen bygger främst på registreringsavgifter för fysiska möten som hålls tre gånger per år.[98] Till skillnad från traditionella standardiserings-

[94] https://interoperable-europe.ec.europa.eu/collection/european-committee-standardization-cen (hämtad 2026-03-12).
[95] https://www.cencenelec.eu/european-standardization/ (hämtad 2026-03-12).
[96] Regeringsbeslut, *Riktlinjer för budgetåret 2026 avseende SIS, SKA-rådet, SEK och ITS*.
[97] https://www.etsi.org/about (hämtad 2026-03-12).
[98] https://www.ietf.org/about/introduction/ (hämtad 2026-03-12).

organ består IETF av individuella deltagare snarare än representanter för länder eller organisationer. De flesta svenska deltagare kommer dock från organisationer som exempelvis Ericsson, Internetstiftelsen, forskningsinstitutet RISE (Research Institutes of Sweden) och Försvarets radioanstalt (FRA).[99]

NIST

The National Institute of Standards and Technology (NIST) är en del av USA:s handelsdepartementet. NIST arbetar bland annat med att utveckla standarder och teknik som stödjer innovation.[100] NIST bedriver också forskning inom en rad områden, bland annat avancerad tillverkning, cybersäkerhet, kvantteknik, nästa generations kommunikation och energiteknik.[101]

NIST spelar en central och strategisk roll i USA:s strategi för standarder genom att fungera som statens nav i ett system för framtagande av standarder, som i grunden leds av privat sektor. Den amerikanska modellen skiljer sig från många andra länder genom att staten möjliggör, samordnar och stärker företagens och marknadens arbete. Detta skapar förtroende och incitament för företag att aktivt delta i standardutveckling, ofta genom samarbete mellan offentlig sektor och privat sektor. På så sätt bidrar NIST till att stärka USA:s innovationsförmåga, konkurrenskraft och inflytande över globala standarder, samtidigt som den marknadsdrivna standardmodellen upprätthålls.

Ett sätt som NIST arbetar på för att ta fram nya standarder är genom att arrangera tävlingar. Genom tävlingarna identifieras och utvärderas lösningar innan de fastställs som standarder.[102] Även europeiska forskare deltar ofta i sådana tävlingar.[103]

NIST har också föreslagits som ansvarig för att hålla det register för differentiell integritet (se avsnitt 3.5.1) som OpenDP har skapat.[104]

[99] https://datatracker.ietf.org/meeting/124/proceedings/attendees/ (hämtad 2026-03-12).
[100] https://www.nist.gov/about-nist (hämtad 2026-03-12).
[101] https://www.nist.gov/topics (hämtad 2026-03-12).
[102] https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges (hämtad 2026-03-13).
[103] https://www.inria.fr/en/inria-au-nist (hämtad 2026-04-27).
[104] https://opendp.org/2025/11/25/launching-the-differential-privacy-deployments-registry/ (hämtad 2026-03-16).

5.5.2 Tekniska standarder för integritetsfrämjande teknik

Standardiseringsarbetet som rör integritetsfrämjande teknik utvecklas snabbt och är i viss mån svåröverskådligt. Detta medför att det kan vara svårt att skapa sig en samlad bild av vilka standarder som är relevanta och ändamålsenliga att tillämpa i olika sammanhang.

Ett område som ligger nära integritetsfrämjande teknik men som är mer moget och under snabb utveckling är kryptering av elektronisk kommunikation. Det området ger en rimlig bild av hur lämpliga tekniska standarder för integritetsfrämjande teknik kan identifieras framöver. Tekniska standarder på det området certifieras inom EU enligt Common Criteria[105]. Europeiska cybersäkerhetsbyrån (Enisa) har en grupp för cybersäkerhetscertifiering som har tagit fram en lista på lämpliga standardiserade kryptografiska mekanismer.[106] Enisa hänvisar där till 9 standarder och 13 rekommendationer från NIST, 11 standarder från ISO och 11 standarder från IETF. Endast enstaka hänvisningar förekommer till andra standardiseringsorganisationer, så som till exempel ETSI. För kvantsäkra algoritmer rekommenderar Nationella cybersäkerhetscentret (NCSC) vid Försvarets radioanstalt (FRA) att endast standardiserade algoritmer som används internationellt av företag och myndigheter i omfattande skala ska användas.[107] De ger fem exempel på sådana algoritmer, alla standardiserade av NIST.

För närvarande har ingen svensk myndighet fastställt kriterier för vilka standarder som bör tillämpas inom området för integritetsfrämjande teknik. Det har inte heller lämnats några uttryckliga rekommendationer i detta avseende. En ändamålsenlig ordning framöver kan vara att tydliga kriterier formuleras även för integritetsfrämjande teknik och att exempel på standarder som uppfyller dessa kriterier identifieras, på motsvarande sätt som har skett inom området kvantdatorsäkra algoritmer för elektronisk kommunikation.

[105] Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC).
[106] Europeiska unionens cybersäkerhetsbyrå (Enisa), European Cybersecurity Certification Group Sub-group on Cryptography, 2025, *Agreed Cryptographic Mechanisms*, version 2.0.
[107] Nationellt cybersäkerhetscenter vid FRA, 2026, *Nationella rekommendationer för övergången till kvantsäker kryptografi*, s. 10 f.

Detta bör dock ske i takt med att integritetsfrämjande teknik utvecklas och får ökad tillämpning.

Även om det inte finns några rekommendationer om vilka standarder som ska användas så finns det en del tekniska standarder för integritetsfrämjande tekniker framtagna. Nedan nämns några av de standarder som är mest intressanta vid användning av integritetsfrämjande teknik. Det är enbart exempel och utgör inte rekommendationer.

Avidentifieringstekniker

ISO har tagit fram en internationell standard för avidentifiering av data där det framgår vad som ska beaktas under en avidentifieringsprocess.[108] Det finns även en svensk standard om pseudonymisering inom hälso- och sjukvårdsinformatik. Standarden definierar bland annat en grundläggande metod för pseudonymisering ur både tekniskt och organisatoriskt perspektiv samt ger vägledning om riskbedömning gällande återidentifiering.[109]

Differentiell integritet

NIST har publicerat en handledning för utvärdering av mjukvarulösningar som tillämpar differentiell integritet.[110] Handledningen beskriver tekniken och de matematiska grunderna för den så kallade integritetsbudgeten (privacy budget) samt ger vägledning om hur vanliga praktiska problem kan identifieras och åtgärdas. Den anger dock inget fast värde för vilken nivå av integritetsförlust (epsilon, ε) som kan accepteras, men NIST har öppnat för att sådana standarder kan komma tas fram.

[108] ISO/IEC 27559:2022 *Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework*.
[109] ISO 25237:2017 *Hälso- och sjukvårdsinformatik – Pseudonymisering*.
[110] National Institute of Standards and Technology, *NIST SP800-226 Guidelines for Evaluating Differential Privacy Guarantees*.

Betrodda exekveringsmiljöer

En betrodd exekveringsmiljö baseras på hårdvarans egenskaper. Det är svårt att utforma standarder för hårdvara som är tillräckligt detaljerade för att vara praktiskt användbara samtidigt som de är tillräckligt generella för att omfatta flera plattformar. Det är däremot enklare att standardisera hur användaren kommunicerar med miljön för att säkerställa dess integritet. Användaren måste kunna verifiera att miljön inte har kompromitterats, vilket kan ske genom utfärdande av intyg på distans (remote attestation). Standardisering av sådana processer sker främst inom en arbetsgrupp hos IETF.[111]

NIST har publicerat en rapport om säkerhet genom hårdvara i användarfall för bland annat databehandling i moln, vilket inkluderar betrodda exekveringsmiljöer.[112] NIST har även tagit fram en säkerhetsvägledning för virtuell hybridmolnsinfrastruktur som tjänst, vilken är relevant för dessa exekveringsmiljöer.[113]

ETSI har publicerat en rapport om betrodda exekveringsmiljöer med fokus på användarfall inom artificiell intelligens.[114]

GlobalPlatform är ett branschkonsortium som standardiserar teknik för betrodda exekveringsmiljöer. Dess standarder och specifikationer omfattar arkitektur, säkerhet och API:er. De mest grundläggande är TEE System Architecture som behandlar säkerhet och funktionalitet samt TEE Internal Core API som reglerar kommunikationen mellan icke-betrodda och betrodda program i en betrodd exekveringsmiljö.

Institute of Electrical and Electronics Engineers (IEEE) har en standard med tekniska krav för en allmän säker datorplattform. Den omfattar områden som isolering, konfidentialitet, kompatibilitet, prestanda, användbarhet och säkerhet.[115]

[111] https://datatracker.ietf.org/wg/rats/about/ (hämtad 2026-04-21).
[112] National Institute of Standards and Technology, *NIST IR 8320 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*.
[113] National Institute of Standards and Technology, *NIST SP 1800-19 Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments*.
[114] European Telecommunications Standards Institute (ETSI), *GR SAI 006 Securing Artificial Intelligence (SAI); The role of hardware in security of AI*.
[115] IEEE 2952-2023, *IEEE Standard for Secure Computing Based on Trusted Execution Environment*.

Säker flerpartsberäkning

ISO har publicerat två internationella standarder om säker flerpartsberäkning. Den första är generell och innehåller definitioner, terminologi och processer för säker flerpartsberäkning och relaterad teknik. Syftet med standarden är att fastställa en taxonomi och möjliggöra interoperabilitet.[116] Den andra standarden avser säker flerpartsbehandling av konfidentiella data.[117]

Homomorf kryptering

Det pågår för närvarandet ett arbete med att ta fram standardisering av fullständig homomorf kryptering inom standarden ISO/IEC 28033. Det förväntas vara klart i slutet av 2026.[118]

Nollkunskapsbevis

De kommande digitala identitetsplånböckerna inom EU driver på standardiseringen av kvantsäkra nollkunskapsbevis.[119] På IETF studeras även nollkunskapsschemat Longfellow[120] som delvis finansieras av den svenska stiftelsen Siros.[121]

Fortsatt arbete med att ta fram standarder

Nya standarder för integritetsfrämjande teknik tas fram löpande, exempelvis har NIST ett större projekt med federala myndigheter i USA.[122] På deras senaste konferens i januari 2026 presenterades 26 förslag till nya standarder av forskare från hela världen och mer

[116] ISO/IEC 4922-1:2023 *Information security – Secure multiparty computation – Part 1: General*.
[117] ISO/IEC 4922-2:2024 *Information security – Secure multiparty computation – Part 2: Mechanisms based on secret sharing*.
[118] Se översikten av detta standardiseringsarbete på https://www.linkedin.com/pulse/fhe-standardization-enterprise-guide-iso-nist-desilo-lcbdc (hämtad 2026-03-19).
[119] https://datatracker.ietf.org/meeting/125/materials/slides-125-cfrg-longfellow-zk-00 (hämtad 2026-03-19).
[120] https://eprint.iacr.org/2024/2010 (hämtad 2026-03-19).
[121] https://siros.org/blog/zero-knowledge-proofs-selective-disclosure-and-the-future-of-scalable-wallets (hämtad 2026-03-19).
[122] https://csrc.nist.gov/projects/threshold-cryptography (hämtad 2026-02-27) och https://csrc.nist.gov/projects/pec (hämtad 2026-02-27).

än 600 personer från 60 länder deltog.[123] Förslagen till nya standarder handlar alla om hur data kan delas upp och samlas ihop mellan olika parter på ett integritetsfrämjande sätt. Det är förslag på standarder för säker flerpartsberäkning, homomorf kryptering och nollkunskapsbevis samt enklare kryptografiska komponenter som kan sättas ihop för nya typer av integritetsfrämjande tekniker som bygger på kryptografi. Därutöver behandlades ett flertal generella standarder för informationssäkerhet och teknik.

5.5.3 Standarder för ledningssystem

Ett ledningssystem används för att systematiskt planera, leda och kontrollera en verksamhets kvalitet.[124] Det är vanligt att föreskrifter om ledningssystem hänvisar till standarder. Ett exempel är Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Av 3 kap. 1 § i föreskrifterna framgår att vårdgivare genom ledningssystemet ska säkerställa tillgänglighet, riktighet, konfidentialitet och spårbarhet. I det allmänna rådet till 3 kap. 1 § hänvisas till standarder i ISO/IEC 27000-serien. Myndigheten för civilt försvar har även en liknande hänvisning till standarder i ISO/IEC 27000-serien i förslaget till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt cybersäkerhetslagen (2025:1506).[125]

ISO/IEC 27000-serien, som avser ledningssystem för informationssäkerhet, omfattade ursprungligen inte personuppgifter och integritetsskydd. Dessa aspekter tillkom senare som en följd av införandet av dataskyddsförordningen. Anpassning av internationella standarder till nationell lagstiftning är ofta kontroversiellt på grund av att det kan finnas motstridiga politiska intressen.[126] Eftersom olika länder har olika rättsliga och tekniska förutsättningar utformas standarderna i regel som kompromisser och de behöver

[123] https://csrc.nist.gov/pubs/ir/8214/c/final (hämtad 2026-02-27).
[124] https://www.socialstyrelsen.se/kunskapsstod-och-regler/regler-och-riktlinjer/Ledningssystem/ (hämtad 2026-02-27).
[125] Förslag till Myndigheten för civilt försvars föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning, dnr MCF 2026-04554.
[126] T. Rühlig, ”China, Europe and the New Power Competition over Technical Standards”, *Utrikespolitiska institutet brief 1/2021*, S. Hoffmann, D. Lazanski, & E. Taylor, 2020, ”Standardising the splinternet: how China’s technical standards could fragment the internet”, *Journal of Cyber Policy*, 5(2), A. Mueller & C. S. Yoo, ”Crouching Tiger, Hidden Agenda?: The Emergence of China in the Global Internet Standard-Setting Arena”, *Federal Communications Law Journal*, Vol. 76 Issue 2.

vara generella för att passa i många länder. Ett exempel på ett sådant område är informationssäkerhet och integritetshantering som över tid delvis utvecklats i olika riktningar inom serien.[127] För att motverka detta problem finns det sedan hösten 2025 ett separat ledningssystem för integritetsinformation[128] i ISO/IEC 27701:2025. Standarden är antagen som svensk standard men har ännu inte översatts.[129] Standarden innehåller bland annat krav på klassificering av information med hänsyn till personuppgifter, baserat på konfidentialitet, integritet, tillgänglighet och relevanta intressentkrav. Detta ligger nära vad som anges i exempelvis Socialstyrelsens föreskrifter.

Integritetsfrämjande teknik ingår naturligt i implementeringen av ledningssystem för integritetsinformation. Vägen från ledningssystemet via metodbeskrivningar till tekniska och matematiska standarder är dock lång, eftersom den går från strategisk ledning till operativ verksamhet via juridik och policyer. En implementering som inte når den operativa nivån uppfyller inte sitt syfte.[130]

ISO/IEC 27701:2025 syftar bland annat till att uppfylla principerna om inbyggt dataskydd och dataskydd som standard. För detta krävs bland annat att organisationen definierar och dokumenterar mål för dataminimering samt vilka mekanismer (exempelvis avidentifiering) som används för att uppnå dessa. Som stöd för att definiera och dokumentera mål för dataminimering och mekanismer kan exempelvis standarden ISO/IEC 20889:2018 om terminologi och klassificering av tekniker för integritetsfrämjande avidentifiering användas. Den ger en översiktlig beskrivning av hur homomorf kryptering kan tillämpas och hänvisar vidare till ISO/IEC 18033-6:2019, som matematiskt beskriver metoder för homomorf kryptering.

För att underlätta tillsyn och revision kan verksamheter certifieras mot etablerade standarder. Certifiering mot standarder i ISO/IEC 27000-serien är ett sätt att påvisa ett systematiskt informationssäkerhetsarbete.

---

[127] M. Suora & P. Helo, 2024, "Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis", *Information Security Journal: A Global Perspective*, Volume 33.
[128] PIMS – Privacy Information Management System. Ordet "integritetsinformation" har valts av SIS i deras översättning av titeln till den engelskspråkiga ISO-standarden.
[129] SS-EN ISO/IEC 27701:2025 *Informationssäkerhet, cybersäkerhet och integritetsskydd – System för hantering av integritetsinformation – Krav och vägledning*.
[130] Inom det närliggande cybersäkerhetsområdet har denna problematik hanterats inom EU genom lagstiftning i stället för med standarder. I 2 kap 3 § cybersäkerhetslagen (2025:1506) pekas det ut säkerhetsåtgärder som ska vidtas.

5.5.4 Kostnadsfri tillgång till standarder

Standarder köps normalt från de olika standardiseringsorganisationerna. I vissa fall måste dock tillgången till standarderna vara kostnadsfri.

EU-domstolen har i flera domar slagit fast att harmoniserade standarder som EU-rättsakter hänvisar till ska anses utgöra en del av unionsrätten på grund av de rättsverkningar de medför.[131] Detta eftersom en harmoniserad standard närmare kan beskriva vilka rättigheter och skyldigheter som enskilda har. Tillgången till sådana standarder är således nödvändig för att kunna kontrollera om en viss vara eller tjänst uppfyller kraven. Sådana harmoniserade standarder ska därför, på samma sätt som för övrig unionsrätt, vara fritt tillgängliga för allmänheten utan kostnad.

Enligt ett ställningstagande från Konkurrensverket 2024 utgör hänvisningar till standarder en del av upphandlingsunderlaget och dessa standarder måste finnas att tillgå kostnadsfritt enligt kravet på kostnadsfri tillgång till upphandlingsdokumenten enligt 10 kap. 7 § lagen (2016:1145) om offentlig upphandling.[132]

[131] Se domstolens dom av den 21 april 2026, Nederlandse Voedsel- en Warenautoriteit m.fl. mot Stichting Rookpreventie Jeugd, C-155/24, EU:C:2026:327, domstolens dom av den 9 november 2023, Global Silicones Council m.fl. mot Europeiska kommissionen, C-558/21 P, EU:C:2023:839 och domstolens dom av den 22 februari 2022, Stichting Rookpreventie Jeugd m.fl. mot Staatssecretaris van Volksgezondheid, Welzijn en Sport, C-160/20, EU:C:2022:101.

[132] Konkurrensverket, dnr 232/2024, Ställningstagande 2024:1 *Konkurrensverkets ställningstagande om kostnadsfri tillgång till upphandlingsdokument*.

6 Möjligheter och hinder för användningen av integritetsfrämjande teknik

6.1 Inledning

Internationella exempel visar att det finns flera användningsområden för integritetsfrämjande teknik och potential att möjliggöra en förbättrad datadelning. Trots det visar utredningens kartläggning att de flesta integritetsfrämjande teknikerna endast används i begränsad omfattning inom offentlig förvaltning (se kapitel 4). Under utredningens arbete har ett antal faktorer identifierats vilka försvårar användandet av teknikerna.

I detta kapitel redovisas utredningens bedömning av de möjligheter och hinder som finns vid datadelning med integritetsfrämjande teknik. Inledningsvis redogör vi för skälen till varför teknikerna bör användas i större utsträckning, lämpliga användningsområden, nyttor och den tekniska mognadsgraden för teknikerna (avsnitt 6.2). Vi redovisar därefter de faktorer som vi bedömer är orsaken till den begränsade användningen (avsnitt 6.3 och 6.4).

6.2 Användningen av integritetsfrämjande teknik i förvaltningen bör öka

6.2.1 Teknikerna möjliggör modern datadelning i förvaltningen

Utredningens bedömning

Integritetsfrämjande teknik utgör ett effektivt verktyg för att möjliggöra en förbättrad datadelning inom offentlig förvaltning.

Skälen för utredningens bedömning

Teknikerna kan begränsa överskottsinformation och öka möjligheterna till datadelning

Det finns i dagsläget behov av en utökad datadelning inom olika delar av den offentliga förvaltningen. För att tillgodose dessa behov har olika sekretessbrytande bestämmelser och uppgiftsskyldigheter införts. Syftet har både varit att underlätta samarbetet mellan myndigheter och att upprätthålla kraven på förvaltningens effektivitet och rättssäkerhet. Den nya generella sekretessbrytande bestämmelsen i 10 kap. 15 a § offentlighets- och sekretesslagen (2009:400), OSL, är ett exempel på en sådan bestämmelse. Andra exempel är lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna och lagen (2024:307) om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet. Dessa bestämmelser gör det möjligt att utbyta både offentliga uppgifter och annars sekretessbelagda uppgifter i olika situationer. Vilka uppgifter som får och behöver delas i olika situationer skiljer sig åt mellan olika aktörer. Det avgörs bland annat av mottagarens behov och av de regleringar som styr dennes verksamhet.

I många fall behöver den som efterfrågar data bara ett urval av de uppgifter som finns i en viss datamängd. Det kan exempelvis röra sig om uppgifter om personer som uppfyller två specifika kriterier, snarare än uppgifter om samtliga personer som uppfyller vart och ett av kriterierna var för sig. Att dela uppgifter om samtliga personer är dessutom inte alltid möjligt med hänsyn till dataskydds-

regelverket eller sekretessbestämmelser. I en sådan situation kan integritetsfrämjande teknik, exempelvis säker flerpartsberäkning, användas för att identifiera den begränsade datamängd som är relevant att dela. På så vis möjliggör integritetsfrämjande teknik en datadelning som annars inte hade varit möjlig.

Med utökade möjligheter till datadelning kommer den offentliga förvaltningen också kunna utbyta uppgifter för att genomföra analyser eller utveckla olika analysverktyg i större utsträckning än tidigare.[1] Uppgifter kan också komma att delas i syfte att träna AI-modeller, eftersom AI-träning i regel kräver tillgång till stora mängder data för att resultatet inte ska bli missvisande eller leda till diskriminering.[2] Möjligheterna till att dela data för träning av AI-modeller kan öka med både federerad inlärning och moderna avidentifieringstekniker, som syntetiska data och differentiell integritet.

Teknikerna är samtidigt inte en enkel lösning på utmaningarna med att åstadkomma ökad datadelning och samverkan inom förvaltningen. Det finns även andra utmaningar, exempelvis interoperabilitet och datakvalitet. Det finns också utmaningar som beror på hur styrningen och finansieringen av förvaltningen är utformad. Det handlar till exempel om att regeringens styrning ofta inte är tillräckligt sammanhållen. Teknikerna har dock betydelse för förmågan att frigöra värdet i ökad datadelning, utan att kompromissa med den personliga integriteten.

Utökade rättsliga möjligheter till att dela data påverkar inte skyldigheten att följa dataskyddsregelverket

I samband med att nya bestämmelser som syftar till att öka datadelningen i offentlig förvaltning har införts, har vikten av principen om uppgiftsminimering lyfts fram.[3] De rättsliga möjligheterna till en utökad datadelning påverkar inte skyldigheten att uppgiftsminimera. De påverkar inte heller andra dataskyddsrättsliga krav, exempelvis avseende skyddsåtgärder. De aktörer som ska dela data måste

[1] Jfr SOU 2024:63 *Ökat informationsutbyte mellan myndigheter – Behov och föreslagna förändringar*, s. 443 f.
[2] Statskontoret, OOS 51, *Myndigheterna och AI - En studie om möjligheter och risker med att använda AI i statsförvaltningen*, s. 33.
[3] Prop. 2024/25:180 *Ökat informationsutbyte mellan myndigheter*, s. 81 och prop. 2024/25:65 *Ökat informationsflöde till brottsbekämpningen*, s. 185. Jfr också prop. 2023/24:85 *En ny lag om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet*, s. 57.

därför se till att tillgången till personuppgifter begränsas och vidta åtgärder för att säkerställa en lämplig skyddsnivå för uppgifterna.

Det är således inte bara de rättsliga möjligheterna genom sekretessbrytande bestämmelser eller uppgiftsskyldigheter som är avgörande för ökad datadelning. Även förutsättningarna för att uppfylla dataskyddsrättsliga krav, exempelvis på uppgiftsminimering, har stor betydelse. Integritetsfrämjande teknik är ett viktigt verktyg för att motverka de integritetsrisker som en ökad datadelning kan medföra. Enligt utredningens uppfattning kommer teknikerna i vissa fall dessutom vara nödvändiga för att de nya bestämmelserna om ökat informationsutbyte ska vara proportionerliga i praktiken. Med integritetsfrämjande teknik kan den offentliga förvaltningen fullt ut nyttja de utökade rättsliga möjligheterna till datadelning.

6.2.2 Det finns flera lämpliga tillämpnings- och användningsområden

Utredningens bedömning

Det finns flera lämpliga tillämpnings- och användningsområden för integritetsfrämjande teknik i offentlig förvaltning.

Skälen för utredningens bedömning

Teknikerna möjliggör samarbetsanalyser

Utredningen bedömer att det finns vissa områden där integritetsfrämjande teknik är av särskild betydelse. Det rör sig om både generella och mer specifika användningsområden. De generella användningsområdena är relevanta för hela eller stora delar av den offentliga förvaltningen medan de mer specifika berör särskilda typer av data eller behandlingar som sker för ett visst syfte.

Användningen av integritetsfrämjande tekniker som möjliggör analyser utan att underliggande data delas är ett tillämpningsområde som gäller generellt för hela den offentliga förvaltningen. Syftet med att analysera data är att nå insikter och se mönster i data som sedan kan användas som underlag för hur en viss situation ska hanteras. När den offentliga förvaltningen ska genomföra analyser samlas

vanligtvis stora mängder data in av den aktör som ska genomföra analysen. Ibland är det inte möjligt att samla in relevant data till analysen på grund av dataskyddsregelverket eller sekretess. Sådan traditionell datainsamling kan ersättas med hjälp av integritetsfrämjande teknik så att insikterna från analysen delas i stället för de underliggande uppgifterna. Det kan förbättra olika verksamheters förmåga att arbeta förebyggande och med mer underbyggda beslutsunderlag, till exempel inom brottsförebyggande verksamhet och inom socialtjänsten.

Tekniker som är lämpliga för analyser i samarbete med flera offentliga aktörer är till exempel federerad inlärning och säker flerpartsberäkning. Federerad inlärning möjliggör exempelvis gemensam träning av AI-modeller utan att underliggande data delas. Detta är särskilt relevant när bestämmelserna om sekretess eller dataskydd hindrar att data delas, men det ändå finns behov av att dela insikter. Enligt utredningens bedömning lämpar sig tekniken väl för kommuner och regioner, eftersom de har samma uppdrag och liknande datamängder. Med säker flerpartsberäkning sker analyser på krypterade data och sedan delas endast resultatet av analysen. Säker flerpartsberäkning möjliggör bland annat jämförelser av uppgifter hos flera offentliga aktörer och analyser på sekretessbelagda uppgifter, eftersom de är krypterade på ett sätt som gör att deltagarna i analysen inte kan ta del av dem. Säker flerpartsberäkning kan exempelvis användas för samarbetsanalyser som syftar till att identifiera individer som är berättigade till förmåner som de inte ansökt om. Ett framgångsrikt sådant exempel återfinns inom socialförsäkringen i Nederländerna (se avsnitt 4.4.3). Tekniken kan även användas för efterhandskontroller i syfte att upptäcka misstänkta bidragsbrott enligt bidragsbrottslagen (2007:612), exempelvis när ändrade förhållanden inte har anmälts.

Ett annat potentiellt användningsområde för samarbetsanalyser med säker flerpartsberäkning är analyser av data från olika kommunala förvaltningar som inte kan delas på grund av sekretess, exempelvis mellan socialtjänst och skolförvaltning. Genom sådana analyser kan insikter om barn och unga med förhöjd risk för att dras in i kriminalitet delas, vilket möjliggör riktade stödinsatser. Även om direkta personuppgifter inte alltid kan delas, kan förvaltningarna få bättre beslutsunderlag till sin verksamhetsplanering.

Avidentifieringstekniker är av särskild betydelse vid träning av AI-modeller

Integritetsfrämjande teknik utgör en central komponent vid såväl framtagande av träningsdata som vid utveckling och träning av AI-modeller. En grundläggande utmaning vid AI-utveckling är att tillgång till omfattande och representativa data ofta förutsätter en omfattande behandling av personuppgifter. Utan adekvata skyddsåtgärder riskerar sådan behandling att stå i strid med dataskyddsregelverket. Det riskerar även att undergräva allmänhetens förtroende för användningen av AI.

I takt med att AI används i allt större utsträckning inom offentlig förvaltning ökar behovet av att säkerställa att personuppgifter behandlas på ett rättsligt, tekniskt och etiskt korrekt sätt. Integritetsfrämjande teknik kan här bidra till att reducera integritetsriskerna utan att begränsa möjligheten till att använda data.

Vid framställning av träningsdata är olika former av avidentifieringstekniker av särskild betydelse. Sådana tekniker minskar risken för att enskilda individer ska kunna identifieras i den data som används för modellutveckling. Enligt vår bedömning har syntetiska data här en framträdande roll, då dessa kan efterlikna verkliga datamönster utan att innehålla information hänförlig till verkliga individer. Med syntetiska data kan AI-modeller tränas och användas utan att personuppgifter behandlas i AI-modellen. Syntetiska data kan dessutom genereras i stora volymer i situationer där det finns en begränsad tillgång till verkliga data. Därutöver kan differentiell integritet tillämpas vid skapandet av syntetiska data för att säkerställa att den syntetiska datan inte innehåller uppgifter som går att hänföra till en verklig individ.

Federerad inlärning utgör ytterligare en viktig teknik för träning av AI-modeller eftersom den minskar behovet av att träningsdata samlas in centralt. Det stärker skyddet för uppgifterna och säkerställer att principen om uppgiftsminimering upprätthålls. Utredningen bedömer även att kryptografiska tekniker som möjliggör integritetsbevarande maskininlärning (privacy-preserving machine learning) kommer att vara viktiga för AI-träning på sikt. Genom att AI-modellerna tränas på data som är krypterad, med exempelvis säker flerpartsberäkning eller homomorf kryptering, erbjuds ett ytterligare skyddslager. Det kan vara användbart i situationer där det

på grund av sekretess eller dataskydd ställs höga krav på skyddsåtgärder.

Teknikerna kan användas för att förbättra datadelningen inom hälso- och sjukvård

Ett mer specifikt användningsområde där integritetsfrämjande teknik är av särskild betydelse rör datadelning inom hälso- och sjukvården. I patientjournaler finns bland annat uppgifter om diagnoser, behandlingar, genetiska förutsättningar och psykisk hälsa. Dessa uppgifter utgör känsliga personuppgifter enligt dataskyddsförordningen, vilket medför högre krav på skyddsåtgärder och behandlingsrutiner. Uppgifter om enskildas hälsotillstånd omfattas också som huvudregel av sekretess. Samtidigt som lagstiftningen skyddar hälsouppgifterna finns det ett stort behov av att dela data inom hälso- och sjukvården för exempelvis medicinsk forskning, utveckling av nya behandlingsmetoder och utveckling av AI-baserade diagnosverktyg.

Det finns stora datamängder inom hälso- och sjukvården som kan skapa nytta, men som ofta inte kan delas. Det är därför inte alltid möjligt att samla in den data som behövs inom hälso- och sjukvården när den är utspridd hos flera olika aktörer. Då kan exempelvis federerad inlärning användas för att träna AI-modeller för diagnosverktyg utan att träningsdata delas mellan aktörerna. För att stärka skyddet ytterligare och minska risken för att AI-modellen minns den data den tränats på kan träningsdata även avidentifieras med differentiell integritet innan den används. Även säker flerpartsberäkning kan användas för att göra analyser med data från flera olika aktörer inom hälso- och sjukvården. Ett exempel på det är forskningsprojektet Federated Secure Computing (se avsnitt 4.4.1).

Teknikerna kan minska överskottsinformation i brottsbekämpande verksamhet

Integritetsfrämjande teknik kan skapa nya möjligheter för brottsbekämpande myndigheter att bearbeta data på ett rättssäkert sätt. Vid utredning av vissa typer av brott, exempelvis ekonomisk brottslighet och bidragsbrott, finns ofta ett behov av att sammanställa

information som finns hos olika delar av den offentliga förvaltningen. Möjligheten att samla in data i syfte att identifiera misstänkta brott kan i vissa fall begränsas av regler om dataskydd och sekretess. Integritetsfrämjande teknik kan möjliggöra strukturerade och rättssäkra analyser över flera datakällor och på så vis fungera som ett stöd för brottsbekämpande myndigheter. Vidare kan teknikerna bidra till att skapa en balans mellan effektiv brottsbekämpning och ett högt skydd för den personliga integriteten.

Av särskild betydelse i detta sammanhang är säker flerpartsberäkning som möjliggör bearbetning på krypterade data från flera datakällor utan att de underliggande uppgifterna delas. Detta kan ge brottsbekämpande myndigheter utökad kunskap om olika upplägg och mönster, samtidigt som skyddet för personuppgifter och sekretessbelagda uppgifter upprätthålls. Det kan också ge brottsbekämpande myndigheter utökade möjligheter att identifiera relevanta individer för vidare utredning utan att överskottsinformation delas. Eftersom endast resultatet delas, i form av relevanta träffar eller riskindikatorer, minimeras behandlingen av personuppgifter som inte är relevanta i sammanhanget. Detta reducerar integritetsrisker och bidrar till ett rättssäkert arbetssätt.

6.2.3 Integritetsfrämjande teknik vid datadelning kan medföra flera betydande nyttor

Utredningens bedömning

Det finns betydande nyttor med att öka användningen av integritetsfrämjande teknik vid datadelning inom offentlig förvaltning.

Skälen för utredningens bedömning

Teknikerna utgör ett centralt verktyg för att realisera de potentiella nyttor som följer av förbättrad datadelning

Vi bedömer att en ökad användning av integritetsfrämjande teknik vid datadelning inom offentlig förvaltning kan medföra flera betydande positiva effekter (nyttor). Detta gäller särskilt för moderna tekniker så som differentiell integritet, federerad inlärning och säker

flerpartsberäkning. Den samhällsekonomiska analys som utredningen har låtit genomföra visar att integritetsfrämjande teknik utgör ett centralt verktyg för att realisera de potentiella nyttor som följer av förbättrad datadelning inom förvaltningen. Den samlade samhällsekonomiska nyttopotentialen av ökad och förbättrad datadelning i offentlig förvaltning uppskattas till cirka 30–80 miljarder kronor per år. Av detta bedöms 10–40 miljarder kronor årligen vara direkt beroende av användningen av integritetsfrämjande teknik.[4]

Möjligheterna att använda integritetfrämjande teknik är särskilt stora inom verksamheter som genererar och hanterar omfattande mängder känsliga eller sekretessbelagda uppgifter. Det gäller bland annat hälso- och sjukvård, socialtjänst och brottsbekämpande verksamhet. De uppskattade nyttorna återfinns därför i huvudsak inom dessa områden.[5]

Teknikerna kan skapa ökad effektivitet och säkerhet inom förvaltningen

Integritetsfrämjande teknik kan enligt utredningens bedömning bidra till ökad effektivitet inom offentlig förvaltning på flera sätt. Genom förbättrade förutsättningar för datadelning mellan offentliga aktörer kan tidsåtgången och kostnaderna för insamling, hantering och analys av data minska.

Inom hälso- och sjukvården kan detta exempelvis innebära minskad manuell informationshantering och kortare dokumentationstider. Det kan också innebära effektivare arbetsflöden samt förbättrade möjligheter till prioritering och resursplanering. Teknikerna kan även bidra till att minska dubbelarbete, så som upprepade undersökningar av patienter, och möjliggöra användning av fler relevanta datakällor. Det kan i sin tur leda till bättre analyser och beslut. Utredningens samhällsekonomiska analys visar att olika integritetsfrämjande tekniker, exempelvis federerad inlärning och säker flerpartsberäkning, kan möjliggöra användningen av klinisk AI och beslutsstöd vid val av behandlingsmetoder. Det kan bland annat förbättra diagnostik, prediktion av vårdbehov och ge snabbare

[4] Bilaga 2, *Samhällsekonomisk analys av potentialen för ökad användning av integritetsfrämjande teknik i offentlig förvaltning*, s. 12.
[5] En fördjupad redovisning av nyttor och slutsatser från den samhällsekonomiska analysen lämnas i konsekvensutredningen (se avsnitt 9.5).

behandlingsbeslut. Nyttopotentialen vid tillämpningen av teknikerna för klinisk AI och beslutsstöd uppskattas till minst 4,9 miljarder kronor per år.[6]

Integritetsfrämjande teknik kan även bidra till snabbare handläggning och effektivare myndighetsbeslut. Genom förbättrade analysmöjligheter kan verksamheter i högre grad automatisera och effektivisera sina processer och tjänster. Förbättrad datadelning mellan myndigheter kan exempelvis möjliggöra AI-drivna automatiserade kontroller av bidragsutbetalningar och därigenom minska risken för felaktiga utbetalningar. Utredningens samhällsekonomiska analys visar att användningen av säker flerpartsberäkning för registerkontroller vid exempelvis AI-drivna automatiserade kontroller av utbetalningar kan minska och motverka felaktiga skatte- och bidragsutbetalningar. Nyttopotentialen för sådana registerkontroller uppskattas till minst 500 miljoner kronor per år.[7]

Integritetsfrämjande teknik kan även minska behovet av att dela eller lagra stora mängder data, vilket reducerar exponeringen av känsliga uppgifter och stärker skyddet för den personliga integriteten. Säkerheten kan också förbättras genom att data i större utsträckning bearbetas lokalt, vilket minskar behovet av dataöverföring och därmed risken för obehörig åtkomst.

Teknikerna kan öka kvaliteten och servicen till enskilda och företag

En ökad användning av integritetsfrämjande teknik kan möjliggöra en mer sammanhållen, effektiv och datadriven offentlig förvaltning. Teknikerna skapar förutsättningar för att förena hög kvalitet i beslut och tjänster med ökad tillgänglighet och förbättrad service till både enskilda och företag.

Genom att möjliggöra analys av data över organisatoriska gränser kan en mer heltäckande bild av samhällsutmaningar och individers behov uppnås. Det kan bidra till förbättrade beslutsunderlag och mer träffsäkra insatser inom bland annat hälso- och sjukvård, socialtjänst och arbetsmarknadspolitik. Det gäller till exempel inom precisionsmedicin som förutsätter en stor mängd data, inklusive känsliga personuppgifter, för att möjliggöra skräddarsydd prevention,

[6] Bilaga 2, *Samhällsekonomisk analys*, s. 26 f.
[7] Bilaga 2, *Samhällsekonomisk analys*, s. 39 f.

diagnos, behandling och uppföljning. När större datamängder tillgängliggörs kan behandlingar och annat utgå från den enskilde patientens unika förutsättningar, exempelvis genetisk profil och specifika biomarkörer. Utredningens samhällsekonomiska analys visar även att användningen av integritetsfrämjande teknik, däribland differentiell integritet, kan möjliggöra ökad sekundäranvändning av hälsodata för forskningsändamål. Det kan bland annat bidra till att nya läkemedel och förbättrade behandlingsmetoder tas fram. Nyttopotentialen för användning av teknikerna för detta ändamål uppskattas till minst 800 miljoner kronor per år.[8]

Med integritetfrämjande teknik kan det också skapas bättre förutsättningar för ett mer individanpassat stöd och beslutsfattande. Den samhällsekonomiska analysen visar att användning av integritetsfrämjande teknik kan bidra till att förbättra och effektivisera samordningen av individstöd, särskild vid ärenden som kräver insatser från flera huvudmän. Nyttopotentialen uppskattas inom detta tillämpningsområde till minst 2,4 miljarder kronor årligen.[9] Ett annat exempel på när integritetsfrämjande teknik kan bidra till ett mer situationsanpassat stöd är AI-baserad vägledning som på ett sammanhållet sätt stödjer enskilda och företag vid mötet med den offentliga förvaltningen. En sådan lösning finns redan i Estland i form av AI-assistenten Bürokratt som ger ett individanpassat stöd för enskilda som kontaktar den offentliga förvaltningen (se avsnitt 4.4.5).

Teknikerna kan förbättra insikter om samhällsutmaningar

Integritetsfrämjande teknik stärker möjligheterna till samverkan inom offentlig förvaltning, exempelvis mellan olika organisationer, förvaltningsnivåer och sektorer. Genom att i högre grad kunna utbyta analyserade insikter i stället för underliggande uppgifter förbättras förutsättningarna för ett helhetsperspektiv och samordnade insatser. Detta är särskilt relevant vid hantering av komplexa samhällsutmaningar, så som brottsförebyggande och brottsbekämpande verksamhet, där insatser ofta kräver samverkan mellan flera offentliga aktörer. Vår samhällsekonomiska analys visar att integritetsfrämjande teknik kan vara ett viktigt verktyg för en förbättrad be-

[8] Bilaga 2, *Samhällsekonomisk analys*, s. 30 f.
[9] Bilaga 2, *Samhällsekonomisk analys*, s. 38 f.

kämpning av välfärdsbrott. Genom att exempelvis möjliggöra en automatiserad matchning av uppgifter från flera aktörer kan säker flerpartsberäkning användas för att identifiera mönster och indikatorer som tyder på organiserad brottslighet, vilket kan leda till minskade välfärdsbrott. Nyttopotentialen uppskattas inom detta tillämpningsområde till minst 1,7 miljarder kronor per år.[10]

Teknikerna kan även stödja ett mer proaktivt och förebyggande arbetssätt genom att möjliggöra tidigare identifiering av mönster och riskfaktorer. Inom exempelvis socialtjänsten kan analyser av data från flera källor bidra till att minska risken för sena eller felaktiga insatser och därmed öka möjligheterna till att åtgärder vidtas innan problem uppstår eller förvärras. Utredningens samhällsekonomiska analys visar exempelvis att federerad inlärning och differentiell integritet kan förbättra möjligheten att tidigt identifiera barn och unga med behov av stödinsatser. Nyttopotentialen uppskattas inom detta tillämpningsområde till minst 1,1 miljarder kronor per år.[11]

Teknikerna ökar innovation

En ökad användning av integritetsfrämjande teknik bedöms även bidra till stärkt innovationsförmåga inom offentlig förvaltning. Genom att flytta gränserna för vilken data och vilka insikter som kan delas, möjliggör teknikerna ett mer omfattande samarbete mellan aktörer och underlättar att data från flera källor kombineras. Detta kan öka både takten och kvaliteten i innovationsarbetet. Samtidigt bidrar teknikerna till att reducera riskerna vid databehandling, vilket kan öka organisationers benägenhet att initiera, testa och investera i nya lösningar.

[10] Bilaga 2, *Samhällsekonomisk analys*, s. 42 f.
[11] Bilaga 2, *Samhällsekonomisk analys*, s. 38 f.

6.2.4 Den tekniska mognadsgraden varierar

Utredningens bedömning

Den tekniska mognadsgraden för olika integritetsfrämjande tekniker skiljer sig åt.

Det finns integritetsfrämjande tekniker som är tillräckligt tekniskt mogna för att användas i större utsträckning och användningen av dessa bör därför öka inom offentlig förvaltning.

Skälen för utredningens bedömning

Flera faktorer har betydelse för bedömningen av teknikernas mognadsgrad

Den tekniska mognadsgraden för integritetsfrämjande teknik varierar. Med teknisk mognadsgrad avses hur redo tekniken är för bred användning inom förvaltningen, det vill säga hur välutvecklad och användbar tekniken är i praktiken. Vissa tekniker används redan i dag i offentlig förvaltning för att möjliggöra datadelning. Andra tekniker används i liten omfattning eller inte alls.

För att avgöra om en viss teknik är mogen för användning i offentlig förvaltning har vi bedömt de tekniska förutsättningarna för användning. I vår bedömning har vi särskilt beaktat teknikernas behov av infrastruktur, kompatibilitet med befintliga system, säkerhet och befintlig kompetens om teknikerna. För de integritetsfrämjande tekniker som är tekniskt mogna att använda i dag bedömer vi att beräkningskapacitet inte är en avgörande faktor. Däremot är beräkningskapaciteten mer avgörande för tekniker som kan bli aktuella att använda i större utsträckning på längre sikt. När det gäller befintlig kompetens om teknikerna har både den offentliga förvaltningens kunskap och den kompetens som är tillgänglig på den privata marknaden vägts in (se avsnitt 4.3).

Tekniker som redan används kan få ökad användning

De etablerade teknikerna, så som anonymisering och pseudonymisering, används i dag i betydande omfattning i offentlig förvaltning. Även om det finns risk för återidentifiering med dessa tekniker så bedömer utredningen att etablerade avidentifieringstekniker även fortsättningsvis kommer att användas. Det kan noteras att klargörandet från EU-domstolen[12] avseende att pseudonymiserade uppgifter inte alltid anses vara personuppgifter hos mottagaren kan medföra att dessa tekniker får en ökad användning.

Vad gäller moderna tekniker används även några av dessa i viss utsträckning i dag. Syntetiska data används till exempel för att skapa träningsdata. Utredningen bedömer att det inte föreligger några hinder för fortsatt användning och att behovet av syntetiska data sannolikt kommer att öka i takt med att AI används i större utsträckning i förvaltningen.

Betrodda exekveringsmiljöer är enklare i sin tekniska utformning än andra tekniker som skyddar data under bearbetning. Det har bidragit till att tekniken redan används i relativt stor omfattning inom offentlig förvaltning (se avsnitt 4.2.1). Europeiska datatillsynsmannen (EDPS) har i en rapport lyft fram konfidentiell databehandling (confidential computing) med betrodda exekveringsmiljöer som en trend för 2025–2026.[13] Utredningens bedömning är användningen av tekniken kommer att öka inom förvaltningen.

Det finns tekniker som borde användas i större utsträckning

Det finns integritetsfrämjande tekniker med stor potential, men som används i begränsad omfattning i offentlig förvaltning trots att teknikerna är tekniskt mogna. Utredningens bedömning är att användningen av dessa tekniker bör öka.

Differentiell integritet är en teknik som används i större omfattning internationellt än i den svenska förvaltningen. Tekniken har potential att komplettera och i vissa fall ersätta etablerade avidentifieringstekniker eftersom tekniken erbjuder ett starkare skydd mot angrepp. En viktig fråga för ökad användning är behovet av vägled-

[12] Domstolens dom av den 4 september 2025, Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden, C-413/23 P, EU:C:2025:645, se även avsnitt 2.4.4.
[13] Europeiska datatillsynsmannen (EDPS), *TechSonar Report 2025–2026*, s. 24.

ning gällande vilken tillåten nivå av integritetsförlust (epsilon, ε) som bör användas.

Federerad inlärning är i dagsläget inte utbredd inom offentlig förvaltning, men det finns inga betydande tekniska hinder mot att tekniken tillämpas. Vår bedömning är att användningen kommer att öka i takt med den fortsatta utvecklingen av AI.

Säker flerpartsberäkning är en teknik som endast någon enstaka offentlig aktör har använt. Tekniken möjliggör att insikter delas i stället för underliggande data vilket gör att den kan användas för att göra analyser på sekretessbelagd information. Även om bearbetning av data under kryptering är resurskrävande har säker flerpartsberäkning inte lika stora tekniska utmaningar som exempelvis homomorf kryptering. Det är därför sannolikt att intresset för säker flerpartsberäkning kommer att öka. Tekniken är redan i dag tillräckligt tekniskt mogen för att användas inom flera områden i offentlig förvaltning.

Det finns tekniker som för tillfället inte är tekniskt mogna för användning

Homomorf kryptering erbjuder mycket höga säkerhetsgarantier, men är förknippad med tekniska utmaningar. Tekniken är resurskrävande, komplex att implementera och ofta inkompatibel med befintliga system. Även om den tekniska utvecklingen går snabbt är utredningens bedömning att det inte är realistiskt att anta att tekniken kommer att få en bred användning inom offentlig förvaltning i närtid.

Nollkunskapsbevis är en annan avancerad kryptografisk teknik. Vi anser att de utmaningar och problem som går att lösa med nollkunskapsbevis mellan myndigheter i många fall bör gå att lösa med mindre komplicerade lösningar.[14] Utredningen bedömer därför att tekniken under de närmaste åren inte kommer börja användas i någon större utsträckning för datadelning mellan myndigheter. Den tekniska mognaden hos nollkunskapsbevis kan dock påskyndas om tekniken införs i de digitala plånböckerna inom EU. En sådan användning skulle sannolikt öka efterfrågan och kunskapen om tekniken.

[14] Exempel på lösningar som möjliggör delandet av begränsade data, så som att en person är myndig, bygger på standarden OAuth 2.0 från IETF. Se https://datatracker.ietf.org/doc/html/rfc6749 (hämtad 2026-03-06).

Därigenom skulle även incitament för utveckling av förbättrade och standardiserade protokoll för nollkunskapsbevis skapas.

Trots att utredningen bedömer att dessa tekniker inte är tekniskt mogna för användning i dagsläget så går teknikutvecklingen snabbt. Om några år kan det därför finnas lämpliga användningsområden för dessa tekniker i förvaltningen.

6.2.5 Ökad användning förbättrar möjligheten att påverka den fortsatta utvecklingen

Utredningens bedömning

Ökad användning av integritetsfrämjande teknik skapar bättre möjligheter för Sverige att påverka både den tekniska och rättsliga utvecklingen.

Skälen för utredningens bedömning

Utvecklingen av integritetsfrämjande teknik har under det senaste decenniet gått från teoretisk forskning till praktiskt tillämpbara lösningar. Genom utveckling av mjukvara och hårdvara som möjliggör implementering samt genom framtagandet av allt fler relevanta standarder har flera tekniker nått en teknisk mognadsgrad som gör dem användbara i praktiken. Det har också skapats en större förståelse för hur teknikerna kan skapa affärsmöjligheter och samhällsnytta.

Integritetsfrämjande teknik befinner sig i ett skede där konkreta behov och användningsfall i allt högre grad påverkar den fortsatta tekniska utvecklingen. Genom att identifiera användningsfall som kan bidra till ökad effektivitet i offentlig förvaltning och därefter styra införandet av integritetsfrämjande teknik mot dessa områden, kan flera nyttor uppnås. Förutom att effektivisera den offentliga förvaltningen kan Sverige inta en tidig position i det tekniksprång som nu sker, vilket skapar förutsättningar för export av tjänster och produkter som utvecklas nationellt. Sverige kan även få förbättrade möjligheter att påverka utvecklingen av internationellt tillgängliga lösningar, vilket kan bidra till att dessa är anpassade till de behov och krav som finns inom svensk förvaltning.

Utredningen kan konstatera att även det rättsliga området för datadelning genomgår betydande förändringar, inte minst på europeisk nivå. Efter en period av relativt omfattande reglering pågår nu en utveckling mot förenklingar och harmonisering. Nya direktiv, förordningar och europeiska dataområden innebär att regelverket kontinuerligt förändras. Även nationell rätt har de senaste åren gett utökade förutsättningar för datadelning (se avsnitt 6.2.1). Med hänsyn till att det införts krav på användning av integritetsfrämjande teknik i olika EU-rättsakter (avsnitt 5.2.1) finns det skäl för Sverige att prioritera användningen av integritetsfrämjande inom offentlig förvaltning.

Utredningen bedömer att om Sverige tidigt visar hur integritetsfrämjande teknik kan användas i konkreta tillämpningar skapas exempel på hur teknik och juridik kan samverka på ett ändamålsenligt sätt. Dessa erfarenheter kan bidra till det fortsatta europeiska lagstiftningsarbetet och därigenom öka möjligheterna att framtida regleringar blir ändamålsenliga i en svensk kontext.

6.3 Begränsad kunskap och styrning begränsar användningen av integritetsfrämjande teknik

6.3.1 Kunskapen om vissa tekniker är låg

Utredningens bedömning

Kunskapsnivån om integritetsfrämjande teknik inom offentlig förvaltning behöver förbättras för att användningen ska öka på ett ändamålsenligt sätt.

Skälen för utredningens bedömning

Förvaltningens kunskap är begränsad

En grundläggande förutsättning för att kunna använda sig av en viss teknik är kunskap om tekniken. Det handlar inte enbart om att förstå den tekniska och rättsliga tillämpningen av tekniken, utan också om att förstå potentiella användningsområden och nyttor.

En ökad förståelse av nyttorna med tekniken är en viktig faktor för att den ska börja användas i större utsträckning.

Under utredningens arbete har det framkommit att kunskapen om integritetsfrämjande teknik inom offentlig förvaltning är begränsad. När integritetsfrämjande teknik kommer på tal hänvisas i första hand till etablerade tekniker så som anonymisering och pseudonymisering. Som stöd vid användningen av dessa tekniker finns bland annat vägledning från Myndigheten för digital förvaltning (Digg) och Statistiska centralbyrån (SCB) om skyddade data. Det finns också riktlinjer om pseudonymisering från Europeiska dataskyddsstyrelsen (EDPB).

Det finns även andra tekniker än de etablerade avidentifieringsteknikerna som används i viss utsträckning i dag. Så är fallet vad gäller exempelvis syntetiska data och betrodda exekveringsmiljöer. Kunskapsnivån för just dessa tekniker är något högre än för andra moderna tekniker. Det framgår också av att det främst är dessa tekniker som har testats i olika svenska projekt och regulatoriska sandlådor. Det finns dock inte samma sorts kunskapsstöd för dessa integritetsfrämjande tekniker som det finns för etablerade tekniker.

För övriga moderna integritetsfrämjande tekniker är kunskapen mycket begränsad och i vissa fall obefintlig inom stora delar av den offentliga förvaltningen. Det finns i dagsläget inte heller etablerade stödstrukturer som gör det möjligt för förvaltningen att i större utsträckning inhämta eller utveckla kunskap om teknikerna, till exempel i form av stöd och vägledning avseende teknikerna.

Utredningen bedömer att kunskapen om moderna integritetsfrämjande tekniker inom förvaltningen behöver förbättras för att de ska börja användas i större utsträckning.

Det krävs kunskap för att välja rätt teknik

Integritetsfrämjande teknik utgör inte en enhetlig kategori av tekniker utan omfattar lösningar med skilda egenskaper, riskprofiler och skyddslogiker. Skillnaderna mellan teknikerna gäller inte endast deras tekniska uppbyggnad utan också vilken typ av risker de hanterar och hur skyddet är avsett att verka. Vissa tekniker erbjuder ett preventivt skydd medan andra utgör kontrollbaserade skyddsåtgärder. Även inom respektive teknikområde varierar funktion,

teknisk mognadsgrad och tillämpningsområde. Som exempel kan nämnas att flera tekniker för skyddad bearbetning bygger på att bearbetningen sker under kryptering, men det gäller inte betrodda exekveringsmiljöer. De flesta avidentifieringstekniker är avsedda att ge ett oåterkalleligt skydd, till skillnad från pseudonymisering som under vissa förutsättningar är reversibel.

Dessa skillnader gällande funktion, metod, skyddslogik och teknisk mognadsgrad försvårar användningen av teknikerna. Bristande kunskap om skillnaderna gör det vidare svårt att bedöma vilka tekniker som är lämpliga i olika situationer eller hur tekniker bör kombineras för att uppnå ett adekvat skydd.

6.3.2 Det saknas styrning av användningen

Utredningens bedömning

Det behövs tydligare styrning för att öka användningen av integritetsfrämjande teknik.

Skälen för utredningens bedömning

Utvecklingen av integritetsfrämjande teknik har skett under en längre tid men med lite styrning och samordning. För att realisera teknikernas potential i offentlig förvaltning krävs en ökad nationell styrning och organisering avseende integritetsfrämjande teknik. EU har under de senaste åren infört krav på att integritetsfrämjande teknik ska användas för att stärka integritetsskyddet. Den styrning som kommer från EU är dock begränsad till att vissa tekniker ska användas i vissa situationer men det saknas styrning av hur teknikerna ska användas, vilket skapar osäkerhet och leder till att teknikerna inte används eller att de används på olika sätt.

Regeringen har endast i begränsad utsträckning styrt användningen av integritetsfrämjande teknik, till exempel genom uppgifter och regeringsuppdrag till statliga myndigheter. Det finns i dagsläget ingen myndighet som har ett utpekat ansvar som avser integritetsfrämjande teknik, till exempel vad gäller att främja eller stödja användningen av dessa tekniker inom offentlig förvaltning. Det leder till att det endast i begränsad utsträckning finns stöd och vägled-

ning om hur teknikerna ska användas, särskilt för de moderna teknikerna. Det finns några vägledningar och riktlinjer som rör etablerade tekniker, vilket bidrar till att dessa tekniker används vid datadelning. Det är dock inte tillräckligt för att säkerställa en rättssäker, effektiv och ändamålsenlig användning av integritetsfrämjande teknik. Avsaknaden av juridiskt stöd bidrar också till den osäkerhet om användningen av teknikerna som finns i förvaltningen (se avsnitt 6.4).

Utredningens bedömning är att en ökad datadelning inom offentlig förvaltning kräver att det finns tydligare styrning genom gemensamma vägledningar, riktlinjer och standarder för hur teknikerna ska användas.

6.4 Upplevd juridisk osäkerhet begränsar användningen av integritetsfrämjande teknik

6.4.1 Osäkerhet om teknikerna får användas

Utredningens bedömning

Inom offentlig förvaltning råder en osäkerhet om hur teknikerna får användas i förhållande till dataskyddsregelverket och offentlighets- och sekretessregleringen.

Skälen för utredningens bedömning

Under utredningens arbete har det framkommit att det uppfattas som oklart om teknikerna kan användas, framför allt när det gäller andra tekniker än anonymisering och pseudonymisering (se avsnitt 4.2.3). Centrala rättsliga frågor som måste besvaras vid användningen är om det finns rättslig grund för att behandla personuppgifter och om behandlingen ryms inom de ändamål för vilka aktören får behandla uppgifterna. Det behöver också ske en bedömning av om det sker ett utlämnande av uppgifter och om det i sådana fall finns stöd för utlämnandet i offentlighets- och sekretessregleringen. Utöver dessa rättsliga frågeställningar finns också en rad andra dataskyddsrättsliga frågor som behöver analyseras för att säkerställa

efterlevnaden av dataskyddsförordningen och kompletterande nationell rätt.

Utredningen kan konstatera att det finns en upplevd osäkerhet om de rättsliga förutsättningarna vilket kan leda till en försiktig och strikt tillämpning av regelverken. Det kan i sig motverka innovation och användning av teknikerna.[15] Den snabba teknikutvecklingen leder dessutom till nya frågeställningar och nya osäkerheter om tolkning och tillämpning av regelverken. Vi analyserar och bedömer därför i betänkandet de rättsliga förutsättningarna för användningen av integritetsfrämjande teknik (se vidare avsnitt 7.3).

6.4.2 Osäkerhet om teknikerna har använts i tillräcklig utsträckning

Utredningens bedömning

Inom offentlig förvaltning råder en osäkerhet om när användningen av teknikerna skett i tillräcklig utsträckning för att data ska kunna delas.

Skälen för utredningens bedömning

Utredningen kan konstatera att det råder stor osäkerhet gällande när en avidentifieringsåtgärd kan anses vara tillräcklig för att uppgifterna rättsligt ska vara att betrakta som anonyma. Att det är en svår fråga förtydligas av Europeiska kommissionens senaste förslag om ändringar i definitionen av personuppgifter i dataskyddsförordningen och anteckningarna från EDPB:s intressentmöte om anonymisering och pseudonymisering.[16]

Frågan om när data kan anses vara anonym väcks också vid användningen av moderna avidentifieringstekniker och när AI-modeller tränas med federerad inlärning. I det senare sammanhanget lyfts ofta frågan om en AI-modell kan minnas personuppgifter som används vid träningen. Det som avses är i regel huruvida det vid med-

[15] Jfr bl.a. Integritetsskyddsmyndigheten (IMY), IMY-2024-2570, *Integritet och ny teknik 2020–2024*, s. 11.
[16] https://www.edpb.europa.eu/system/files/2026-02/edpb-report-stakeholder-event-anonymisation-pseudonymisation_en.pdf (hämtad 2026-02-23).

lemskapsinferensattacker[17] (membership inference attacks) eller modellinversionsattacker[18] (model inversion attack) går att återfinna eller återskapa personuppgifter som AI-modellen har tränats på.

En annan osäkerhet som utredningen har uppmärksammat handlar om kryptering, närmare bestämt frågan om när en offentlig aktör kan vara säker på att uppgifter inte anses vara röjda i offentlighets- och sekretesslagens mening. Denna osäkerhet handlar om de tekniker som bearbetar data under kryptering. Av förarbetena till 10 kap. 2 a § OSL framgår det att en uppgift inte bör betraktas som röjd enligt OSL om uppgiften är krypterad på ett sådant sätt att mottagaren saknar teknisk kapacitet att forcera krypteringen. Det finns dock ingen vägledning i hur den bedömningen bör göras eller vilka faktorer som är relevanta, exempelvis framtida möjligheter att bryta krypteringen och utvecklingen av kvantdatorer. Utredningen bedömer att osäkerheten bidrar till att tekniker som bygger på kryptografi inte används. Utredningens förslag för att minska denna osäkerhet finns i avsnitt 8.3–8.4.

[17] En medlemskapsinferensattack utnyttjar att AI-modeller ofta ger mer säkra och specifika svar på data de tränats på, vilket gör att en angripare kan avgöra om en viss datapunkt ingick i träningsdata genom att analysera hur modellen svarar på specifika indata.
[18] En modellinversionsattack innebär att en angripare, genom systematiska frågor och analys av en AI-modells utdata med hjälp av maskininlärning, kan återskapa information om det data som använts vid modellens träning.

7 De rättsliga förutsättningarna för att använda integritetsfrämjande teknik vid datadelning

7.1 Inledning

Inom den offentliga förvaltningen finns en upplevd osäkerhet avseende de rättsliga förutsättningarna som begränsar användningen av integritetsfrämjande teknik (se avsnitt 6.4). Det finns därför skäl att analysera dessa förutsättningar. I detta kapitel beskrivs mer utförligt de rättsliga ramarna för att använda integritetsfrämjande teknik och dela data (avsnitt 7.2). Här redovisas också utredningens slutsatser om att det finns rättsliga förutsättningar för att använda integritetsfrämjande teknik (avsnitt 7.3). Dessa avsnitt är främst av intresse för jurister och andra som vill fördjupa sig i de rättsliga frågorna. Vi redovisar därefter vår bedömning av behovet av att införa särskilda krav på att integritetsfrämjande teknik ska användas samt andra krav vid användningen av integritetsfrämjande teknik (avsnitt 7.4). Slutligen behandlas frågan om när integritetsfrämjande teknik har använts i tillräcklig utsträckning (avsnitt 7.5).

7.2 Ramarna för användning av integritetsfrämjande teknik vid datadelning

Data utgör enligt utredningens begreppsanvändning information i digitalt format, oberoende av medium. Det innebär att data kan innehålla personuppgifter eller andra känsliga uppgifter. Förutsättningarna för att bearbeta och dela uppgifter styrs bland annat av dataskyddsregelverket och offentlighets- och sekretesslagen (2009:400), OSL. I kapitel 2 har vi översiktligt redogjort för de rättsliga ramarna.

Nedan redovisas mer utförligt den gällande rätt som är särskilt relevant för våra bedömningar och förslag.

7.2.1 Närmare om dataskydd

Laglighet och rättslig grund

För att behandling av personuppgifter över huvud taget ska vara tillåten krävs att någon av de rättsliga grunder som anges i artikel 6 i dataskyddsförordningen[1] är tillämpliga. Utöver att någon av dessa ska vara tillämpliga, krävs också att all behandling av personuppgifter följer samtliga grundläggande principer som anges i artikel 5 i dataskyddsförordningen. De rättsliga grunder som i första hand aktualiseras vid personuppgiftsbehandlingar inom den offentliga förvaltningen finns i artikel 6.1 c och e. Där anges att behandlingen är laglig om den är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1 c) eller om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1 e).

De rättsliga grunder som anges i artikel 6.1 c och e måste också vara fastställda i den nationella rätten eller unionsrätten.[2] Den rättsliga grunden i artikel 6.1 e är ofta fastställd i till exempel myndigheters instruktioner eller i annan reglering som styr verksamheten. Den rättsliga grunden i artikel 6.1 c kan bland annat vara fastställd genom författningsreglerade uppgiftsskyldigheter eller sekretessbrytande bestämmelser i offentlighets- och sekretesslagen. I svensk rätt framgår detta förhållande av 2 kap. 1 och 2 §§ dataskyddslagen[3] där det görs hänvisningar till lag, författning och beslut som meddelats med stöd av lag eller författning som rättsliga grunder för personuppgiftsbehandling.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] Artikel 6.3 i dataskyddsförordningen.
[3] Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Ändamålsbegränsning och finalitetsprincipen

En av de grundläggande principerna för behandling av personuppgifter är principen om ändamålsbegränsning (finalitetsprincipen). Den innebär att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålet med en personuppgiftsbehandling sätter ramarna för behandlingen och personuppgifterna får senare inte behandlas för något ändamål som är oförenligt med ursprungsändamålet.[4] Det måste alltid finnas minst ett ändamål med all personuppgiftsbehandling. Att personuppgifter inte får vidarebehandlas på ett sätt som är oförenligt med de ändamål för vilka de samlats in innebär att vidarebehandling för ändamål som *är* förenliga med insamlingsändamålet som utgångspunkt är tillåten. I enlighet med den så kallade ansvarsprincipen är det den personuppgiftsansvarige som ska göra prövningen av om personuppgiftsbehandlingen är förenliga med de ursprungliga ändamålen.[5] Vidarebehandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål anses inte oförenlig med ursprungsändamålen förutsatt att behandlingen omfattas av lämpliga skyddsåtgärder.[6]

För att avgöra om en behandling är förenlig med ursprungsändamålet ska hänsyn bland annat tas till ett antal kriterier. Dessa kriterier är kopplingar mellan ändamålen (a), sammanhanget inom vilket uppgifterna samlades in, särskilt förhållandet mellan den personuppgiftsansvarige och den registrerade (b), personuppgifternas art (c), eventuella konsekvenser för den registrerade (d) och förekomsten av skyddsåtgärder så som pseudonymisering och kryptering (e).[7] EU-domstolen har ansett att dessa kriterier ger uttryck för behovet av ett konkret, logiskt och tillräckligt nära samband mellan ursprungsändamålet och den senare behandlingen av personuppgifterna.[8] När det gäller om en vidarebehandling kan anses tillåten eller inte har Integritetsskyddsmyndigheten (IMY) uttryckt att förekomsten av olika skyddsåtgärder, särskilt integritetsfrämjande teknik, är en viktig åtgärd i bedömningen av om en vidarebehandling kan anses tillåten eller inte. IMY har inom ramen för sin inno-

[4] Artikel 5.1 i dataskyddsförordningen.
[5] Artikel 5.2 i dataskyddsförordningen.
[6] Artikel 5.1 b och artikel 89.1 i dataskyddsförordningen.
[7] Artikel 6.4 i dataskyddsförordningen.
[8] Domstolens dom av den 20 oktober 2022, Digi Távközlési és Szolgáltató Kft. mot Nemzeti Adatvédelmi és Információszabadság Hatóság, C-77/21, EU:C:2022:805, p. 34.

vationssandlåda för dataskydd genomfört ett projekt som visar att förutsättningarna för att vidarebehandla personuppgifter för att skapa syntetiska data i syfte att träna en AI-modell är större än förutsättningarna för att direkt använda personuppgifter som träningsdata.[9]

Som en generell utgångspunkt bör ett utlämnande av en uppgift till en annan myndighet, i syfte att uppgiften ska användas i en helt annan verksamhet än den som den samlades in till, utgöra en behandling som är oförenlig med insamlingsändamålet.[10]

Tillåten vidarebehandling för oförenliga ändamål

För det fall det nya ändamålet anses oförenligt med det ursprungliga, får personuppgifterna endast vidarebehandlas om den registrerade har samtyckt till vidarebehandlingen eller om behandlingen grundar sig på unionsrätt eller nationell rätt som utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1. Detta innebär att dataskyddsförordningen ger utrymme för att i nationell rätt föreskriva att ytterligare behandling av personuppgifter får ske, även om vidarebehandlingen inte är förenlig med de eller det ändamål för vilket uppgifterna samlades in.

Det finns två slags bestämmelser som innebär att uppgifter som har samlats in för ett ändamål i en verksamhet får eller ska behandlas för ett annat ändamål i en annan verksamhet. Det kan vara fråga om uppgiftsskyldigheter som regleras utanför offentlighets- och sekretesslagen (att uppgifter ska vidarebehandlas genom utlämnande till en annan myndighet) eller det kan vara fråga om sekretessbrytande bestämmelser i offentlighets- och sekretesslagen (att uppgifter får vidarebehandlas genom utlämnande till en annan myndighet). Sådana bestämmelser kan i vissa fall utgöra en tillämpning av finalitetsprincipen, det vill säga att lagstiftaren har gjort bedömningen att den tillkommande behandlingen är förenlig med insamlingsändamålet. I de flesta fall bör dock sekretessbrytande bestämmelser ge uttryck för lagstiftarens ställningstagande om att vidarebehandling

[9] Integritetsskyddsmyndigheten (IMY), IMY-2025-23536, *Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell*, s. 3 och 15.
[10] SOU 2025:45 *Ökat informationsutbyte mellan myndigheter – några anslutande frågor*, s. 103.

genom utlämnande är nödvändigt och proportionerligt för att säkerställa ett viktigt mål av allmänt intresse.[11]

7.2.2 Närmare om sekretess och sekretessbrytande bestämmelser

Sekretess som kan begränsa datadelning inom den offentliga förvaltningen

Inom den offentliga förvaltningen gäller sekretess och tystnadsplikt i olika omfattning för de datamängder som de olika aktörerna förfogar över. Om uppgifter finns hos aktörer som inte omfattas av offentlighets- och sekretesslagen, som till exempel enskilt bedriven verksamhet inom hälso- och sjukvård och socialtjänst, kan tystnadsplikt framgå av andra regelverk.[12]

En uppgift för vilken sekretess eller tystnadsplikt gäller får som utgångspunkt inte lämnas ut. Bestämmelser om sekretess till skydd för uppgift om enskildas personliga eller ekonomiska förhållanden finns i 21–40 kap. OSL. I 15–18 kap. OSL finns också bestämmelser om sekretess till skydd för allmänna intressen som till exempel sekretess till skydd främst för myndigheters verksamhet för inspektion, kontroll eller annan tillsyn (17 kap. OSL) och sekretess till skydd främst för intresset av att förebygga eller beivra brott (18 kap. OSL).

Sekretess och tystnadsplikt är i normala fall reglerad för ett avgränsat tillämpningsområde och gäller för vissa angivna uppgifter, i en viss typ av ärenden, i en viss typ av verksamhet eller hos en viss myndighet. Det innebär att förutsättningarna för att lämna ut uppgifter och dela data skiljer sig åt mellan olika aktörer inom den offentliga förvaltningen. Vad som gäller för respektive aktör redovisas inte närmare här.

[11] Jfr prop. 2024/25:180 *Ökat informationsutbyte mellan myndigheter*, s. 80.
[12] Se bland annat 6 kap. 12–16 §§ patientsäkerhetslagen (2010:659) och 17 kap. 11 och 12 §§ socialtjänstlagen (2025:400).

Sekretess som kan skydda uppgifter i samband med användning av teknikerna

Utöver de sekretessbestämmelser som kan begränsa rätten att dela data mellan olika offentliga aktörer, finns det också bestämmelser i offentlighets- och sekretesslagen som kan skydda uppgifter vid användning av integritetsfrämjande teknik. Dessa bestämmelser kan säkerställa ett skydd för själva bearbetningen med teknikerna. Bestämmelser som får anses särskilt relevanta för att skydda uppgifter i samband med användningen av integritetsfrämjande teknik redovisas närmare nedan.

Säkerhets- eller bevakningsåtgärd

I 18 kap. 8 § OSL finns bestämmelser om sekretess för olika brottsförebyggande åtgärder som i huvudsak hänför sig till annan verksamhet än polisens. Vissa av åtgärderna i bestämmelsen syftar endast indirekt till att förebygga brott. Sekretess gäller bland annat för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information.[13] Med system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka och distribuera information. Bestämmelsen används till exempel för att hålla uppgifter om säkerheten vid datorkommunikation hemliga, till exempel i ett allmänt datanät.[14]

Sekretess gäller också om åtgärden avser behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling.[15] Sekretessen gäller i första hand uppgifter om behörighetskoder och behörighetsnycklar samt arrangemang och fördelning av dessa. Bestämmelsen gäller inte bara behörighet avseende upptagningar som utgör hemliga, allmänna handlingar i tryckfrihetsför-

[13] 18 kap. 8 § första stycket 3 p. offentlighets- och sekretesslagen (2009:400), OSL.
[14] E. Lenberg, A. Tansjö & U. Geijer, *Offentlighets- och sekretesslagen* (5 december 2025, Version 32, JUNO), kommentaren till 18 kap. 8 §.
[15] 18 kap. 8 § första stycket 4. OSL.

ordningens mening, utan bestämmelsen gäller behörighet avseende alla typer av handlingar.[16]

Chiffer och kod

En annan bestämmelse som kan bli tillämplig vid användning av integritetsfrämjande teknik är 18 kap. 9 § OSL. Enligt bestämmelsen gäller sekretess för uppgift som lämnar eller kan bidra till upplysning om chiffer, kod eller liknande metod om det kan antas att syftet med metoden motverkas om uppgiften röjs och metoden har till syfte att underlätta befordran eller användning i allmän verksamhet av uppgifter utan att föreskriven sekretess åsidosätts. Om exempelvis uppgifter som omfattas av sekretess pseudonymiseras eller krypteras, skyddas således också kodnyckeln av sekretess. Omfattas uppgifterna däremot inte av sekretess, omfattas inte heller kodnyckeln av sekretess.[17]

Bestämmelsen syftar till att skydda hemliga uppgifter i allmän verksamhet även om de är sekretesskyddade med hänsyn till något annat intresse som avses i 2 kap. 2 § tryckfrihetsförordningen, TF.[18] Sekretessen i 18 kap. 9 § OSL gäller endast om ett röjande av uppgiften kan antas motverka syftet med chiffret, det vill säga att slå vakt om sekretessen i allmän verksamhet. Sekretessen är begränsad genom ett rakt skaderekvisit. Presumtionen vid en sekretessprövning är därmed offentlighet.

Teknisk bearbetning och teknisk lagring

I 40 kap. 5 § OSL regleras sekretess hos myndigheter som enbart tekniskt bearbetar eller tekniskt lagrar uppgifter för annans räkning. Av bestämmelsen framgår att sekretessen gäller för uppgift om en enskilds personliga eller ekonomiska förhållanden.[19]

Handlingar som förvaras hos en myndighet för enbart teknisk bearbetning eller teknisk lagring är enligt 2 kap. 10 § TF inte allmänna. Sekretessen enligt 40 kap. 5 § OSL är därför en tystnads-

[16] *Offentlighets- och sekretesslagen* (Version 32, JUNO), kommentaren till 18 kap. 8 § OSL.
[17] S., Öman, *Dataskyddsförordningen* (11 september 2025, Version 3A, JUNO), kommentaren till artikel 4.5.
[18] Prop. 1979/80:2 *med förslag till sekretesslag m.m.,* Del A s. 143.
[19] 40 kap. 5 § OSL.

pliktsbestämmelse för de som har tillgång till uppgifterna. Bestämmelsen omfattar teknisk bearbetning och teknisk lagring för annans räkning av uppgifter om enskilda generellt, det vill säga inte bara personuppgifter. Eftersom föremålet för sekretessen är uppgifter om en enskilds personliga eller ekonomiska förhållanden skyddas även juridiska personers ekonomiska förhållanden.[20]

Verksamhet som omfattar teknisk bearbetning och teknisk lagring har ett nära samband med utvecklingen av en digital offentlig förvaltning och myndighetssamverkan avseende it-drift. När en myndighet tillhandahåller it-baserade funktioner åt andra myndigheter och behandlar uppgifter för dessa myndigheters räkning kan det i praktiken innebära en form av utkontraktering. Sekretessen gäller hos en myndighet såväl då det är fråga om teknisk bearbetning eller teknisk lagring för enskildas räkning som då det gäller teknisk bearbetning eller teknisk lagring för en annan myndighets räkning. När det gäller utkontraktering till en annan myndighet kan också andra sekretessbestämmelser vara tillämpliga. I sådana situationer blir det den regel som resulterar i att uppgifterna bedöms vara sekretessbelagda som ska gälla i det särskilda fallet.[21] Eftersom sekretessen enligt bestämmelsen är absolut blir det i praktiken bara denna paragraf som tillämpas.[22]

En myndighet hos vilken sekretess gäller får givetvis lämna ut uppgifter till uppdragsgivare och till andra i enlighet med myndighetens åtaganden enligt uppdraget. Det ska här noteras att det inte finns någon rätt för myndigheten eller dess personal att vid sidan av ingångna överenskommelser lämna ut sådana uppgifter.[23] Sekretessen är undantagen såväl tillämpningsområdet för generalklausulen i 10 kap. 27 § OSL som den nya sekretessbrytande generella bestämmelsen i 10 kap. 15 a § OSL.

Får en myndighet en uppgift från en annan myndighet enbart för teknisk bearbetning eller teknisk lagring och uppgiften är sekretessreglerad av hänsyn till ett allmänt intresse hos den utlämnande myndigheten, blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten.[24] Den tystnadsplikt som överförs är den

[20] Prop. 2016/17:198 *Utökat sekretesskydd i verksamhet för teknisk bearbetning och lagring,* s. 28.
[21] Jfr 7 kap. 3 § OSL.
[22] Se *Offentlighets- och sekretesslagen* (Version 32, JUNO), kommentaren till 40 kap. 5 § OSL.
[23] Prop. 1979/80:2 Del A s. 273.
[24] 11 kap. 4 a § OSL.

som följer av sekretessbestämmelser till skydd för allmänna intressen (15–20 kap. OSL).

Sekretessbrytande bestämmelser

Möjligheten att utbyta uppgifter utgör en viktig förutsättning för att olika offentliga aktörer ska kunna fullgöra sina uppdrag och för en fungerande samverkan i övrigt. Det har därför införts ett flertal sekretessbrytande bestämmelser i offentlighets- och sekretesslagen och uppgiftsskyldigheter i andra författningar. Några av de sekretessbrytande bestämmelser som kan anses relevanta i sammanhanget redovisas nedan.

Nödvändigt uppgiftsutlämnande

Enligt 10 kap. 2 § OSL hindrar inte sekretess att en myndighet lämnar ut en uppgift om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sitt uppdrag. Bestämmelsen ska tolkas restriktivt och avsikten är inte att man enbart av effektivitetsskäl ska kunna bryta sekretessen.[25]

Generalklausulen

I 10 kap. 27 § OSL finns den så kallade generalklausulen som innebär att sekretess inte hindrar att uppgifter lämnas till en annan myndighet om det är uppenbart att intresset av att uppgifterna lämnas har företräde framför det intresse som sekretessen ska skydda. Syftet med generalklausulen är att den ska utgöra en ventil för det fall ett utbyte av uppgifter uppenbart behöver ske och situationen inte har kunnat förutses i lagstiftningen.

En förutsättning för att generalklausulen ska vara tillämplig är att det inte finns en specialreglering av uppgiftslämnandet i fråga i annan lag eller förordning. Det innebär att bestämmelsen är subsidiär i förhållande till andra sekretessbrytande bestämmelser. Har det till exempel föreskrivits att en viss myndighet kan ta del av annars sekretessbelagda uppgifter hos en annan myndighet genom angivna

[25] *Offentlighets- och sekretesslagen* (Version 32, JUNO), kommentaren till 10 kap. 2 §.

villkor, är det inte aktuellt att lämna ut uppgifterna med stöd av generalklausulen om de angivna villkoren inte är uppfyllda.[26]

Viss sekretess är också undantagen från bestämmelsen tillämpningsområde.

Uppgiftsskyldighet

Enligt 10 kap. 28 § OSL hindrar inte sekretess att en uppgift lämnas till en annan myndighet, om det finns en uppgiftsskyldighet som följer av lag eller förordning. Sekretessbrytande uppgiftsskyldigheter bygger som utgångspunkt på överväganden om vilket sekretesskydd uppgiften har hos den utlämnande myndigheten och huruvida den mottagande myndighetens behov generellt sett kan anses väga tyngre än det intresse som sekretessen skyddar. Bestämmelser om uppgiftsskyldighet mellan myndigheter är alltså ett sätt för lagstiftaren att reglera ett ofta förekommande informationsutbyte och säkerställa att en verksamhet får tillgång till de uppgifter som behövs i den mottagande myndighetens verksamhet. Om en myndighet enligt lag eller förordning är skyldig att lämna uppgifter till en annan myndighet bryts således sekretesskyddet med stöd av 10 kap. 28 § OSL.[27]

Teknisk bearbetning och teknisk lagring

Sekretess hindrar inte att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften. Det krävs dock att det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Detta framgår av 10 kap. 2 a § OSL.

Ett uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifter kan exempelvis bestå i att införa, förvalta, utveckla och så småningom avveckla en it-driftstjänst. Under dessa olika faser kan en mängd olika åtgärder behöva vidtas för att upprätthålla den tillgänglighet, funktionalitet och prestanda i tjänsten som har avtalats mellan par-

[26] Prop. 1979/80:2 Del A s. 328.
[27] Det finns bestämmelser som anger att bl.a. 10 kap. 28 § första stycket OSL inte ska tillämpas i vissa fall. Det gäller bl.a. uppgifter som erhållits genom internationella avtal och som är sekretessbelagda enligt 15 kap. 1 a §, 27 kap. 5 § eller 34 kap. 4 § OSL.

terna. Det kan röra sig om förändring och tillägg i en befintlig tjänsts funktionalitet, etablering av en tilläggstjänst, integration med andra tjänster, konfiguration, test och utveckling samt tillhandahållande av supporttjänster. Det kan också röra sig om säkerhetstester och andra säkerhetshöjande åtgärder som uppgradering, uppdatering, säkerhetskopiering, kryptering, anonymisering, pseudonymisering och incidenthantering. Vid avveckling av en tjänst kan myndighetens uppgifter behöva migreras eller exporteras tillbaka till myndigheten eller till en annan uppdragstagare. Vilka slags åtgärder som kan omfattas av uttrycket teknisk bearbetning eller teknisk lagring kan komma att förändras över tid med anledning av den tekniska utvecklingen.[28]

Att det ska vara fråga om endast teknisk bearbetning eller teknisk lagring hindrar inte att personal hos uppdragstagaren tar del av de uppgifter som hanteras för den uppdragsgivande myndighetens räkning. Det kan vara nödvändigt för att personalen ska kunna utföra sina arbetsuppgifter som ett led i den tekniska bearbetningen eller tekniska lagringen. Främst handlar det om drifts- och säkerhetsrelaterad information, exempelvis uppgifter om användarkonton, loggar, krypteringsnycklar, lösenord och säkerhetsinställningar. Det kan också röra sig om andra uppgifter i läsbar form.[29]

En uppgift får inte lämnas ut om det med hänsyn till omständigheterna är olämpligt. Det innebär att en myndighet, innan en uppgift lämnas ut, ska pröva om det finns skäl som talar emot att uppgiften lämnas ut. Omständigheter som kan ha betydelse är exempelvis vilken typ av uppgifter det rör sig om, vilka intressen som ligger till grund för sekretessen och uppgifternas omfattning. En omständighet som med viss tyngd kan tala emot ett utlämnande är att det är fråga om uppgifter av särskilt känsligt slag, exempelvis uppgifter av synnerlig betydelse för rikets säkerhet när det gäller totalförsvaret. Det bör också beaktas vilka åtgärder som uppgiftsmottagaren vidtar för att skydda uppgifterna och om denne omfattas av en lag- eller avtalsreglerad tystnadsplikt. Även avtalsförhållandet mellan parterna ska beaktas och då i synnerhet sådana avtalsvillkor som riskerar att frånta den utlämnande myndigheten kontrollen över uppgifterna.[30]

[28] Prop. 2022/23:97 *Sekretessgenombrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter*, s. 17.
[29] Prop. 2022/23:97 s. 17 och jfr prop. 1975/76:160 *om nya grundlagsbestämmelser angående allmänna handlingars offentlighet*, s. 87.
[30] Prop. 2022/23:97 s. 17.

Uppgift om enskilds personliga eller ekonomiska förhållanden

Den 1 december 2025 trädde en ny generellt sekretessbrytande bestämmelse i kraft, 10 kap. 15 a § OSL. Bestämmelsen möjliggör för myndigheter att under vissa förutsättningar lämna uppgifter om enskilda till andra myndigheter. Bestämmelsen bryter viss sekretess till skydd för enskilds personliga eller ekonomiska förhållanden som regleras i 21–40 kap. OSL om det behövs för vissa angivna syften. En uppgift får dock inte lämnas om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Från bestämmelsens tillämpningsområde undantas viss sekretess. Det gäller till exempel sekretess i verksamhet som avser förande av eller uttag ur en forskningsdatabas, sekretess i verksamhet som avser statistik, viss närmare angiven hälso- och sjukvårdssekretess och sekretess i samband med lagring och teknisk bearbetning för någon annans räkning.

En uppgift får lämnas om det behövs för något av de i bestämmelsen angivna syftena och får lämnas av en myndighet till en annan myndighet såväl på eget initiativ som efter begäran från den mottagande myndigheten. De syften som anges är om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet samt för att utreda brott. En uppgift får också lämnas ut om det behövs för att förebygga eller förhindra att en ekonomisk förmån, ett ekonomiskt stöd, en skatt eller en avgift beslutas, betalas ut eller tillgodoräknas felaktigt eller med ett för högt eller ett för lågt belopp. Vidare får en uppgift lämnas ut om det behövs för att upptäcka eller utreda redan inträffade felaktigheter avseende sådana utbetalningar och tillgodoräknanden. En uppgift får också lämnas ut om det behövs för att förebygga, förhindra, upptäcka eller utreda fusk och överträdelser av regler, villkor i beslut eller avtal.

7.2.3 Förhållandet mellan teknikerna, dataskyddsregelverket och offentlighets- och sekretessreglerna

När det gäller avidentifieringstekniker som innebär att identifierande uppgifter förändras på ett oåterkalleligt sätt är det viktigt att skilja mellan den åtgärd som leder fram till själva avidentifieringen och hur resultatet efter bearbetningen hanteras. Behandlingen som leder fram till en avidentifiering faller in under dataskyddsregleringen,

eftersom det där sker en behandling av personuppgifter. Finns det inga personuppgifter kvar efter bearbetningen och det inte heller går att återskapa uppgifterna anses de inte längre vara personuppgifter. Därmed faller en efterföljande delning utanför tillämpningsområdet för dataskyddsförordningen. Det innebär också att delningen av data inte innebär något röjande av sekretessbelagda uppgifter om en enskilds personliga förhållanden i offentlighets- och sekretesslagens mening.

Om det i stället är fråga om uppgiftsminimerade tekniker eller om uppgifterna är bearbetade på ett sådant sätt att det hos mottagaren går att identifiera individer eller återskapa uppgifterna är det fråga om en behandling av personuppgifter även vid delningen. Vid delning av data som innebär ett utlämnande av personuppgifter faller alltså även den behandling som själva utlämnandet innebär in under dataskyddsregleringen. Det krävs då att det finns en rättslig grund för den vidarebehandling som ett utlämnande innebär. Det krävs också att uppgifterna som delas får lämnas ut enligt offentlighets- och sekretesslagen.

Till stöd för utlämnande av uppgifter finns bestämmelser i offentlighets- och sekretesslagen och i andra lagar och förordningar som den lagen hänvisar till. Den generella informationsskyldigheten i 6 kap. 5 § OSL är tillämplig när en myndighet begär att få ta del av uppgifter hos en annan myndighet. Även sekretessbrytande bestämmelser eller uppgiftsskyldigheter som anger att uppgifter får eller ska lämnas ut kan ge stöd för att lämna ut uppgifter, till exempel när uppgifter lämnas på eget initiativ. Bestämmelserna utgör då också den rättsliga grunden för den behandling av personuppgifter som sker. Dataskyddsregelverket och offentlighets- och sekretessreglerna samspelar alltså på så sätt att om det finns en skyldighet att lämna ut uppgifter, till exempel enligt 6 kap. 5 § OSL, utgör denna bestämmelse också en rättslig grund för den personuppgiftsbehandling som utlämnandet utgör.[31]

[31] Jfr SOU 2025:45, s. 101 f.

7.3 Det finns rättsliga förutsättningar att använda integritetsfrämjande teknik

7.3.1 Teknikerna kan förbättra datadelningen inom befintliga rättsliga ramar

Utredningens bedömning

Integritetsfrämjande teknik kan bidra till en ökad och säkrare datadelning inom befintliga rättsliga ramar även med beaktande av de begränsningar som finns i form av sekretess.

Teknikerna ger i sig inte någon rätt att dela data. Förutsättningar och stöd för den offentliga förvaltningen att dela uppgifter finns bland annat i offentlighets- och sekretesslagen.

Skälen för utredningens bedömning

Teknikerna kan bidra till en förbättrad datadelning inom befintliga rättsliga ramar

I offentlighets- och sekretesslagen finns bestämmelser om sekretess som begränsar möjligheterna att dela data. Integritetsfrämjande teknik kan dock göra delning av data möjlig utan att underliggande personuppgifter eller andra skyddsvärda uppgifter röjs. Det innebär att datadelning som av integritetsskäl annars inte hade varit tillåten kan göras möjlig med bibehållet skydd för enskilda. Som exempel kan nämnas att säker flerpartsberäkning kan möjliggöra att flera aktörer genomför gemensamma bearbetningar på sina respektive datamängder utan att underliggande uppgifter delas. I stället krypteras uppgifterna hos avsändaren och bearbetas i krypterad form. Ett annat exempel är federerad inlärning som är en metod som möjliggör gemensam modellträning utan att underliggande träningsdata delas.

Integritetsfrämjande teknik utgör alltså ett nytt sätt att dela data genom att insikter delas i stället för de underliggande uppgifterna. Teknikerna kan på så vis bidra till en modern datadelning inom befintliga rättsliga ramar även med beaktande av de begränsningar som finns i form av sekretess.

Teknikerna ger inte i sig någon rätt att dela data utan datadelningen måste ha stöd i rättsordningen

Vid all förvaltningsverksamhet får en myndighet endast vidta åtgärder som har stöd i rättsordningen. Det krävs alltså någon form av normmässig förankring för all typ av verksamhet som en myndighet bedriver.[32] Det gäller generellt, det vill säga även för informationshantering och datadelning. Användningen av integritetsfrämjande teknik ger inte i sig något stöd för den offentliga förvaltningen att dela data utan tar sikte på hur data kan bearbetas och delas.

Myndigheternas verksamhet styrs enligt legalitetsprincipen av de föreskrifter om arbetsuppgifterna som lagstiftaren eller någon annan normgivare har meddelat. Myndigheter har också en skyldighet att samarbeta och bistå varandra vilket bland annat kommer till uttryck i 8 § första stycket förvaltningslagen (2017:900) där det anges att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter. Formerna för myndigheternas samverkan kan vara av många olika slag och variera med hänsyn till ändamålet. Bestämmelsen om samverkan ger inte stöd för samverkan som faller utanför respektive myndighets verksamhetsområde. Syftet med samverkan mellan myndigheter är att den ska leda till att förvaltningen generellt ska bli så enhetlig och effektiv som möjligt.[33] Det finns även andra bestämmelser som anger att olika offentliga aktörer ska samverka eller samarbeta med varandra. Generella bestämmelser om samverkan eller samarbete innebär dock inte någon skyldighet att dela data.

Delning av data utgör samtidigt en viktig förutsättning för att olika offentliga aktörer ska kunna fullgöra sina uppdrag och för att samverkan mellan myndigheter ska fungera i övrigt. Bestämmelser om samverkansskyldighet kompletteras därför av den generella informationsskyldigheten i 6 kap. 5 § OSL som innebär att myndigheter ska dela vissa uppgifter med varandra. Bestämmelsen anses vara en precisering av den allmänna samverkansskyldighet och innebär att data, under vissa förutsättningar, ska delas på begäran av en annan myndighet.[34]

[32] Se 5 § förvaltningslagen (2017:900) och prop. 2016/17:180 *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 57 f.
[33] Prop. 2016/17:180 s. 70 f.
[34] Det ska noteras att det i SOU 2025:45 föreslås att en ny bestämmelse, 6 kap. 5 a § OSL införs. Förslaget innebär en ny rättslig grund när uppgifter lämnas ut på initiativ av den utlämnande myndigheten.

Detta innebär att även om integritetsfrämjande teknik i sig inte ger något stöd för den offentliga förvaltningen att dela data så finns det förutsättningar och stöd för att dela data i bland annat offentlighets- och sekretesslagen.

7.3.2 Integritetsfrämjande teknik utgör skyddsåtgärder

Utredningens bedömning

Den bearbetning av personuppgifter som sker med integritetsfrämjande teknik är en skyddsåtgärd som har till syfte att uppfylla kraven i dataskyddsförordningen.

Skälen för utredningens bedömning

Teknikerna utgör skyddsåtgärder som ska användas

I dataskyddsförordningen finns krav på att en personuppgiftsansvarig ska genomföra lämpliga tekniska och organisatoriska åtgärder som är utformade för ett effektivt genomförande av dataskyddsprinciper. I dataskyddsförordningen nämns pseudonymisering som en lämplig åtgärd.[35] Det ställs också krav på att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt, bland annat pseudonymisering och kryptering av personuppgifter.[36]

Europeiska dataskyddsstyrelsen (EDPB) har i ett utkast till riktlinjer angett att integritetsfrämjande teknik kan vara en lämplig skyddsåtgärd. I utkastet har syntetiska data och homomorf kryptering nämnts som exempel.[37] Även IMY har lyft fram att integritetsfrämjande teknik kan utgöra en teknisk skyddsåtgärd.[38]

Den behandling som bearbetningen med integritetsfrämjande teknik i sig innebär har som syfte att följa dataskyddsförordningen,

[35] Artikel 25.1 i dataskyddförordningen.
[36] Artikel 32 i dataskyddsförordningen.
[37] Europeiska dataskyddsstyrelsen (EDPB), *Guidelines 1/2026 on processing of personal data for scientific research purposes*, adopted version for public consultation, s. 65.
[38] Integritetsskyddsmyndigheten (IMY), IMY-2025-5444, *Betrodda exekveringsmiljöer för uppkopplade fordon*, s. 5, 13 och 23.

till exempel kan pseudonymisering användas för att uppfylla kraven på uppgiftsminimering. Bearbetningen utgör därför enligt utredningens bedömning en skyddsåtgärd.[39] Integritetsfrämjande teknik bör dock inte användas isolerat utan som ett komplement till andra skyddsåtgärder. De utgör därmed ett ytterligare skyddslager som kan minska risker i samband med datadelning, men ersätter inte behovet av exempelvis behörighetsstyrning, loggning och organisatoriska åtgärder.

Integritetsfrämjade teknik är ”den senaste utvecklingen”

I bedömningen av vad som är lämpliga skyddsåtgärder ska bland annat den senaste utvecklingen beaktas. Begreppet *den senaste utvecklingen (state of the art)* saknar definition i dataskyddsförordningen och det finns ingen vedertagen metod för att fastställa vad som är den senaste utvecklingen. EDPB har noterat att den kan ”fastställas mellan den tekniska nivån för ’den befintliga vetenskapliga kunskapen och forskningen’ och de mer etablerade ’allmänt accepterade tekniska reglerna’.”[40] Enligt EDPB är begreppet dynamiskt och behöver bedömas kontinuerligt i förhållande till den tekniska utvecklingen.

Utredningen bedömer att flera av de integritetsfrämjande teknikerna kan anses vara *den senaste utvecklingen*. Det gäller särskilt de tekniker som är tekniskt mogna för användning men som ännu inte används i någon större utsträckning, det vill säga differentiell integritet, syntetiska data och säker flerpartsberäkning. Det är tekniker som förekommit inom forskningen och i akademiska sammanhang under en längre tid men som ännu inte blivit etablerade som allmänt använda tekniker. Med hänsyn till kravet på att beakta den senaste utvecklingen vid val av skyddsåtgärder ska integritetsfrämjande teknik, när det är lämpligt, användas enligt dataskyddsförordningen.

[39] Jfr artikel 25.1 och artikel 32 i dataskyddsförordningen.
[40] Europeiska dataskyddsstyrelsen (EDBP), *Riktlinjer 4/2019 om artikel 25 Dataskydd som standard och inbyggt dataskydd*, version 2.0, s. 8 f.

7.3.3 Det måste finnas rättslig grund för att behandla personuppgifter vid användningen av teknikerna

Utredningens bedömning

Det måste finnas rättslig grund för behandlingen av personuppgifter i samband med användningen av integritetsfrämjande teknik. Det är det bakomliggande syftet med behandlingen som är avgörande för om behandlingen är tillåten eller inte.

Skälen för utredningens bedömning

När personuppgifter behandlas ska det finnas rättslig grund för behandlingen

All behandling av personuppgifter måste ha en rättslig grund och följa de principer som anges i dataskyddsförordningen. Behandling är ett brett begrepp och innefattar i princip allt som kan göras med personuppgifter. Till exempel kan man samla in, registrera, lagra, analysera, lämna ut eller radera dem.[41] Att tekniskt bearbeta personuppgifter för att framställa till exempel anonyma uppgifter eller syntetiska data utgör en personuppgiftsbehandling som måste leva upp till kraven i dataskyddsförordningen. Det är varje personuppgiftsansvarigs skyldighet att se till att endast sådan data som får behandlas inom verksamheten behandlas och att personuppgiftsbehandlingen är förenlig med det för aktören aktuella regelverket. Integritetsfrämjande teknik innebär inte att offentliga aktörer som saknar legitima skäl att behandla personuppgifter ges en rättslig möjlighet att göra det.

Det är också den personuppgiftsansvarige som ansvarar för att personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte vidarebehandlas för ändamål som är oförenliga med insamlingsändamålet. Om den behandling som sker när teknikerna används ryms inom den aktuella aktörens ändamål, behöver behandlingen inte ett eget ändamål. Bearbetningen med integritetsfrämjande teknik i sig kan då enligt vår mening inte anses vara oförenlig med de ändamål för vilka uppgifterna får behandlas.[42]

[41] Jfr artikel 4.2 i dataskyddsförordningen.
[42] Jfr *Dataskyddsförordningen* (Version 3A, JUNO), kommentaren till artikel 5.1b.

En datadelning som innebär ett utlämnande av personuppgifter i syfte att uppgiften ska användas i en helt annan verksamhet än den som den samlades in till, utgör vanligtvis en vidarebehandling som inte är förenlig med insamlingsändamålet. I svensk rätt föreskrivs tillåtligheten av vidarebehandling genom utlämnande i regel genom införandet av sekretessbrytande bestämmelser i offentlighets- och sekretesslagen eller uppgiftsskyldigheter i annan författning. Lagstiftaren har alltså genom bestämmelser om att uppgifter får eller ska lämnas ut tagit ställning till frågan om behandlingens förenlighet med finalitetsprincipen samt att lagstiftningen uppfyller ett mål av allmänt intresse och är proportionellt mot det legitima mål som eftersträvas. Bestämmelserna är då ett uttryck för att ett utlämnande är förenligt med insamlingsändamålet eller att en vidarebehandling genom utlämnande är tillåten, trots att den inte är förenlig med insamlingsändamålet. Detta innebär att sekretessbrytande bestämmelser eller uppgiftsskyldigheter som anger att uppgifter ska eller får lämnas ut, som till exempel 6 kap. 5 § och 10 kap. 15 § OSL, utgör den rättsliga grunden för den behandling av personuppgifter som sker vid ett utlämnande av uppgifter.

Det är det bakomliggande syftet med behandlingen som är avgörande för om behandlingen är tillåten eller inte

Integritetsfrämjande teknik kan göra delning av data möjlig utan att de underliggande personuppgifterna eller andra skyddsvärda uppgifter i data delas. Teknikerna kan också användas för att uppgiftsminimera när själva syftet med användningen är att begränsa mängden data som är avsedd att delas. Som exempel kan säker flerpartberäkning eller federerad inlärning nämnas, där flera aktörer kan genomföra gemensamma bearbetningar på sina respektive datamängder utan att behöva dela underliggande uppgifter med varandra vid själva bearbetningen. Däremot kan det finns skäl att dela resultatet som kan innehålla en begränsad mängd personuppgifter eller andra skyddsvärda uppgifter. Vid delning av resultatet kan då data som innehåller personuppgifter komma att lämnas ut. Även den behandling som själva utlämnandet innebär faller då in under dataskyddsregelverket och det krävs att det finns en rättslig grund för den vidarebehandling som ett utlämnande innebär. Det krävs också att

uppgifterna som delas får lämnas ut enligt offentlighets- och sekretesslagen.

Om integritetsfrämjande teknik används som en teknisk skyddsåtgärd för att möjliggöra eller säkra en redan laglig datadelning, och behandlingen sker för samma ändamål, omfattas den enligt utredningens mening av samma rättsliga grund. Det innebär att det är det bakomliggande syftet med behandlingen, det vill säga datadelningen som är avgörande för om bearbetningen genom integritetsfrämjande teknik är tillåten eller inte. Den behandling som en integritetsfrämjande teknik ger upphov till kan då anses rymmas inom den rättsliga grund som ligger till grund för datadelningen och är då endast ett verktyg för att antingen se till att inga personuppgifter delas eller för att uppfylla kraven på uppgiftsminimering. Det innebär att det undantag från principen om att uppgifter inte får vidarebehandlas för något ändamål som är oförenligt med insamlingsändamålet, vilket har införts genom sekretessbrytande bestämmelser och uppgiftsskyldigheter, även omfattar den bearbetning som sker med integritetsfrämjande teknik. Den bearbetning som sker är då nödvändig för att, med beaktande av principen om uppgiftsminimering, fullgöra en rättslig förpliktelse som myndigheten har eller nödvändig för att utföra en uppgift av allmänt intresse.

7.4 Det bör inte införas nya krav för användningen av integritetsfrämjande teknik

7.4.1 De krav som finns på att teknikerna ska användas är tillräckliga

Utredningens bedömning

Det bör inte införas några krav på att integritetsfrämjande teknik ska användas.

Skälen för utredningens bedömning

Att införa ett krav i nationell rätt om att integritetsfrämjande teknik ska användas, antingen generellt eller i specifika situationer, skulle kunna vara ett sätt att öka användningen av teknikerna i offentlig för-

valtning. Som framgår av avsnitt 2.4.3 innehåller dataskyddsförordningen bestämmelser om inbyggt dataskydd och dataskydd som standard. Genom bestämmelserna ställs krav på att datasystem utformas på ett sådant sätt att det säkerställs att behandlingen sker med iakttagande av bland annat principen om uppgiftsminimering.[43] Det framgår också att en personuppgiftsansvarig vid fastställandet av vilka medel som behandlingen utförs med och vid själva behandlingen ska genomföra lämpliga tekniska och organisatoriska åtgärder.[44] Dataskyddsförordningen ställer således redan krav på att offentliga aktörer ska vidta lämpliga skyddsåtgärder vid datadelning och integritetsfrämjande teknik är en sådan skyddsåtgärd. Precis som med alla skyddsåtgärder bör dock integritetsfrämjande teknik bara användas när det är motiverat utifrån den enskilda situationen.

Den offentliga förvaltningen har ett brett spann av datadelningar, med olika sorters uppgifter och olika syften. Detta är omständigheter som det är nödvändigt att ta hänsyn till vid valet av skyddsåtgärder. Det är också nödvändigt att ta hänsyn till vem som är mottagare av uppgifterna. Att införa generella krav på att integritetsfrämjande teknik alltid ska användas skulle därför kunna hämma den offentliga förvaltningens datadelning. Utredningen bedömer därför att det inte är ändamålsenligt att införa krav på användningen av integritetsfrämjande teknik i specifika situationer. Vad som är lämpliga skyddsåtgärder bör i stället bedömas i det enskilda fallet.

[43] Artikel 5.1 c i dataskyddsförordningen.
[44] Artikel 25.1 i dataskyddsförordningen.

7.4.2 Det behöver inte införas särskilda krav när teknikerna används

Utredningens bedömning

Det bör inte införas några särskilda krav vid användningen av integritetsfrämjande teknik i författning.

Skälen för utredningens bedömning

Det saknas skäl att införa särskilda krav vid användningen

Att införa särskilda krav vid användning integritetfrämjande teknik i samband med datadelning kan bidra till tydlighet och förutsägbarhet. Det kan i sin tur minska den osäkerhet som offentliga aktörer upplever gällande de rättsliga förutsättningarna. Sådana krav riskerar dock även att hämma teknikernas spridning och användning. Regleringar som innebär ytterligare administrativa eller tekniska bördor kan medföra att aktörer avstår från att implementera lösningar som annars skulle kunna möjliggöra datadelning eller stärka skyddet för den personliga integriteten.

Att tekniskt bearbeta personuppgifter genom integritetsfrämjande teknik utgör en personuppgiftsbehandling som måste leva upp till kraven i dataskyddsförordningen. Eftersom teknikerna utgör skyddsåtgärder omfattas datadelningen redan av de allmänna dataskyddsrättsliga kraven samt av de krav som i övrigt gäller för den offentliga förvaltningen, exempelvis avseende legalitet och proportionalitet. Att införa ytterligare särskilda krav vid användningen av dessa tekniker kan medföra att tröskeln för användning höjs. Detta gäller oavsett vilken typ av krav som skulle införas.

Att reglera hur teknikerna ska användas genom att införa generella krav vid användningen är också förenat med utmaningar, eftersom det på förhand är svårt att bedöma vilka krav som bör gälla i olika situationer. Utredningen bedömer därför att det inte bör införas några särskilda krav i samband med att teknikerna används. De befintliga krav som finns i dataskyddsförordningen är tillräckliga. Åtgärder för att minska osäkerheten vid användningen bör i stället vidtas inom ramen för uppdraget att ge stöd och vägledning om användning av integritetsfrämjande teknik (se avsnitt 8.3).

Nedan redogörs för de krav som har övervägts samt skälen till att utredningen bedömer att sådana krav inte bör införas.

Samråd vid användningen kan tillgodoses utan ny reglering

Ett möjligt krav att ställa hade varit att den offentliga förvaltningen ska samråda med vissa myndigheter när integritetsfrämjande teknik ska användas. IMY hade varit en naturlig part att samråda med för i princip alla tekniker och Nationella cybersäkerhetscentret (NCSC) vid Försvarets Radioanstalt (FRA) för tekniker som bygger på kryptografi. Det kan också finnas andra aktörer som skulle ha varit aktuella att ha ett sådant samrådskrav med.

Ett särskilt krav på att offentlig förvaltning ska samråda vid användningen av teknikerna riskerar enligt utredningens bedömning att bli allt för resurskrävande för de aktuella myndigheterna. Det finns också en risk för att ett sådant krav har en begränsande påverkan för användningen, till exempel genom väntetider vilket skulle kunna påverka myndigheternas effektivitet. Därtill kan nämnas att det redan i dag finns möjlighet att få vägledning av IMY i ett särskilt fall genom myndighetens innovationssandlåda för dataskydd. FRA har också i uppdrag att stödja användningen av kryptografi. Mot denna bakgrund konstaterar utredningen att det redan i dag finns viss möjlighet att få expertstöd i enskilda fall.

Kryptering ska användas när det är ändamålsenligt

Kryptering är en skyddsåtgärd som ofta omnämns och med vissa av teknikerna för skyddad bearbetning kan även bearbetningen av data ske under kryptering. Att kryptera data ger ett starkare skydd för informationen och den personliga integriteteten. Det motverkar också att data röjs i offentlighets- och sekretesslagens mening (se avsnitt 2.5.2). Ett möjligt krav hade därför kunnat vara att data alltid ska vara krypterat, även under bearbetning.

Att alltid kryptera data och att bearbeta den under kryptering är i dagsläget kostsamt och därför inte ändamålsenligt. Om den data som ska delas varken är integritetskänslig, omfattas av sekretess eller av annan anledning behöver skyddas särskilt saknas det skäl att i dagsläget använda kryptering annat än för själva överföringen.

På längre sikt kan ett sådant krav dock vara ändamålsenligt (se avsnitt 3.9.2).

Behov av enhetlig semantik kommer i tillräcklig utsträckning tillgodoses genom föreslagen föreskriftsrätt

För att integritetsfrämjande teknik ska kunna tillämpas på ett tillförlitligt sätt krävs att de datamängder som används uppvisar en hög grad av enhetlighet. Detta omfattar krav på gemensamma format, datastrukturer, begreppsdefinitioner och andra semantiska egenskaper. Utan sådan harmonisering finns en risk att analyserna leder till felaktiga eller missvisande resultat.

I lagen om interoperabilitetskrav för datadelning inom den offentliga förvaltningen[45] finns en föreskriftsrätt om interoperabilitetskrav vid datadelning, vilket bland annat omfattar semantik.[46] Lagen träder i kraft den 15 augusti 2026. Utredningens bedömning är att de behov av enhetlig semantik som finns vid användningen av integritetsfrämjande teknik kan tillgodoses inom ramen för föreskriftsrätten för interoperabilitetskrav vid datadelning. Det saknas därför skäl att för tillfället föreslå ytterligare krav om semantik.

Behov av ett rapporteringskrav kan tillgodoses utan krav i reglering

Det finns flera olika krav på transparens vid hantering av data, exempelvis i dataskyddsförordningen, AI-förordningen och dataförvaltningsförordningen. Ju mer data som tillgängliggörs för bearbetning desto fler kan dessa krav antas bli. I Nederländerna finns till exempel ett offentligt register, Algoritmeregistret, över de algoritmer som statliga och kommunala myndigheter använder i sina verksamheter. Syftet med registret är att stärka allmänhetens insyn i hur algoritmiskt beslutsstöd fungerar och tillämpas. Det är i dag frivilligt att anmäla algoritmer till registret men avsikten är att rapporteringen framöver ska bli obligatorisk.[47]

[45] Lagen beslutades den 11 juni 2026 men vid tryck av betänkandet hade lagen ännu inte fått ett SFS-nummer.
[46] Prop. 2025/26:244 Nya krav på interoperabilitet vid datadelning inom den offentliga förvaltningen, s. 38.
[47] https://algoritmes.overheid.nl/en (hämtad 2026-03-25).

Utredningen har övervägt om det bör införas ett krav på transparens vid användningen av integritetsfrämjande teknik, till exempel genom ett liknade register dit offentliga aktörer ska rapportera användningen av integritetsfrämjande teknik. Ett sådant register skulle dels ge enskilda en ökad insyn i vilka skyddsåtgärder som tillämpas vid behandlingen av deras personuppgifter, dels kunna fungera som inspiration för andra offentliga aktörer.

Med hänsyn till att det också finns andra krav på transparens så anser utredningen att det finns en risk för att ytterligare rapporteringskrav blir för administrativt betungande jämfört med den nytta som uppstår. Det är redan möjligt för enskilda att få insikt i hur deras personuppgifter hanteras genom de krav som ställs i dataskyddsförordningen. I den mån det finns behov av ytterligare krav på transparens bör det tas ett samlat grepp om de behoven för att undvika att kraven blir fragmenterade. Det skulle också säkerställa att ytterligare administrativa bördor blir så små som möjligt i förhållande till dess positiva effekter.

Att införa ett register med rapporteringskrav endast för att registret ska verka som inspiration för övriga delar av den offentliga förvaltningen är inte ändamålsenligt. En sådan inspiration kan uppnås på andra sätt. Vi anser därför i stället att det inom uppdraget att tillhandahålla stöd och vägledning bör ingå att informera om relevanta användningsfall inom förvaltningen (se avsnitt 8.3.3).

7.5 Tillräcklig avidentifiering eller kryptering med integritetsfrämjande teknik

Det finns en osäkerhet inom den offentliga förvaltningen när integritetsfrämjande teknik har använts i tillräcklig utsträckning (se avsnitt 6.4.2). För avidentifieringstekniker avser osäkerheten vad som krävs för att uppgifterna rättsligt ska anses vara anonyma hos mottagaren. Den rättsliga osäkerheten kan leda till att datadelning försvåras eller uteblir eftersom riskerna anses för stora hos antingen avsändare eller mottagare, eller hos båda parter. Det är också svårt att förutse om uppgifterna i ett senare skede kommer att begäras ut av en tredje part, antingen från avsändaren eller från mottagaren.

Det finns vidare en osäkerhet i den offentliga förvaltningen när uppgifter kan anses vara krypterade på ett sådant sätt att de inte

betraktas som röjda i offentlighets- och sekretesslagens mening. Denna osäkerhet grundar sig i att kryptering kan brytas och att det inte är klart under hur lång tid som risken för att krypteringen kan brytas ska bedömas, särskilt med hänsyn till utvecklingen av kvantdatorer.

7.5.1 Bedömning av om en fysisk person är identifierbar eller om krypterade uppgifter är röjda

Frågan om huruvida personuppgifter har avidentifierats i tillräcklig utsträckning för att anses som anonyma respektive om uppgifter är krypterade på ett sådant sätt att de inte röjs vid datadelning förutsätter en bedömning i det enskilda fallet. Bedömningen ska göras i förhållande till mottagaren. Det innebär att om mottagaren i det enskilda fallet inte kan identifiera personer i uppgiftsmängden är uppgifterna, för mottagaren, inte längre personuppgifter. Det framgår av dataskyddsförordningen och EU-domstolens praxis (se avsnitt 2.4.4). Motsvarande gäller för bedömningen om en uppgift kan anses röjd, det vill säga att en uppgift inte anses vara röjd enligt offentlighets- och sekretesslagen om uppgiften är krypterad på ett sådant sätt att mottagaren saknar teknisk kapacitet att forcera krypteringen.[48]

Rätt använt är integritetsfrämjande teknik ett kraftfullt verktyg för att avsevärt minska risken för oavsedd återidentifiering. Teknikerna utgör emellertid ingen garanti för att denna risk helt och hållet har uteslutits. Det är därför nödvändigt att göra en bedömning av om risken har reducerats till en nivå som är tillräckligt låg med hänsyn till de medel som rimligen kan komma att användas vid ett återidentifieringsförsök. Som stöd i en sådan bedömning av vidtagna avidentifieringsåtgärder kan till exempel attacktjänster användas (se även avsnitt 7.5.4).

Att det ska göras välgrundade och rimliga bedömningar följer bland annat av skäl 26 i dataskyddsförordningen där det framgår att alla hjälpmedel som rimligen kan komma att användas ska beaktas för att avgöra om en uppgift direkt eller indirekt kan identifiera en person. För att fastställa om ett hjälpmedel med rimlig sannolikhet kan komma att användas bör samtliga objektiva faktorer beaktas.

[48] Prop. 2022/23:97 s. 7.

Det kan röra sig om kostnader, tidsåtgång för identifiering, tillgänglig teknik vid tidpunkten för behandlingen och den tekniska utvecklingen. Det är enligt utredningens uppfattning rimligt att resonera på samma sätt när det gäller möjligheten att bryta en kryptering.

Vid bedömningen av om uppgifter är att betrakta som personuppgifter eller av om uppgifter är röjda är även den tid under vilken uppgifterna hanteras av betydelse. Om avidentifierade eller krypterade uppgifter hanteras under en begränsad tid minskar såväl risken för att skyddsåtgärderna kan motverkas som risken för att uppgifterna begärs ut av tredje man. Eftersom integritetsfrämjande teknik utgör skyddsåtgärder torde det sällan finnas behov av att bevara avidentifierade eller krypterade datamängder under längre tid, särskilt inte hos den aktör som lämnar ut uppgifterna. Denna aktör har redan tillgång till uppgifterna i deras ursprungliga form. Eventuell kompletterande information eller krypteringsnycklar bör dessutom gallras eller raderas när behovet av dem har upphört, förutsatt att det är förenligt med arkivlagstiftningen.

För den offentliga aktör som tar emot data finns det i regel skäl att bevara de avidentifierade uppgifter som har inkommit, medan det i regel bör saknas skäl att spara de uppgifter som bearbetats under kryptering efter att bearbetningen är färdig (se avsnitt 8.6.5). Någon bedömning av om kompletterande information eller krypteringsnycklar ska sparas bör därför inte aktualiseras hos mottagaren i dessa fall, eftersom det skulle motverka syftet med den vidtagna skyddsåtgärden att dela dessa med mottagaren.

7.5.2 Det bör förtydligas när vidtagna avidentifieringsåtgärder är tillräckliga

Utredningens bedömning

Det finns i dagsläget inte skäl eller utrymme inom ramen för uppdraget att föreslå rättsliga begränsningar gällande återidentifiering av avidentifierade uppgifter.

Den osäkerhet som finns inom offentlig förvaltning angående risken för återidentifiering bör i första hand avhjälpas genom stöd och vägledning.

Skälen för utredningens bedömning

Rättsliga begränsningar av möjligheten att återidentifiera delade uppgifter skulle kunna minska osäkerheten

Av EU-domstolens dom i mål C-582/14[49] framgår att en uppgift kan vara anonym om identifiering av den aktuella personen är förbjuden i lag. En reglering som hindrar återidentifiering hos mottagaren skulle därför kunna vara ett alternativ för att avhjälpa den osäkerhet som offentlig förvaltning upplever rörande tillräcklig avidentifiering. Att mottagaren saknar lagliga möjligheter att identifiera den registrerade skulle då kunna beaktas vid bedömningen av om de överförda uppgifterna utgör personuppgifter hos mottagaren och om vidtagna skyddsåtgärder kan anses tillräckliga. Detta skulle kunna öka förutsättningarna för datadelning.

Det bör i dagsläget inte införas ett generellt förbud mot återidentifiering

Ett förbud mot återidentifiering i författning har alltså betydelse vid bedömningen av när en datamängd ska anses innehålla personuppgifter hos en mottagande organisation. Det kan nämnas att det i dag finns en bestämmelse i svensk rätt som hindrar återidentifiering som gäller för uppgifter i den officiella statistiken.[50] Förbudet innebär att uppgifter i den officiella statistiken inte får sammanföras med andra uppgifter i syfte att utröna enskildas identiteter.

Utredningen bedömer att det i dagsläget inte finns tillräckliga skäl för att föreslå en reglering som generellt förbjuder återidentifiering av avidentifierade uppgifter. Inledningsvis kan det konstateras att det i dataskyddsregleringen föreligger rättsliga begränsningar redan i dag. För att en myndighet ska kunna vidta återidentifieringsåtgärder förutsätts enligt dataskyddsförordningen att det finns såväl en rättslig grund som ett berättigat ändamål för behandlingen, i annat fall saknas lagliga möjligheter att genomföra åtgärden.

[49] Domstolens dom av den 19 oktober 2016, Patrick Breyer/Förbundsrepubliken Tyskland, C-582/14, EU:C:2016:779. Se även domstolens dom av den 4 september 2025, Europeiska datatillsynsmannen mot Gemensamma resolutionsnämnden, C-413/23 P, EU:C:2025:645, p. 82.
[50] 6 § lagen (2001:99) om den officiella statistiken.

Det finns även invändningar av mer principiell och praktisk natur mot ett förslag om ett generellt återidentifieringsförbud. Ett förbud skulle riskera att hindra återidentifiering även i legitima och motiverade situationer vilket i sin tur skulle kräva ett flertal undantag, exempelvis för brottsutredande eller brottsförebyggande verksamhet. Ett förbud med omfattande undantag skulle därmed riskera att förlora sin avsedda effekt. I mål C-582/14 konstaterar EU-domstolen att även om det enligt tysk rätt inte var tillåtet att direkt överföra ytterligare upplysningar som behövdes för att identifiera en person så fanns det ändå, vid exempelvis en it-attack, lagliga möjligheter att erhålla sådan information via en behörig myndighet. Därmed fanns det hjälpmedel som rimligen kunde komma att användas för att identifiera någon och uppgifterna ansågs vara personuppgifter. Således kan möjligheten att via behöriga myndigheter lagligen få tillgång till kompletterande information innebära att identifiering ändå är möjlig, trots formella begränsningar. Motsvarande resonemang skulle kunna aktualiseras vid ett förbud som medger undantag för vissa ändamål. Det är enligt utredningens uppfattning dessutom svårt att på förhand överblicka och avgränsa vilka undantag som skulle behövas inom den offentliga förvaltningen.

Utredningen skulle dessutom, mot bakgrund av uppdragets avgränsning, endast kunna föreslå ett återidentifieringsförbud för uppgifter som delas inom offentlig förvaltning. Det är inte säkert att ett sådant förbud skulle få önskad effekt eftersom det inte träffar alla datadelningssituationer. Därtill har kommissionen lagt fram förslag på ändringar i dataskyddsförordningen (se avsnitt 2.4.4) som bör behandlas färdigt innan det kan bli aktuellt att överväga en nationell reglering.

Att införa en möjlighet att ställa upp förbehåll vid delning till andra myndigheter kräver en omfattande analys

Ett annat sätt att begränsa mottagarens möjligheter till återidentifiering är att införa en möjlighet att ställa upp ett förbehåll vid delningen liknande den möjlighet som myndigheter har i förhållande till enskilda enligt bestämmelsen i 10 kap. 14 § OSL. Förbehåll enligt bestämmelsen är avsedda att undanröja risken för skada eller men vid utlämnande av sekretessbelagda uppgifter och som utan ett för-

behåll inte hade kunnat lämnas ut.[51] Om en uppgift kan lämnas ut utan inskränkningar föreligger ingen sekretess. Någon möjlighet att ställa upp förbehåll finns då inte.[52]

När det gäller möjligheten att införa en ordning med förbehåll mellan myndigheter konstaterar utredningen att sådana, till skillnad från ett generellt förbud, skulle kunna utformas med hänsyn till omständigheterna i det enskilda fallet. Samtidigt aktualiserar en sådan ordning komplicerade förvaltningsrättsliga och offentligrättsliga frågor.

En myndighet är som utgångspunkt skyldig att lämna ut uppgifter till en annan myndighet om uppgiften inte är sekretessbelagd eller om utlämnandet följer av uppgiftsskyldighet enligt lag eller förordning.[53] Uppgiftsskyldigheten enligt 6 kap. 5 § OSL omfattar varje uppgift som myndigheten förfogar över. Den nuvarande regleringen är utformad efter lagstiftarens avvägning mellan sekretessintressen och behovet av datadelning. En ordning där enskilda myndigheter kan uppställa förbehåll vid ett utlämnande till andra myndigheter skulle kräva en reglering som inskränker mottagarens rätt att förfoga över inkomna handlingar. En sådan ordning skulle förutsätta noggranna överväganden om tillämpningsområde, adressater och förhållandet till offentlighetsprincipen samt sekretessbrytande bestämmelser. Utredningen bedömer att detta skulle kräva en betydligt mer omfattande analys än vad som ryms inom ramen för vårt uppdrag.

Andra åtgärder bör först vidtas

Utredningen anser att det finns starka skäl att förtydliga och undanröja den osäkerhet som finns vad gäller i vilken utsträckning vidtagna åtgärder är tillräckliga för att uppgifter inte längre ska kunna återidentifieras. Frågan är dock på vilket sätt detta bör ske och i vilken utsträckning det är motiverat eller möjligt att införa en ändamålsenlig reglering som förbjuder eller ger en möjlighet att begränsa återidentifiering hos en mottagande myndighet.

Utredningens sammantagna bedömning är att det i nuläget inte finns tillräckliga skäl eller är möjligt att inom ramen för vårt upp-

[51] Prop. 1979/80:2 Del A s. 349 f.
[52] Se bl.a. Kammarrätten i Stockholm mål nr 3363-19.
[53] 6 kap. 5 § OSL.

drag föreslå en reglering som förbjuder eller begränsar återidentifiering av avidentifierade uppgifter som delas inom offentlig förvaltning. Den osäkerhet som identifierats i fråga om tillräcklig avidentifiering bedöms i stället kunna minska genom de förslag som vi lämnar om stöd och vägledning (se vidare avsnitt 8.3.4). För det fall att våra föreslagna åtgärder inte får avsedd effekt kan det dock finnas skäl för regeringen att återkomma i frågan.

7.5.3 Det bör förtydligas när krypterade uppgifter anses röjda

Utredningens bedömning

Den osäkerhet som finns inom offentlig förvaltning angående risken för att sekretessbelagda uppgifter röjs vid användning av integritetsfrämjande teknik som bygger på kryptografi bör avhjälpas genom stöd och vägledning samt förvaltningsgemensamma tjänster.

Skälen för utredningens bedömning

När data krypteras görs det med hjälp av en krypteringsnyckel, som sedan kan användas för att dekryptera datamängden. En säker hantering av krypteringsnycklar är nödvändig för att minska risken för att krypteringen bryts. Det innefattar enligt utredningens mening bland annat att offentliga aktörer ska följa standarder för kryptografi och ha organisatoriska åtgärder på plats. De ska också säkerställa att krypteringsnycklar och krypterade datamängder inte bevaras under längre tid än vad som är nödvändigt.

Under den tid som krypteringsnycklar behöver bevaras kan dessa omfattas av sekretess. De sekretessbestämmelser som framför allt aktualiseras i en sådan situation är sekretess för säkerhets- eller bevakningsåtgärd eller för chiffer och kod (se avsnitt 7.2.2). Det bör dock i regel inte finnas behov av att bevara krypteringsnycklar under någon längre tid när data bearbetas med exempelvis säker flerpartsberäkning.

Utredningen bedömer att en begränsning av tiden för bevarande av krypterade data eller krypteringsnycklar minskar risken att krypteringen bryts. Det kan till exempel ske genom att myndigheter

säkerställer att dessa kan gallras när de inte längre behövs. I den mån offentliga aktörer ser att det finns en risk för att krypteringen bryts med kvantdatorer kan till exempel full homomorf kryptering användas eftersom den har bedömts vara kvantsäker.[54] De kryptografiska algoritmer som är sårbara för kvantdatorer är dock främst sådana som används mellan parter som använder asymmetrisk kryptering för att utbyta nycklar, eftersom de saknar upprättade kanaler för säker kommunikation.[55] Offentliga aktörer har möjlighet att använda säkra kommunikationslösningar för att utväxla nycklar varför även säker flerpartsberäkning och andra varianter av homomorf kryptering kan kvantsäkras med mindre komplexa metoder.

Med hänsyn till att dessa frågor är komplexa och kräver en hög kunskap bedömer utredningen att den offentliga förvaltningen behöver stöd och vägledning även i frågor som rör integritetsfrämjande teknik som möjliggör bearbetning av data under kryptering. Att erbjuda förvaltningsgemensamma tjänster för sådana tekniker kan också avhjälpa osäkerheten genom att säkerställa att krypteringen utförs på ett korrekt och säkert sätt.

7.5.4 Andra åtgärder som offentlig förvaltning kan vidta

Att använda standarder kan bidra till en ökad kvalitet och säkerhet samtidigt som tillförligheten ökar (se avsnitt 5.5). På motsvarande sätt kan en certifiering, exempelvis av en viss tjänst, visa att fastställda krav uppnås och på så vis utgöra en garanti för de som vill nyttja tjänsten. Det finns också tjänster som genomför attacktester mot avidentifierade data och kan användas för att utvärdera om avidentifieringsåtgärder har vidtagits i tillräckligt stor utsträckning.

Standarder och certifieringar som berör integritetsfrämjande teknik används inte i någon större utsträckning i dagsläget. Inte heller används attacktester i någon större utsträckning. Enligt utredningens uppfattning utgör standarder, certifieringar och attacktjänster verktyg som skulle kunna nyttjas av den offentliga förvaltningen i större utsträckning i syfte att minska osäkerheterna avseende

[54] https://digitalprivacy.ieee.org/publications/topics/types-of-homomorphic-encryption/ (hämtad 2026-04-24).
[55] Nationellt cybersäkerhetscenter vid FRA, 2026, *Rekommendationer för övergången till kvantsäker kryptografi*.

användningen av integritetsfrämjande teknik. Även ytterligare stöd och vägledning i dessa frågor kan bidra.

Certifiering för dataskydd

Dataskyddsförordningen innehåller bestämmelser om certifieringsmekanismer som ett sätt att stärka efterlevnaden och öka transparensen vid personuppgiftsbehandlingar. Enligt artiklarna 42 och 43 kan personuppgiftsansvariga och personuppgiftsbiträden välja att certifieras i förhållande till fastställda certifieringskriterier, bland annat avseende tekniska och organisatoriska skyddsåtgärder. EDPB har i sina riktlinjer för certifiering beskrivit att exempelvis säker inloggning är en behandlingsåtgärd som skulle kunna certifieras, om det finns en sådan godkänd certifieringsordning.[56] I Sverige prövar IMY certifieringsordningarnas kriterier, medan certifieringsorgan som utfärdar certifikat ska vara ackrediterade av Styrelsen för ackreditering och teknisk kontroll (Swedac). Certifiering kan också ske på EU-nivå och då prövar EDBP certifieringsordningens kriterier.

Även om ett certifikat i sig inte visar att en personuppgiftsbehandling lever upp till dataskyddsförordningens krav så visar det att personuppgiftsbehandlingen lever upp till kriterierna i en certifieringsordning. Eftersom dessa är godkända av IMY eller EDPB kan certifierade personuppgiftsbehandlingar anses omfattas av en hög nivå av dataskydd.[57] För personuppgiftsbiträden som regelbundet tillhandahåller tjänster, exempelvis levererar it-tjänster, har IMY framfört att det kan vara en konkurrensfördel att certifiera sig.[58]

Det finns ännu inte några svenska certifieringsorgan som är ackrediterade specifikt för certifiering enligt dataskyddsförordningen.[59]

[56] Europeiska dataskyddsstyrelsen (EDPB), *Riktlinjer 1/2018 om certifiering och fastställande av certifieringskriterier i enlighet med artiklarna 42 och 43 i förordningen*, version 3, s. 18.
[57] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/uppforandekoder-och-certifieringar/certifieringar/ (hämtad 2026-04-29).
[58] https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/uppforandekoder-och-certifieringar/certifieringar/ (hämtad 2026-05-11).
[59] https://www.swedac.se/tjanster/ackreditering/utveckling-av-nya-amnesomraden-for-ackreditering/ (hämtad 2026-04-29).

Utvärdering genom attacktester

Det finns i dag ett antal tjänster tillgängliga som open sourcelösningar som möjliggör testattacker mot avidentifierade data eller AI-modeller i syfte att bedöma risken för återidentifiering eller dataläckage.

Det resultat som erhålls efter attacktesterna ger den som har utfört avidentifieringsåtgärder, eller tränat en AI-modell, en uppfattning om hur stor risken för att någon annan kan återskapa personuppgifter är. Sådana attacktester utförs ofta tusentals gånger under optimala förhållanden där den som utför testattacken vanligtvis har tillgång till mer information om den avidentifierade datamängden eller den aktuella modellen än vad en faktisk angripare normalt kan förutsättas ha. Med hänsyn till antalet attacker och de optimala förutsättningarna kan det antas att några sådana försök alltid kommer att vara framgångsrika. Resultatet och de vidtagna åtgärderna kan trots det vara acceptabla. Ett sådant resultat visar nämligen att återskapande av personuppgifter förutsätter tillgång till omfattande information samt att ett stort antal försök krävs för att nå framgång. Det är förutsättningar som en utomstående i regel saknar. Resultatet kan således visa att risken för att enstaka försök att återskapa personuppgifter är låg, särskilt när försöken inte görs under optimala förhållanden.

Genom att använda attacktjänster kan den offentliga förvaltningen få en uppfattning om vidtagna avidentifieringsåtgärder faktiskt får avsedd effekt och därigenom minska den osäkerhet som råder. Det kan också vara användbart för att utvärdera de säkerhetsåtgärder som vidtagits för att minska riskerna med en personuppgiftsbehandling, till exempel i samband med en översyn av en konsekvensbedömning avseende dataskydd enligt artikel 35 i dataskyddsförordningen.

8 Förslag för att öka användningen av integritetsfrämjande teknik

8.1 Inledning

Utredningen anser att användningen av integritetsfrämjande teknik i förvaltningen bör öka. Vi anser också att det behövs flera åtgärder för att tillgodose de behov som vi har identifierat rörande användningen av integritetsfrämjande teknik i offentlig förvaltning.

I detta kapitel redovisas utredningens överväganden och förslag för att främja en ökad användning av teknikerna. Inledningsvis redovisas några grundläggande överväganden för våra förslag (avsnitt 8.2). Vi redovisar därefter våra förslag om hur stöd och vägledning till offentlig förvaltning bör styras och utformas (avsnitt 8.3). Därefter redogör vi för våra bedömningar och förslag avseende styrning och organisering av förvaltningsgemensamma tjänster för integritetsfrämjande teknik (avsnitt 8.4–8.6) samt andra förslag som kan främja användningen av integritetsfrämjande teknik (avsnitt 8.7).

8.2 Förslagen ska främja och stödja en ökad användning av integritetsfrämjande teknik

Utredningen bedömer att det främsta hindret för att öka användningen av integritetsfrämjande teknik i förvaltningen är bristande kunskap om teknikerna och vilka nyttor de bidrar med. Det gäller främst de moderna teknikerna. Vi anser även att avsaknaden av styrning av hur och när integritetsfrämjande teknik ska användas har bidragit till en osäkerhet i förvaltningen som ytterligare hindrar användning. Vissa integritetsfrämjande tekniker, särskilt moderna tekniker som bygger på kryptografi, kräver också tillgång till avancerade

tekniska lösningar. Detta kan också utgöra ett hinder mot användningen av teknikerna för offentliga aktörer.

Mot bakgrund av detta anser utredningen att det behövs åtgärder för att höja kunskapsnivån i offentlig förvaltning om integritetsfrämjande teknik och om hur teknikerna kan användas. Sådan kunskap är central för att sänka tröskeln för användning av teknikerna och för att stärka den offentliga förvaltningens förmåga att dela data. Olika typer av främjande och stödjande åtgärder är enligt vår uppfattning de mest lämpliga åtgärderna för att höja kunskapsnivån och skapa förutsättningar för ökad användning av integritetsfrämjande teknik i hela den offentliga förvaltningen.

8.2.1 Den privata marknadens kompetens bör tillvaratas

Den offentliga förvaltningens förmåga att utveckla och använda integritetsfrämjande teknik är beroende av tillgång till specialiserad teknisk kompetens. Denna kompetens finns i dag hos privata aktörer på den svenska och europeiska marknaden. Den offentliga förvaltningen bör därför så långt det är möjligt använda sig av kunskap och lösningar som finns hos eller utvecklas av privata aktörer. Att utgå från befintliga lösningar på den privata marknaden kan också bidra till ett mer kostnadseffektivt utvecklingsarbete. Privata aktörers kompetens och tjänster behöver därför användas på ett systematiskt och strategiskt sätt.

Privata aktörer kan bidra till ökad användning av integritetsfrämjande teknik i förvaltningen genom att tillhandahålla färdiga tekniska lösningar som är tillgängliga för upphandling. De privata aktörerna kan även bidra genom rådgivning, kompetensöverföring samt stöd i samband med införande, drift och vidareutveckling av sådan teknik. Vi anser därför att de olika uppdragen som vi föreslår behöver utföras med stöd av aktörer på den privata marknaden. Det är nödvändigt för att offentlig förvaltning ska kunna använda integritetsfrämjande teknik på ett effektivt, rättssäkert och ändamålsenligt sätt.

8.2.2 Styrningen bör vara långsiktig och flexibel

Utredningen bedömer att en förbättrad datadelning inom offentlig förvaltning kräver att det finns tydligare styrning för hur och när teknikerna ska användas. Regeringens styrning av integritetsfrämjande teknik är i dagsläget begränsad, exempelvis finns inga statliga myndigheter med ansvar och uppdrag som avser integritetsfrämjande teknik.

Utredningen anser vidare att det är viktigt att regeringens styrning av integritetsfrämjande teknik skapar långsiktiga förutsättningar för offentlig förvaltning. Det behövs för att offentliga aktörer ska kunna bygga upp kompetens avseende teknikerna, men även för att utforska möjliga användningsområden. En stor del av de potentiella ekonomiska nyttorna av teknikerna är också beroende av att regeringen och offentliga aktörer genomför åtgärder som sker systematiskt över tid.[1]

Regeringen behöver även använda styrmedel som innebär en viss flexibilitet eftersom den tekniska utvecklingen inom området går snabbt. Det är i dagsläget svårt att förutse framtida behov utifrån nya tekniker och nya användningsområden. Sammantaget innebär det att ansvar och uppdrag avseende integritetsfrämjande teknik behöver vara relativt långsiktiga och flexibla för att kunna anpassas i takt med förvaltningens behov och den tekniska utvecklingen.

Olika styrmedel har olika syften

Regeringens styrning av statliga myndigheter kan ske på olika sätt. Förordningsreglering genom myndigheters instruktioner är det huvudsakliga långsiktiga styrmedlet för regeringen att styra statliga myndigheter. Instruktioner bör dock inte innehålla alltför tidsbegränsade uppgifter eller mer utförliga uppgifter och uppdrag.[2] Regeringsuppdrag är ett mer flexibelt sätt för regeringen att styra myndigheter och ger regeringen möjlighet att tydliggöra och specificera styrningen.

Regeringsuppdrag kan både ges i regleringsbrev och som så kallade särskilda uppdrag. Regleringsbreven beslutas årsvis inför det nya

[1] Bilaga 2, *Samhällsekonomisk analys av potentialen för ökad användning av integritetsfrämjande teknik i offentlig förvaltning*, kapitel 7.
[2] Prop. 2009/10:175 *Offentlig förvaltning för demokrati, delaktighet och tillväxt*, s. 111.

budgetåret men kan trots detta innehålla uppdrag som redan initialt är avsedda att sträcka sig över flera år. Fördelen med att regleringsbrevet beslutas varje år är att uppdraget vid behov kan finjusteras utifrån eventuella nya förutsättningar som tillkommit. Regeringen kan också under året besluta om tilläggsändringar i regleringsbrev. Regleringsbrev används i regel för regeringens årliga och övergripande styrning av myndigheters löpande verksamhet. Särskilda uppdrag beslutas genom separata regeringsbeslut och används i regel för specifika och mer tillfälliga insatser som är avgränsade i tid och omfattning. Dessa uppdrag kan enbart justeras genom ett tilläggsuppdrag.

Myndigheters uppdrag kan även regleras genom författningsreglering, exempelvis i en särskild lag eller förordning. Sådana författningar skapar förutsättningar för en mer långsiktig styrning men är samtidigt mindre flexibla som styrmedel. Dessutom bör de endast införas när det finns ett tydligt och välmotiverat behov av dem.

8.2.3 Myndigheternas nuvarande ansvars- och expertområden bör beaktas

Integritetsfrämjande teknik berör flera myndigheters ansvarsområden och sträcker sig över flera sektorer och verksamheter. Beroende på den specifika tekniken finns också mer direkta beröringspunkter med vissa myndigheters expertområden, till exempel när det gäller tekniker som kan användas vid statistikframställning eller tekniker som bygger på kryptografi. Utredningen anser därför att styrningen och organiseringen för integritetsfrämjande teknik behöver omfatta flera myndigheter. Det är också mer effektivt att använda den samlade kompetensen som finns i förvaltningen i stället för att bygga upp ny kompetens hos en enskild aktör. Det kan vara särskilt svårt när det gäller specialistkompetens som ofta finns i begränsad omfattning. Samtidigt förutsätter detta att det finns fungerande strukturer för samverkan och samordning.

Det är centralt med tydliga roller och ansvar vid samverkan mellan flera myndigheter. Det kan till exempel handla om att en myndighet inom ramen för ett uppdrag får ett utpekat ansvar för samverkan. Ett sammanhållet ansvar underlättar exempelvis när flera myndigheter behöver tillhandahålla stöd och kunskapsspridning

inom offentlig förvaltning.[3] Även här är det viktigt med långsiktiga förutsättningar för myndigheterna att bygga upp dessa strukturer.[4]

Myndigheter med relevanta ansvars- och expertområden

För att utformningen av främjande och stödjande åtgärder ska bli så effektiv som möjligt bör myndigheters nuvarande ansvars- och expertområden beaktas i så stor utsträckning som möjligt. Utredningen anser att det finns ett antal myndigheter som är särskilt relevanta när det gäller att främja och stödja användningen av integritetsfrämjande teknik. Vi anser därför att dessa i första hand bör tilldelas olika ansvar och roller avseende integritetsfrämjande teknik. I följande avsnitt redogör vi kortfattat för dessa.

Försvarets radioanstalt

Försvarets radioanstalt (FRA) har till uppgift att upprätthålla kompetens för de nationella behoven inom kryptologi.[5] Inom myndigheten finns även det nationella cybersäkerhetscentret (NCSC) med uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. NCSC styrs av en egen förordning och har till uppgift att utgöra en nationell plattform för samverkan och informationsutbyte mellan aktörer, såväl privata som offentliga, i frågor som rör cybersäkerhet.[6] Ansvaret för frågor om informations- och cybersäkerhet vid Myndigheten för civilt försvar kommer den 1 juli 2026 överföras till NCSC. FRA har främst expertkunskap inom de tekniker som bygger på kryptografi.

[3] Statskontoret, OOS 49, *Att styra med kunskap – en studie om statlig kunskapsstyrning riktad till kommuner och regioner*, s. 37.
[4] Se t.ex. Statskontoret, OOS 44, *Regeringens styrning i tvärsektoriella frågor – en studie om erfarenheter och utvecklingsmöjligheter*, s. 53 f.
[5] 2 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt.
[6] 2 § förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY) har till uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter och att underlätta det fria flödet av sådana uppgifter inom EU. I myndighetens uppgifter ingår bland annat att följa, analysera och beskriva utvecklingen inom it-området avseende frågor som rör integritet och ny teknik. [7] Myndigheten är också tillsynsmyndighet enligt dataskyddsförordningen[8].

Myndigheten för digital förvaltning

Myndigheten för digital förvaltning (Digg) har till uppgift att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra offentlig förvaltning mer effektiv och ändamålsenlig.[9] Digg ansvarar även för den nationella digitala infrastrukturen Ena och merparten av de lösningar som ingår i Ena.

Myndigheten har vidare erfarenhet av vägledningsuppdrag, bland annat som samordnande och behörigt organ enligt dataförvaltningsförordningen. Inom ramen för uppdraget som behörigt organ har Digg tillsammans med Statistiska centralbyrån (SCB) publicerat en rättslig vägledning om skyddade data som innehåller information om anonymisering och pseudonymisering.[10] Digg ska dessutom ge vägledning till offentlig förvaltning i juridiska frågor inom ramen för den förvaltningsgemensamma digitaliseringen.[11]

Från och med den 1 januari 2027 kommer Diggs uppgifter att överföras och inordnas i Post- och telestyrelsen (PTS).[12] Regeringen har aviserat att myndigheten då ska byta namn till Digitaliseringsmyndigheten.[13]

[7] Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten.
[8] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[9] 1 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[10] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/vagledning-om-skyddade-data (hämtad 2026-03-12).
[11] 6 § 6 förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[12] Finansdepartementet, Fi2025/00654 Fi2025/02303, *Uppdrag till Post- och telestyrelsen att förbereda ett inordnande av Myndigheten för digital förvaltnings uppgifter*.
[13] https://www.regeringen.se/pressmeddelanden/2026/05/digg-och-pts-blir-digitaliseringsmyndigheten/ (hämtad 2026-05-18).

Statistiska centralbyrån

Statistiska centralbyrån (SCB) ansvarar för att utveckla, framställa och sprida officiell statistik och annan statlig statistik samt för att samordna systemet för den officiella statistiken.[14] Inom myndighetens verksamhet finns expertis om vissa avidentifieringstekniker, eftersom dessa ofta används inom statistikframställning. SCB är även behörigt organ för att tillhandahålla tekniskt stöd enligt dataförvaltningsförordningen. SCB har vidare, tillsammans med Digg, i uppdrag att inrätta en ny funktion som ska främja god datahantering inom offentlig förvaltning.[15]

8.3 Funktion för stöd och vägledning

8.3.1 Det behövs stöd och vägledning för att öka användningen

Utredningens bedömning

Stöd och vägledning är ett ändamålsenligt sätt att skapa ökad tydlighet och förutsägbarhet för användningen av integritetsfrämjande tekniker.

Skälen för utredningens bedömning

För att öka kunskapen om integritetsfrämjande teknik bedömer utredningen att det behövs ett utpekat ansvar för stöd och vägledning om teknikerna till offentlig förvaltning. En myndighet bör därför få i uppdrag att tillhandahålla en funktion för stöd och vägledning avseende integritetsfrämjande teknik.

Med vägledning menar vi insatser som syftar till att öka kunskapen och förmågan hos aktörerna själva så att de kan använda teknikerna på ett verksamhetsanpassat sätt. Det är också något som kan göras lättillgängligt för hela den offentliga förvaltningen. Utredningen ser samtidigt ett behov av att komplettera vägledning med ett mer verksamhetsnära och tillämpbart stöd, till exempel i form av metodstöd

[14] 1 § förordningen (2016:822) med instruktion för Statistiska centralbyrån.
[15] Finansdepartementet, Fi2026/00909, *Uppdrag till Myndigheten för digital förvaltning och Statistiska centralbyrån att förbereda inrättandet av en funktion för främjande av datahantering*.

och anpassade utbildningar (se vidare i avsnitt 8.3.3). Stödet bör dock inte utformas som rådgivning, som är mer av ett enskilt och situationsanpassat stöd. Behovet av teknisk och juridisk rådgivning avseende integritetsfrämjande teknik bör i stället tillgodoses av privata aktörer.

Vi anser att stöd och vägledning är ett mer ändamålsenligt sätt att skapa ökad tydlighet och förutsägbarhet för användningen av teknikerna, än att ställa olika typer av krav på att och hur teknikerna ska användas (se avsnitt 7.4). Skälet till det är bland annat att krav riskerar att höja i stället för att sänka tröskeln för användning av teknikerna, till exempel genom att bidra till ytterligare administrativa och tekniska bördor.

8.3.2 Digg får i uppdrag att tillhandahålla stöd och vägledning

Utredningens förslag

Myndigheten för digital förvaltning ska få i uppdrag att tillhandahålla stöd och vägledning om integritetfrämjande teknik till offentlig förvaltning.

Skälen för utredningens förslag

Diggs ansvar inom den förvaltningsgemensamma digitaliseringen gör myndigheten särskilt lämpad för uppdraget

Det är lämpligt att stöd och vägledning tillhandahålls av en myndighet vars nuvarande ansvars- och expertområden har ett myndighetsöverskridande perspektiv. Det bör också vara en myndighet som har vana av att tillhandahålla stöd och vägledning gentemot offentlig förvaltning.

Utredningen anser att Digg är mest lämpad att få det stödjande och vägledande uppdraget om integritetsfrämjande teknik. Digg har ansvaret för den förvaltningsgemensamma digitaliseringen och den nationella digitala infrastrukturen Ena. Diggs förvaltnings- och sektorsövergripande uppdrag inom digitalisering och datadelning innebär en fördel när det gäller att främja en bred användning av olika typer av integritetsfrämjande tekniker. Därutöver innebär Diggs roll

som behörigt organ enligt dataförvaltningsförordningen att myndigheten redan har uppgifter som omfattar att underlätta datadelning mellan olika aktörer, samtidigt som skyddet för personuppgifter ska säkerställas.

Digg har också erfarenhet av att ta fram vägledningar och på olika sätt stödja den offentliga förvaltningens digitalisering. Det innebär att myndigheten har upparbetade strukturer och kompetens för den typen av verksamhet. Det kan också nämnas att Digg, tillsammans med SCB, har i uppdrag att förbereda inrättandet av en funktion för främjande av datahantering vid SCB. Funktionen ska bland annat ge vägledning till offentliga aktörer för att skapa en god datahantering.[16]

Inom Ena har Digg uppbyggda strukturer för samarbete och kunskapsspridning för offentlig förvaltning. Digg kan vidare överväga att integrera stöd och vägledning för integritetsfrämjande teknik i Ena. Där tillhandahålls redan standarder och vägledning, bland annat för att öka den offentliga förvaltningens tillgängliggörande av data.[17] Utredningen anser sammanfattningsvis att det finns flera potentiella synergier mellan Diggs nuvarande uppgifter och det stödjande och vägledande uppdraget som vi föreslår.

Kommande sammanslagning med Post- och telestyrelsen ger stärkta förutsättningar

Utredningen bedömer att den kommande sammanslagningen mellan PTS och Digg kommer att skapa stärkta förutsättningar för en funktion för stöd och vägledning om integritetsfrämjande teknik. Ett skäl till det är att PTS har erfarenhet av främjande verksamhet, bland annat när det gäller tillgången till elektroniska kommunikationer och till bredband.[18] Erfarenheten kan bidra till att stärka det främjande arbetet för integritetsfrämjande teknik. PTS har också ett tillsynsansvar inom flera EU-regelverk, till exempel inom elektronisk identifiering och elektronisk kommunikation. Ansvaret ger ytterligare en fördel när det gäller att följa och påverka utvecklingen på EU-nivå som kan vara relaterad till integritetsfrämjande teknik. Regeringen har även i budgetpropositionen för 2026 aviserat medel

[16] *Uppdrag till Myndigheten för digital förvaltning och Statistiska centralbyrån att förbereda inrättandet av en funktion för främjande av datahantering*.
[17] Myndigheten för digital förvaltning (Digg), dnr 2024–4511, *Förslag till långsiktig utveckling och förvaltning av Ena*.
[18] Se förordning (2007:951) med instruktion för Post- och telestyrelsen.

till PTS under 2027 och 2028 (10 miljoner kronor årligen) för arbete med den offentliga förvaltningens datadelning enligt kommande lagstiftning om interoperabilitet.[19] De aviserade medlen kan även bidra till stärkta förutsättningar för stöd och vägledning avseende integritetsfrämjande teknik eftersom interoperabilitet underlättar användningen.

Det ska dock noteras att varken Digg eller PTS har den expertkompetens som i vissa fall behövs för att ge stöd och vägledning om integritetsfrämjande teknik, särskilt när det gäller vissa tekniker. Vi ser därför ett behov av att Digg samverkar med IMY samt vid behov med SCB och NCSC vid FRA. Genom sådan samverkan kan Digg få tillgång till den specialistkompetens som kan behövas för att ge stöd och vägledning om integritetsfrämjande teknik (se vidare i avsnitt 8.3.5).

Alternativa mottagare av uppdraget som har övervägts

Under utredningens arbete har vi övervägt om det finns skäl att ge det stödjande och vägledande uppdraget till andra myndigheter som har ansvarsområden som angränsar till integritetsfrämjande teknik (se avsnitt 8.2.3). Dessa myndigheter kan också ha delar av den kompetens som behövs för att ge stöd och vägledning om integritetsfrämjande teknik.

En sådan myndighet är IMY som bland annat ska följa utvecklingen när det gäller frågor som rör integritet och ny teknik. Det uppdrag som IMY har och den expertis som finns i myndigheten gäller dock integritetsskydd och inte datadelning. Att ge stöd och vägledning om hur datadelningen kan öka och om nyttorna med en ökad datadelning ligger därför inte i linje med IMY:s uppdrag. Utredningens uppfattning är också att det är ett praktiskt och konkret stöd som behövs, mot bakgrund av den begränsade kunskapen och kompetensen om teknikerna hos många offentliga aktörer. Vi ser att IMY:s tillsynsansvar skulle innebära vissa utmaningar när det gäller att ge mer konkret stöd och vägledning för tillämpningen av teknikerna. Det finns en risk för att myndighetens opartiskhet i samband med en efterföljande tillsyn skulle ifrågasättas.[20]

[19] Prop. 2025/26:1 *Budgetpropositionen för 2026*, utgiftsområde 22, s. 127.
[20] Jfr. Statskontoret, OOS 14, *Tänk till om tillsynen. Om utformningen av statlig tillsyn*.

Andra myndigheter som utredningen har övervägt är SCB och FRA. Båda dessa myndigheter har omfattande expertis om vissa integritetsfrämjande tekniker, men inte om alla typer av tekniker. Det skulle kunna medföra en risk för att vissa typer av integritetsfrämjande tekniker hamnar i förgrunden och prioriteras. Detta kan också göra att tyngdpunkten hamnar på ett visst användningsområde, snarare än att fokus ligger på den breda användningspotential som teknikerna har. Sammantaget bedömer vi att dessa myndigheter inte är lämpliga för att ensamma ansvara för uppdraget om stöd och vägledning om integritetsfrämjande teknik.

Vi har även övervägt om det är lämpligt att ge flera myndigheter ett delat ansvar för att tillhandahålla stöd och vägledning för integritetsfrämjande teknik inom deras respektive specialistområden. Utredningens anser dock att det behövs ett sammanhållet ansvar för dessa frågor. Ett sammanhållet ansvar gör det tydligt vilken myndighet som offentliga aktör ska vända sig till. Även Statskontoret har betonat vikten av att det inom tvärsektoriella områden finns en myndighet med ett utpekat ansvar för stöd och vägledning, eftersom det inom dessa områden kan finnas ett stort antal myndigheter som arbetar stödjande.[21]

8.3.3 Innehållet i uppdraget att ge stöd och vägledning

Utredningens förslag

Uppdraget bör omfatta samtliga integritetsfrämjande tekniker och anpassas utifrån förvaltningens behov. Stöd och vägledning bör också ges i frågor som rör val av teknik och kombination av olika tekniker.

Skälen för utredningens förslag

Uppdraget bör inte begränsas till enskilda tekniker

Vad som klassas som integritetsfrämjande teknik förändras i snabb takt. Utredningen bedömer därför att det stödjande och vägledande uppdraget generellt inte bör begränsas till enskilda tekniker utan

[21] Statskontoret, *Att styra med kunskap*, s. 37.

bör omfatta samtliga integritetsfrämjande tekniker. På så vis finns det en flexibilitet i uppdraget att följa den tekniska utvecklingen, även när det tillkommer nya tekniker. Det bör vara förvaltningens övergripande behov och den tekniska utvecklingen som i huvudsak bestämmer fokus och inriktning för det stödjande och vägledande uppdraget.

Under vissa perioder kan det finnas skäl att särskilt styra inriktningen för stöd och vägledning till vissa tekniker. Det kan ske inom ramen för det generella uppdraget. Utredningens uppfattning är att det inledningsvis finns ett sådant behov (se avsnitt 8.3.4).

Utformningen av stöd och vägledning bör anpassas utifrån förvaltningens behov

Det är viktigt att stöd och vägledning för teknikerna är tillräckligt konkret och tillämpbart för att möjliggöra en användning i praktiken. Det kan exempelvis vara aktuellt att ge stöd och vägledning på olika sätt beroende på vilken teknik det är fråga om och beroende på hur den offentliga förvaltningens behov ser ut. Som utredningen tidigare konstaterat utgör teknikerna inte en homogen grupp där behovet av kunskap ser likadant ut (se avsnitt 6.3.1). Det är därför viktigt att anpassa stödet utifrån den aktuella tekniken och förvaltningens övergripande behov.

Stöd och vägledning behöver även anpassas efter förvaltningens kunskap om de olika teknikerna. Det innebär att för etablerade avidentifieringstekniker är behovet av stöd inte lika stort som för moderna tekniker. Motsvarande gäller för vägledning, där det för etablerade avidentifieringstekniker redan finns sådana medan det saknas för moderna tekniker. För vissa tekniker behövs det mer generell, grundläggande kunskap medan det för andra tekniker kommer behövas mer detaljerad och tekniskt inriktad vägledning. Då kan det vara nödvändigt att tillhandahålla konkret metodstöd, till exempel med hänvisning till relevanta tekniska standarder. Som utredningen redovisat finns det redan en del tekniska standarder för integritetsfrämjande teknik, men inga rekommendationer från svenska myndigheter avseende vilka standarder som bör användas (se avsnitt 5.5.2). I uppdraget bör det även ingå att hänvisa till relevanta standarder för ledningssystem, till exempel för integritetsinformation. Därigenom kan de aktörer som använder tekni-

kerna få stöd i hur styrning, processer, system och dokumentation bör utformas för att till exempel säkerställa dataskyddet (se avsnitt 5.5.3). Digg bör även följa utvecklingen och beakta relevant forskning om integritetsfrämjande teknik för att kunna vidareutveckla sitt stöd.

Vid användande av integritetsfrämjande teknik uppstår ofta vissa rättsliga frågor. För en del tekniker kommer behovet av rättslig vägledning att vara stort. I sådana fall är det viktigt att stödet omfattar både vilka frågor som behöver beaktas och hur dessa kan bedömas.

Den offentliga förvaltningen behöver även stöd i valet av teknik och i vilka fördelar som kan uppnås genom att kombinera olika tekniker. Här kan en sammanställning av olika användningsfall fungera som ett sätt att lyfta fram den praktiska tillämpningen av olika tekniker. I uppdraget bör det därför ingå att informera och sprida kunskap om relevanta användningsfall inom förvaltningen (se också avsnitt 7.4.2). Detta kan till exempel ske genom att information om olika användningsfall publiceras på en webbplats. Sådan information bidrar till att sprida goda exempel på användningen av teknikerna och ger samtidigt allmänheten en ökad insyn i vilka skyddsåtgärder som tillämpas vid behandling av deras personuppgifter.

Stöd och vägledning kan behövas kompletteras av kunskapshöjande insatser för att främja användningen

Den typ av stöd och vägledning som utredningen föreslår kan behöva kompletteras med andra insatser. Vi anser att uppdraget om stöd och vägledning kan omfatta olika typer av insatser för att öka kunskapen om potentialen hos olika tekniker. Det är särskilt relevant under det första året av uppdraget för att uppmärksamma förvaltningen på vilka tekniker som finns och vilka nyttor som kan skapas med hjälp av integritetsfrämjande teknik. Detta är extra viktigt bland vissa aktörer, exempelvis på kommunal nivå, där det saknas eller endast finns väldigt begränsad kunskap om de moderna teknikerna. Utredningens uppfattning är att det inledningsvis kommer att behövas särskilda informations- och kommunikationsinsatser för att höja kunskapsnivån. Informations- och kommunikationsinsatser kan dels omfatta information om integritetsfrämjande teknik och de möjligheter som teknikerna ger, dels omfatta information om Diggs roll när det gäller stöd och vägledning. Det kan med fördel ske via Diggs existerande strukturer för informations-

spridning och utbildning, till exempel via myndighetens webbplats eller särskilda webbinarier. Det kan också ske i andra forum som avser digitalisering och datadelning inom offentlig förvaltning.

I ett senare skede kan mer riktade och djupgående utbildningsinsatser avseende specifika tekniker eller användningsområden vara relevanta för att fördjupa kunskapen i förvaltningen. Inom ramen för dessa insatser kan också samarbeten för kunskaps- och erfarenhetsutbyte mellan offentliga aktörer upprättas. Vi anser också att det kan finnas behov av att anordna forum för kunskapsutbyte mellan den privata marknaden och offentlig förvaltning. Det kan ge både Digg och privata leverantörer bättre kunskap om användarbehoven. Det kan också bidra till att höja kunskapen om integritetsfrämjande teknik och potentiella nyttor hos förvaltningen.

8.3.4 Uppdraget bör inledningsvis prioritera vissa tekniker

Utredningens förslag

Myndigheten för digital förvaltning bör inledningsvis ta fram vägledning för differentiell integritet, syntetiska data och för hur risken för återidentifiering kan utvärderas.

Skälen för utredningens förslag

Uppdraget att ge stöd och vägledning bör generellt inte begränsas till att enbart omfatta vissa tekniker. Inledningsvis är det dock särskilt angeläget att ta fram stöd och vägledning för vissa tekniker. Utredningen bedömer att detta gäller för syntetiska data och differentiell integritet. Syntetiska data kan användas för att träna AI-modeller. En ökad användning av syntetiska data kan därför leda till att förvaltningens användning av AI ökar. För att öka integritetsskyddet ännu mer kan differentiell integritet användas för att skapa syntetiska data, vilket också IMY har noterat.[22] Det är därför angeläget att det i ett tidigt skede ges vägledning om båda dessa tekniker.

Vid användningen av differentiell integritet är valet av tillåten nivå av integritetsförlust (epsilon, ε) en viktig fråga. Det är därför

[22] Integritetsskyddsmyndigheten (IMY), IMY-2025-23536, *Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell*, s. 10.

nödvändigt att en vägledning om differentiell integritet också omfattar vägledning i den frågan. Sådan vägledning behöver vara detaljerad så att det blir ett handfast stöd för förvaltningen och kan till exempel innehålla ett spann för den tillåtna nivån av integritetsförlust (epsilon, ε) i olika datadelningssituationer. I avsnitt 8.7.3 lämnar vi ett förslag på ett första område där ett sådant spann kan utforskas.

Ett närliggande område, för vilket det också initialt är viktigt att ta fram stöd och vägledning, är hur risken för återidentifiering ska utvärderas. Det råder en osäkerhet i förvaltningen om när avidentifieringstekniker har använts i tillräcklig utsträckning (se avsnitt 6.4.2) och det behövs ett stöd för att minska den osäkerheten (se avsnitt 7.5.2). En utvärdering av risken för återidentifiering är dessutom relevant vid skapandet av syntetiska data och användningen av differentiell integritet. Vägledning på detta område kan exempelvis ske genom en beskrivning av hur tjänster som möjliggör testattacker mot avidentifierade datamängder eller AI-modeller kan användas. Eftersom attacker i sådana tjänster normalt sker under optimala förhållanden, med tillgång till de underliggande uppgifterna, bör vägledningen också ge stöd avseende hur resultatet från en sådan tjänst kan utvärderas.

Digg bör i arbetet med att ta fram stöd och vägledning för differentiell integritet, syntetiska data och utvärdering av risken för återidentifiering samverka med SCB och IMY givet myndigheternas expertis. Digg bör också samverka med forskningsinstitutet RISE (Research Institutes of Sweden) som har ett pågående projekt om utvärdering av risken för återidentifiering.[23]

[23] I projektet LeakPro deltar AI Sweden, RISE, Sahlgrenska Universitetssjukhuset, Region Halland, Scaleout Systems AB, SynData AB, och AstraZeneca AB (publ). I referensgruppen ingår bland annat IMY och eSamverkansprogrammet (eSam). Projektet finansieras av Vinnova.

8.3.5 Stöd och vägledning ska tas fram i samverkan med berörda myndigheter

Utredningens förslag

Myndigheten för digital förvaltning ska vid framtagande av stöd och vägledning om integritetsfrämjande teknik samverka med Integritetsskyddsmyndigheten.

Myndigheten för digital förvaltning ska vid behov även samverka med Skatteverket, Nationella cybersäkerhetscentret vid Försvarets radioanstalt och Statistiska centralbyrån inom respektive myndighets expertområde.

Skälen för utredningens förslag

Det finns integritetsfrämjande tekniker som förutsätter en viss specialistkompetens som det inte är effektivt att Digg bygger upp på egen hand. Integritetsfrämjande teknik syftar ytterst till att stärka skyddet för den personliga integriteten, vilket innebär att området har ett nära samband med IMY:s verksamhet. Utredningen föreslår därför att Digg, vid framtagandet av stöd och vägledning, bör ha en löpande samverkan med IMY. Det gäller oavsett vilken typ av integritetsfrämjande teknik som avses.

Olika avidentifieringstekniker används ofta inom statistikområdet. Som konstaterats tidigare har SCB kunskap och ger vägledning om vissa av de etablerade avidentifieringsteknikerna. Andra tekniker bygger på kryptografi där FRA är expertmyndighet. Utredningen anser att den specialistkompetens som finns hos respektive myndighet bör tas tillvara. I samband med att stöd och vägledning om integritetsfrämjande teknik utarbetas av Digg bör de därför samverka med dessa myndigheter när frågor som berör deras respektive expertområden uppkommer.

När det gäller FRA bedömer vi det som lämpligt att samverkan sker inom ramen för den verksamhet som sker vid NCSC, givet NCSC:s uppgift att fungera som en nationell plattform för samverkan och informationsutbyte mellan aktörer.[24] Övriga delar av

[24] 2 § förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

FRA kan samtidigt behöva stötta NCSC med kompetens i vissa frågor, till exempel när det gäller kryptografi.

Digg bör även samverka med Skatteverket, som vi föreslår ska tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik (se avsnitt 8.4.2). Behovet av stöd och vägledning kan påverkas av vilka förvaltningsgemensamma tjänster som erbjuds. Myndigheterna kommer inom ramen för sina respektive uppdrag få kännedom om behov som berör den andra myndighetens uppdrag (se även avsnitt 8.4.5).

8.3.6 Uppdragen bör ges i regleringsbrev

Utredningens förslag

Uppdraget till Myndigheten för digital förvaltning att ge stöd och vägledning för integritetsfrämjande teknik bör ges i myndighetens regleringsbrev.

Uppdragen till Integritetsskyddsmyndigheten, Myndigheten för digital förvaltning, Nationella cybersäkerhetscentret vid Försvarets radioanstalt och Statistiska centralbyrån bör ges i respektive myndighets regleringsbrev.

Skälen för utredningens förslag

Uppdraget att ge stöd och vägledning för integritetsfrämjande teknik bör regleras i Diggs regleringsbrev

Ansvaret för stöd och vägledning om integritetsfrämjande teknik bör tydliggöras i form av ett regeringsuppdrag. Skälet till det är bland annat att det är ett nytt område, där kunskapen om användningen av teknikerna är låg. Det behöver därför tydligt framgå vilken myndighet som ansvarar för att stödja och vägleda förvaltningen. Ett utpekat ansvar innebär också bättre förutsättningar för Digg att bygga upp kunskap och kompetens inom området.

Det stödjande och vägledande uppdraget bör ges i Diggs regleringsbrev under flera år eftersom stöd och vägledning behöver ske löpande och utvecklas på längre sikt. Uppdrag i regleringsbrev som löper över flera år ger mer långsiktiga förutsättningar för att bygga

upp kompetens jämfört med särskilda, mer tidsbegränsade regeringsuppdrag. I regleringsbrev finns det dessutom en flexibilitet för att anpassa uppdraget i takt med att nya tekniker når en högre mognadsgrad och beroende på hur regeringen vill inrikta uppdraget. Det kan då förtydligas genom att komplettera den övergripande uppdragsskrivningen i regleringsbrevet. Ett förtydligande om den initiala prioriteringen av att ta fram vägledning för differentiell integritet, syntetiska data och risken för återidentifiering är ett exempel på en sådan kompletterande uppdragsbeskrivning.

Utredningen ser även behov av att regeringen initialt följer utvecklingen inom området. Digg bör därför det första året ta fram och redovisa en kortfattad färdplan till regeringen för vilka integritetsfrämjande tekniker som myndigheten bedömer att det behövs stöd och vägledning för. Eftersom den tekniska utvecklingen för teknikerna rör sig snabbt, bör färdplanen kontinuerligt revideras i takt med att nya behov uppstår och nyare tekniker når en högre mognadsgrad. Om stöd och vägledning för integritetsfrämjande teknik integreras som en del av Ena kan även färdplanen för integritetsfrämjande teknik utgöra en del av den strategiska färdplanen för Ena.[25]

Alternativa sätt att reglera uppdraget som har övervägts

Uppdraget att ge stöd och vägledning kan regleras även på andra sätt. Vi har övervägt att ge det stödjande och vägledande ansvaret för integritetsfrämjande teknik som en uppgift i Diggs instruktion. Myndighetsinstruktioner är ett mer långsiktigt styrmedel för regeringen än regleringsbrev, men ger inte samma flexibilitet och utrymme för att ändra och specificera uppdrag (se avsnitt 8.2.2). Vi anser att det senare är centralt när det gäller integritetsfrämjande teknik, mot bakgrund av den snabba teknikutvecklingen. Det finns också ett behov av att regeringen har möjlighet att närmare specificera vad uppdraget bör omfatta. Uppdrag i regleringsbrev ger bättre möjlighet för detta än uppgifter i instruktion, där uppgifter också bör vara relativt övergripande och teknikneutrala. Vi anser därför att instruktionen lämpar sig mindre väl för den typen av styrning som uppdraget kräver, särskilt i en uppbyggnadsfas.

[25] Digg, *Förslag till långsiktig utveckling och förvaltning av Ena*.

Det stödjande och vägledande uppdraget ryms redan till stora delar inom flera av Diggs uppgifter enligt instruktionen. Det gäller såväl uppgiften att stödja den förvaltningsgemensamma digitaliseringen som uppgiften att samordna frågor som rör förvaltningens elektroniska informationsutbyte.[26] Det gäller även Diggs uppgifter att främja tillgängliggörande och vidareutnyttjande av data från den offentliga förvaltningen och att ge vägledning till förvaltningen i juridiska frågor inom ramen för den förvaltningsgemensamma digitaliseringen.[27] Det finns dock ingen enskild bestämmelse som det föreslagna uppdraget specifikt kan anses rymmas inom, till exempel omfattar uppdraget inte endast vägledning om juridiska frågor. På längre sikt kan det finnas skäl för att ytterligare förtydliga ansvaret för stöd och vägledning för integritetsfrämjande teknik i instruktionen.

Oavsett hur uppgiften förtydligas framöver anser utredningen att det är viktigt att den stödjande och vägledande verksamheten för integritetsfrämjande teknik fortsätter som en integrerad del av Diggs uppgifter och verksamhet på längre sikt, även om uppdraget inte längre återfinns i regleringsbrevet.

Uppdragen att samverka med Digg bör ges i regleringsbrev

I uppdragsbeskrivningen till Digg bör det också anges att Digg ska samverka med IMY vad gäller att ta fram stöd och vägledning för samtliga tekniker. Digg ska också samverka med SCB och NCSC vid FRA vid behov av specifik kompetens inom avidentifieringstekniker respektive kryptografi samt med Skatteverket avseende tekniker som det erbjuds förvaltningsgemensamma tjänster för (se avsnitt 8.3.5).

Även uppdragen att samverka med Digg bör under flera år ges i respektive myndighets regleringsbrev, för att ge dem långsiktiga förutsättningar att utveckla kompetens och fungerande samverkansstrukturer för integritetsfrämjande teknik. Utöver den generella skyldigheten i myndighetsförordningen (2007:515) om samverkan mellan myndigheter, har varken SCB eller IMY den typen av stödjande eller samverkande uppgifter i myndigheternas respektive in-

[26] 1 och 2 §§ förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[27] 6 § förordningen (2018:1486) med instruktion för Myndigheten för digital förvaltning.

struktioner. NCSC har redan i uppgift att samverka med Post- och telestyrelsen (som från och med 1 januari 2027 slås samman med Digg) inom ramen för sin förordningsreglerade verksamhet.[28] Utredningen anser dock att denna samverkan behöver förtydligas särskilt i fråga om integritetsfrämjande teknik. Det är nödvändigt för att skapa tydliga förutsättningar för uppbyggnad av samverkan och kompetens mellan myndigheterna.

8.4 Förvaltningsgemensamma tjänster

8.4.1 Det behövs förvaltningsgemensamma tjänster för att öka användningen

Utredningens bedömning

Förvaltningsgemensamma tjänster för integritetsfrämjande teknik bidrar till en ansvarsfull, innovativ och rättssäker datadelning. Tjänsterna bidrar också till kostnadseffektiva lösningar och samlad kompetens.

Skälen för utredningens bedömning

Tjänsterna bidrar till en ansvarsfull, innovativ och rättssäker datadelning

Integritetsfrämjande teknik utgör ett relativt nytt och tekniskt avancerat område som förenar juridiska, tekniska och organisatoriska aspekter. Många myndigheter, regioner och kommuner saknar i dag både förståelse och erfarenhet av hur sådana tekniker kan användas i praktiken. I flera fall saknas även den tekniska kompetensen som krävs för att självständigt kunna utvärdera, implementera och förvalta sådana lösningar. Bristande kunskap om integritetsfrämjande teknik medför en risk för överdriven försiktighet, vilket kan innebära att nyttorna med datadelning inte realiseras.

Vissa integritetsfrämjande tekniker, särskilt de moderna teknikerna som bygger på kryptografi, förutsätter dessutom tillgång till avancerade tekniska lösningar. Att utveckla eller upphandla tek-

[28] 4 § förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

niska lösningar förutsätter både resurser och kompetens, vilket kan vara svårt för offentliga aktörer att realisera i praktiken. Detta gäller särskilt för små kommuner och myndigheter.

Det innebär att kunskapshöjande insatser behöver kombineras med åtgärder som underlättar tillgången till förvaltningsgemensamma tjänster för integritetsfrämjande teknik. Detta för att ytterligare sänka tröskeln för användningen av teknikerna. Att etablera sådana tjänster bidrar till en konsekvent efterlevnad av regelverk och skapar bättre förutsättningar för förvaltningen att kunna använda data på ett ansvarsfullt, innovativt och rättssäkert sätt.

Tjänsterna bidrar till kostnadseffektiva lösningar och samlad kompetens

Utveckling och drift av avancerade tjänster för integritetsfrämjande teknik innebär initiala investeringar och behov av kompetensuppbyggnad. Om varje myndighet, kommun och region självständigt utvecklar eller upphandlar sådana lösningar riskerar detta att leda till dubbelarbete, fragmentering och varierande kvalitetsnivåer. Genom förvaltningsgemensamma tjänster kan stordriftsfördelar uppnås samtidigt som förutsättningarna för modern datadelning stärks.

Även om kunskap om integritetsfrämjande tekniker finns tillgänglig på den privata marknaden är kompetensen i många fall begränsad och koncentrerad till ett fåtal aktörer. Detta leder till konkurrens om resurser och svårigheter för enskilda offentliga aktörer att både attrahera och behålla relevant kompetens. Genom att etablera förvaltningsgemensamma tjänster för de tekniker där det bedöms lämpligt, kan offentlig förvaltning samla och långsiktigt upprätthålla den spetskompetens som krävs. Förvaltningsgemensamma tjänster kan därmed tillgodose behovet av samordnad kompetens, enhetlig tillämpning och kostnadseffektiva lösningar.

En myndighet bör därför få i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik.

8.4.2 Skatteverket får i uppdrag att tillhandahålla förvaltningsgemensamma tjänster

Utredningens förslag

Skatteverket ska få i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik till offentlig förvaltning.

Skälen för utredningens förslag

Integritetsfrämjande tekniker är relevanta för hela den offentliga förvaltningen. Det är därför inte givet vilken myndighet som bör ges ansvar för att tillhandahålla förvaltningsgemensamma tjänster. Det finns dock ett flertal myndigheter som i dag har ansvarsområden som har ett nära samband med integritetsfrämjande teknik, som Digg, IMY, SCB och FRA (se avsnitt 8.2.3). Utredningen anser att det är av särskild vikt att myndigheten som tillhandahåller förvaltningsgemensamma tjänster för integritetsfrämjande teknik har betydande kapacitet vad gäller utveckling, drift och förvaltning. Skälet till det är bland annat att teknikerna ställer höga krav på att det finns kapacitet och kompetens för att utveckla tjänsterna, liksom för att löpande förvalta och drifta dessa. Det kan vidare på längre sikt bli aktuellt att utveckla integritetsfrämjande teknik som ställer ännu högre krav på it-kapacitet, till exempel vad gäller beräkningskapacitet.

Utredningen anser att någon av leverantörsmyndigheterna enligt 5 § förordningen (2024:1005) om samordnad och säker statlig it-drift är lämpliga kandidater för uppdraget. Även om uppdraget inte omfattar statlig it-drift så har myndigheterna sådan erfarenhet, kompetens och kapacitet avseende it-drift som vi anser vara nödvändig.

Mot bakgrund av Försäkringskassans och Skatteverkets uppdrag att etablera en AI-verkstad finns det fördelar med att någon av dessa myndigheter får ansvaret för att tillhandahålla de förvaltningsgemensamma tjänsterna. Uppdraget bör dock inte inkluderas i uppdraget avseende AI-verkstaden, eftersom förvaltningsgemensamma tjänster för integritetsfrämjande teknik har flera användningsområden som inte berör AI. Det är däremot viktigt att de tjänster som tillhandahålls för integritetsfrämjande teknik och de tjänster som erbjuds inom AI-verkstaden är kompatibla med varandra. På så vis får offent-

lig förvaltning ett sömlöst tjänsteutbud och de offentliga resurserna kan nyttjas på bästa sätt. Vi anser också att uppdraget att etablera AI-verkstaden innebär att myndigheterna får ytterligare kapacitet och kompetens som är relevant för såväl utvecklingen och tillämpningen av integritetsfrämjande teknik som för AI-verkstaden.

Utredningens uppfattning är att Försäkringskassan och Skatteverket är likvärdigt lämpliga att ansvara för de förvaltningsgemensamma tjänsterna avseende integritetsfrämjande teknik. Skillnaden mellan myndigheterna bedöms således inte ligga i deras tekniska förutsättningar, då båda har den kompetens och kapacitet som krävs för uppdraget. De omständigheter som enligt utredningens mening motiverar att uppdraget bör tilldelas Skatteverket är i stället verksamhetsmässiga.

Skatteverket hanterar omfattande och samhällskritiska datamängder som efterfrågas brett inom offentlig förvaltning, till exempel folkbokföringsregistret och beskattningsuppgifter. Myndigheten är därför en viktig aktör i många datadelningssituationer. Vidare har Skatteverket erfarenhet av att tillhandahålla förvaltningsgemensamma lösningar inom Ena eftersom myndigheten ansvarar för Mina ärenden och är driftleverantör för lösningar för digital post. Mot denna bakgrund föreslår utredningen att Skatteverket får i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik.

Alternativa mottagare av uppdraget som har övervägts

Ett alternativ till utredningens förslag är att ge uppdraget till både Försäkringskassan och Skatteverket, eftersom de bedöms ha likvärdiga tekniska förutsättningar att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik. En sådan lösning finns för uppdraget om AI-verkstaden. Utredningen anser dock att det finns övervägande fördelar med en tydlig ansvarsfördelning när det gäller utveckla och tillhandahålla tekniska tjänster. Det kan förenkla och effektivisera genomförandet. Därför bör uppdraget inte ges till myndigheterna gemensamt.

Vi har även övervägt att låta Digg tillhandahålla den förvaltningsgemensamma tjänsten för integritetsfrämjande teknik, mot bakgrund av att vi föreslår att Digg ska tillhandahålla stöd och vägled-

ning för integritetsfrämjande teknik och mot bakgrund av Diggs ansvar för den förvaltningsgemensamma digitaliseringen. Digg ansvarar också för de flesta av de lösningar som ingår i Ena. Samtidigt ansvarar även andra myndigheter för drift och förvaltning av vissa av de digitala lösningar som ingår i Ena. Som exempel kan nämnas att Bolagsverket ansvarar för drift och förvaltning av tjänsten för digitala fullmakter, Mina ombud. Vissa av de tjänster som ingår i Ena har också utvecklats av andra myndigheter, till exempel så har Skatteverket utvecklat tjänsten för digital post, Mina meddelanden. Det tyder på att också andra myndigheters kapacitet behöver användas för vissa förvaltningsgemensamma digitala lösningar.

Behovet av att samordna stödet och vägledningen med de förvaltningsgemensamma tjänster som tillhandahålls kan lösas genom ett krav på samverkan mellan Skatteverket och Digg (se avsnitt 8.3.5 och 8.4.5). Att integrera förvaltningsgemensamma tjänster för integritetsfrämjande teknik som en del i Ena kan även säkerställa att tjänsten drar nytta av den samordningsstruktur som finns för Ena (se vidare i avsnitt 8.4.5).

8.4.3 Innehållet i uppdraget att tillhandahålla förvaltningsgemensamma tjänster

Utredningens förslag

Uppdraget bör omfatta tillhandahållande av förvaltningsgemensamma tjänster för integritetsfrämjande teknik och tjänster som underlättar användningen av sådan teknik. Uppdraget bör inte begränsas till vissa tekniker.

Skälen för utredningens förslag

Uppdraget bör avse utveckling, drift och förvaltning

Med förvaltningsgemensamma tjänster avses i det här sammanhanget olika slags tekniskt stöd som kan nyttjas av hela förvaltningen för att bearbeta data med hjälp av integritetsfrämjande teknik. Det kan enligt utredningens uppfattning inkludera testmiljöer, testbäddar, plattformar och andra typer av tekniska lösningar. Det inkluderar

också tekniskt och praktiskt stöd för användningen av dessa lösningar. Andra former av stöd och vägledning bör tillhandahållas av Digg, exempelvis generell kunskap om specifika tekniker.

Utredningen anser att tillhandahållandet av förvaltningsgemensamma tjänster för integritetsfrämjande teknik bör omfatta utveckling, drift och förvaltning. Den tillhandahållande myndigheten bör i första hand överväga att upphandla hela eller delar av tjänsterna om sådana finns tillgängliga på den privata marknaden. Endast i de fall sådana tjänster inte kan upphandlas bör utveckling bedrivas av den myndighet som ska tillhandahålla tjänsten.

Den myndighet som ska tillhandahålla de förvaltningsgemensamma tjänsterna för integritetsfrämjande teknik bör ha ett tydligt mandat att besluta om prioriteringar, drift och förvaltningsmodell för tjänsterna. Som tillhandahållare ansvarar myndigheten bland annat för informationssäkerhet, incidentrapportering och kontinuitetsplanering. För att möjliggöra en bred användning inom offentlig förvaltning behöver den tillhandahållande myndigheten även etablera en process för stöd inför användning av tjänsterna.

Det ska dock noteras att de offentliga aktörer som använder tjänsterna fortsatt ansvarar för sina respektive datamängder och för att behandlingen sker i enlighet med gällande författningar. Den myndighet som tillhandahåller förvaltningsgemensamma tjänster behöver därför tydliggöra ansvarsfördelningen vid användningen.

Tjänster som stödjer användningen av integritetsfrämjande teknik

Utredningen har identifierat ett antal utmaningar avseende användningen av integritetsfrämjande teknik som är av mer generell karaktär och inte hänförliga till någon enskild teknik. Dessa utmaningar uppstår i arbetsprocessen antingen före eller efter den bearbetning som sker genom teknikerna. Uppdraget att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik behöver därför även inkludera tjänster som inte direkt rör en specifik teknik, men som på olika sätt underlättar eller främjar användningen av dessa.

En sådan stödjande tjänst kan till exempel vara en tjänst för attacktester. Det kan hjälpa den offentliga förvaltningen att säkerställa att olika avidentifieringstekniker har använts i tillräckligt stor utsträckning inför delning av data eller av AI-modeller (se även avsnitt 7.5.4).

Det kan också handla om tjänster som stödjer anpassning av data inför en bearbetning med integritetsfrämjande teknik. Vid exempelvis federerad inlärning och säker flerpartsberäkning behöver de datamängder som ingår uppvisa en hög grad av enhetlighet. Det gäller såväl format och datastrukturer som skalor, begreppsdefinitioner och andra semantiska egenskaper. Bristande harmonisering mellan datakällor riskerar i annat fall leda till felaktiga slutsatser eller analysresultat. De här frågorna har ett nära samband med kommande krav på interoperabilitet vid datadelning inom offentlig förvaltning.

Uppdraget bör inte begränsas till vissa tekniker

Den tekniska utvecklingen gällande integritetsfrämjande teknik sker i snabb takt. Vad som klassas som integritetsfrämjande teknik förändras snabbt och uppdraget behöver ha flexibilitet för att kunna följa den utvecklingen. Utredningen anser därför att det inte finns skäl att detaljreglera vilka specifika tekniker som ska stödjas inom ramen för ett uppdrag om att tillhandahålla förvaltningsgemensamma tjänster.

Vilka tjänster som tillhandahålls ska styras av behov och den tekniska utvecklingen

Uppdraget bör omfatta integritetsfrämjande teknik generellt. Det innebär dock inte att det behöver tillhandahållas förvaltningsgemensamma tjänster för varje enskild teknik. Utredningen anser att förvaltningsgemensamma tjänster bör utvecklas eller upphandlas för de tekniker där det finns behov och fördelar med att tillhandahålla sådana tjänster till förvaltningen. Det gäller i regel tekniker som är tekniskt mogna för användning och har stor potential, men som endast används i begränsad utsträckning.

Således är det behoven och den tekniska utvecklingen som i huvudsak ska styra vilka förvaltningsgemensamma tjänster som erbjuds vid varje tidpunkt. Här bör det särskilt beaktas om behoven av tjänster för integritetsfrämjande teknik i stället kan tillgodoses av privata leverantörer.

Vår uppfattning är att en alltför bred utveckling av förvaltningsgemensamma tjänster för samtliga tekniker skulle vara omotiverat

kostsam sett till den faktiska användningen och nyttan. Vissa tekniker, så som etablerade avidentifieringstekniker, används redan i betydande omfattning inom offentlig förvaltning, medan andra tekniker är av sådan karaktär att de inte är tillräckligt tekniskt komplicerade för att motivera utvecklingen av förvaltningsgemensamma tjänster. Vidare har vissa tekniker ännu inte uppnått den tekniska mognadsgrad som krävs för en bred användning inom förvaltningen.

Ytterligare ett skäl som talar emot att det ska tas fram förvaltningsgemensamma tjänster för samtliga integritetsfrämjande tekniker är att det för vissa tekniker, exempelvis betrodda exekveringsmiljöer, finns färdiga produkter att tillgå på marknaden. Kammarkollegiet har även påbörjat en förstudie om att analysera förutsättningarna för att inrätta ett dynamiskt inköpssystem för innovativa digitala lösningar.[29] Det kan därmed bli enklare för offentliga aktörer att köpa in lösningar för integritetsfrämjande teknik i framtiden.

Om regeringen vid en viss tidpunkt anser att det finns anledning att styra utvecklingen av förvaltningsgemensamma tjänster till en specifik teknik kan det ske inom ramen för det generella uppdraget. Utredningens uppfattning är att det initialt finns skäl att styra prioriteringen för vilken teknik som ska tillhandahållas genom en förvaltningsgemensam tjänst (se vidare avsnitt 8.4.4).

[29] Finansdepartementet, Fi2025/00311, *Uppdrag till Kammarkollegiet att genomföra en förstudie om att inrätta ett dynamiskt inköpssystem för innovativa digitala lösningar*.

8.4.4 En förvaltningsgemensam tjänst för säker flerpartsberäkning bör prioriteras

Utredningens förslag

Skatteverket bör inledningsvis tillhandahålla en förvaltningsgemensam tjänst för säker flerpartsberäkning.

Skälen för utredningens förslag

Det finns nyttor med att prioritera en tjänst för säker flerpartsberäkning

Utredningens anser att säker flerpartsberäkning i dagsläget är den teknik som i störst utsträckning kan lösa den offentliga förvaltningens utmaningar gällande datadelning samtidigt som datakvaliteten kan bibehållas. Det är också en generell och brett användbar teknik som kan nyttjas av stora delar av förvaltningen. Samtidigt är det en komplex teknik och det är därför inte ändamålsenligt att varje enskild aktör utvecklar och förvaltar egna lösningar. En förvaltningsgemensam tjänst för säker flerpartsberäkning främjar därför en kostnadseffektiv och enhetlig tillämpning inom hela förvaltningen. Det kan också ses som ett första steg mot en framtid där data är krypterad under hela sin livscykel (se avsnitt 3.9.2).

Tekniken bidrar vidare till en ny syn på datadelning där säker analys av data över organisationsgränser möjliggörs utan att de underliggande uppgifterna delas. Tekniken bedöms därför även vara lämplig för hantering av särskilt skyddsvärda uppgifter. Detta illustreras av att säker flerpartsberäkning redan används i projekt som avser uppgifter inom hälso- och sjukvården, där kraven på skyddsnivå och rättslig efterlevnad är höga. Även Eurostat arbetar med att utveckla en liknande tjänst för nationella statistikmyndigheter (se avsnitt 4.4.6).

Andra tjänster bör inte prioriteras i dagsläget

Utöver säker flerpartsberäkning är differentiell integritet och federerad inlärning tekniker som används i begränsad utsträckning trots att de är mogna för praktisk användning.

Differentiell integritet är en av de tekniker som vi föreslår att Digg ska prioritera att ta fram stöd och vägledning för (se avsnitt 8.3.4). Ett sådant kunskapsstöd bedöms vara ett tillräckligt första steg för att öka användningen av differentiell integritet. Det är dock viktigt att Skatteverket tillsammans med Digg bevakar och löpande utvärderar behovet av tjänster för differentiell integritet.

Federerad inlärning är en teknik som starkt förknippas med AI och träningen av AI-modeller. Vi anser därför att det i första hand är mer ändamålsenligt att eventuella behov av förvaltningsgemensamma tjänster för federerad inlärning omhändertas inom ramen för arbetet med AI-verkstaden.

Olika typer av förvaltningsgemensamma tjänster som stödjer och underlättar användningen av integritetsfrämjande teknik kan hjälpa förvaltningen att använda integritetfrämjande teknik i ökad utsträckning. Som exempel på sådana tjänster har vi tidigare lyft tjänster för attacktester och för förberedelse av data (se avsnitt 8.4.3). Det finns attacktester som är tillgängliga som öppen källkod och sådana tjänster kan därför relativt enkelt implementeras och användas av enskilda aktörer inom förvaltningen. Detta gör att det inte nödvändigtvis finns ett tillräckligt behov av en förvaltningsgemensam tjänst för attacktester i dagsläget. Utredningen har också föreslagit att Digg ska prioritera att ta fram vägledning om hur risken för återidentifiering kan utvärderas, vilket inkluderar användningen av attacktester. Det är enligt utredningens uppfattning ett tillräckligt första steg för att stödja den offentliga förvaltningen.

När det gäller anpassning av data inför bearbetning med integritetsfrämjande teknik anser utredningen att det inte är ändamålsenligt att tillhandahålla en gemensam tjänst i dagsläget. Varje förberedelse och anpassning av data är unik och förutsätter dialog och gemensam förståelse mellan de parter som deltar i analysen. Utredningens uppfattning är vidare att utmaningarna avseende anpassning av data inför bearbetning med integritetsfrämjande teknik kommer att minska i och med de krav som finns i den kommande lagen om interoperabilitetskrav för datadelning inom den offentliga förvaltningen[30]. Kraven syftar till att data ska kunna delas på ett effektivt, säkert och enhetligt sätt mellan olika system och aktörer. Det för-

[30] Lagen beslutades den 11 juni 2026 men vid tryck av betänkandet hade lagen ännu inte fått ett SFS-nummer.

utsätter bland annat att datamängder har enhetliga format, begrepp och strukturer.[31]

8.4.5 Förvaltningsgemensamma tjänster ska utvecklas i samverkan med berörda myndigheter

Utredningens förslag

Förvaltningsgemensamma tjänster ska utvecklas i samverkan med Myndigheten för digital förvaltning och Integritetsskyddsmyndigheten.

Skatteverket ska vid behov även samverka med Nationella cybersäkerhetscentret vid Försvarets radioanstalt och Statistiska centralbyrån inom respektive myndighets expertområde.

Förvaltningsgemensamma tjänster för integritetsfrämjande teknik bör utgöra en komponent i den nationella digitala infrastrukturen Ena.

Skälen för utredningens förslag

Tjänsterna ska utvecklas i samverkan med berörda myndigheter

Relevant kompetens om integritetsfrämjande teknik finns i dag spridd inom statsförvaltningen. Integritetsfrämjande teknik syftar ytterst till att stärka skyddet för den personliga integriteten. Området har därför ett nära samband med IMY:s verksamhet. Utredningen anser att Skatteverket bör upprätthålla en löpande samverkan med IMY vid utvecklingen av förvaltningsgemensamma tjänster, oberoende av vilken typ av integritetsfrämjande teknik som tjänsterna ska stödja.

Vi anser även att Skatteverket löpande bör samverka med Digg eftersom Digg föreslås få ansvar för att tillhandahålla stöd och vägledning om integritetsfrämjande teknik. Båda myndigheterna kommer inom ramen för respektive uppdrag fånga upp behov som den andra myndigheten behöver få kännedom om. Sannolikt kommer det även finnas frågor där de båda myndigheternas uppdrag överlappar med varandra, som till exempel avseende olika sorters stöd för tekniker

[31] Se prop. 2025/26:244 s. 20 f.

som det tillhandahålls förvaltningsgemensamma tjänster för. Det finns också ett behov av samverkan med Digg givet myndighetens ansvar för Ena.

NCSC vid FRA har expertkunskap inom informationssäkerhet och kryptografi. NCSC kan därmed bidra med stöd i fråga om relevanta standarder och nödvändiga certifieringar när det gäller kryptografi i förvaltningsgemensamma tjänster. SCB har expertis inom avidentifieringstekniker och röjandekontroll. Utredningen anser att deras kompetenser bör tillvaratas. Skatteverket bör därför samverka med dessa myndigheter vid utvecklingen av förvaltningsgemensamma tjänster för tekniker som berör respektive myndighets expertområde.

Tjänsterna bör ingå i Ena

Ena består av gemensamma lösningar som gör det enkelt, säkert och effektivt för offentlig förvaltning att förbättra sin digitalisering. En viktig förutsättning för att realisera nyttorna med en sådan infrastruktur är att data kan hanteras och utbytas på ett säkert, ändamålsenligt och effektivt sätt.

De förvaltningsgemensamma tjänster som utredningen föreslår har till syfte att främja användningen av integritetsfrämjande teknik och därigenom skapa förbättrade förutsättningar för datadelning inom hela den offentlig förvaltningen. Utredningen anser att de föreslagna förvaltningsgemensamma tjänsterna är förenliga med syftet med den nationella digitala infrastrukturen och att tjänsterna bör utgöra en komponent i Ena.

8.4.6 Uppdragen bör ges i regleringsbrev

Utredningens förslag

Skatteverkets uppdrag att tillhandahålla förvaltningsgemensamma tjänster bör ges i myndighetens regleringsbrev.

Uppdragen till Integritetsskyddsmyndigheten, Myndigheten för digital förvaltning, Nationella cybersäkerhetscentret vid Försvarets radioanstalt och Statistiska centralbyrån bör ges i respektive myndighets regleringsbrev.

Skälen för utredningens förslag

Uppdraget att tillhandahålla tjänster ges i Skatteverkets regleringsbrev

Utredningens utgångspunkt är att tillhandahållandet, driften och förvaltningen av förvaltningsgemensamma tjänster innebär ett långsiktigt åtagande. Den snabba utvecklingen av teknikerna innebär att det kommer att behöva ske utveckling av nya tjänster på såväl kort som lång sikt.

Vi anser därför att det är lämpligast att uppdraget ges i Skatteverkets regleringsbrev under flera år. Det skapar relativt långsiktiga förutsättningar, samtidigt som det ger regeringen flexibilitet att styra inriktningen för nya tjänster. Vi anser att en reglering i instruktionen lämpar sig mindre väl för en sådan flexibel och mer detaljerad styrning som uppdraget om förvaltningsgemensamma tjänster behöver.

Uppdraget i regleringsbrevet bör löpa under flera år för att säkerställa kontinuitet i arbetet och möjligheten till att bygga upp kompetens inom området. Om regeringen anser att en specifik teknik ska prioriteras kan uppdraget kompletteras vissa år. En första sådan utpekad prioritering bör ske för säker flerpartsberäkning (se avsnitt 8.4.4). Inom uppdraget att etablera en sådan tjänst kommer vissa initiala analyser av behov och förberedelser vara nödvändiga. Enligt utredningens uppfattning är detta är en naturlig del av ett uppdrag att tillhandahålla en förvaltningsgemensam tjänst och det behöver därför inte anges särskilt i uppdraget.

För att det ska vara möjligt för regeringen att följa utvecklingen av de förvaltningsgemensamma tjänsterna bör Skatteverket skriftligt redovisa vissa delar av arbetet under de första åren. Den första delredovisningen bör ske efter att analys- och pilotfasen för tjänsten är avslutad och omfatta en översiktlig beskrivning av hur implementeringen av en tjänst för säker flerpartsberäkning ska genomföras och en mer detaljerad kostnadsanalys.

På längre sikt kan regeringen överväga att reglera ansvaret för att tillhandahålla de förvaltningsgemensamma tjänsterna för integritetsfrämjande teknik i Skatteverkets instruktion eller inom ramen för en författningsreglering av Ena.[32]

[32] Se Digg, *Förslag till långsiktig utveckling och förvaltning av Ena.*

Alternativ som har övervägts

Ett alternativ till att reglera uppdraget i regleringsbrev hade varit att införa det i en ny författning. En författningsreglering skapar förutsättningar för en mer långsiktig styrning men är samtidigt mindre flexibel som styrmedel. Författningsreglering bör också endast användas när det finns ett tydligt och välmotiverat behov av en sådan. En reglering skulle dock i princip endast reglera Skatteverkets arbetsuppgifter och samverkan med andra myndigheter. Utredningen har inte sett några skäl till att reglera andra förhållanden som rör förvaltningsgemensamma tjänster, så som personuppgiftansvar eller kostnader för användningen av tjänsterna (se även avsnitt 8.6.2 och 8.5.5). Med hänsyn till det begränsade behovet av reglering anser utredningen att det inte vore ändamålsenligt med en ny författning.

Uppdragen att samverka med Skatteverket bör ges i regleringsbrev

Utredningen anser att IMY, SCB och NCSC vid FRA ska ges i uppdrag att samverka med Skatteverket i arbetet med att ta fram förvaltningsgemensamma tjänster för integritetsfrämjande teknik. Deras expertkompetens är nödvändig för att Skatteverket ska kunna ta fram förvaltningsgemensamma tjänster.

Utredningen anser att uppdragen att samverka bör regleras i respektive myndighets regleringsbrev under flera år, på samma sätt som för stöd och vägledning (avsnitt 8.3.6). Detta ger myndigheterna långsiktiga förutsättningar för att utveckla relevant kompetens samt att etablera ändamålsenliga och stabila samverkansstrukturer inom området. Utöver de generella skyldigheterna i myndighetsförordningen om samverkan mellan myndigheter, har varken SCB eller IMY i dag uppgifter som avser samverkan i sina instruktioner. NCSC vid FRA har däremot redan i dag i uppgift att samverka med andra myndigheter i frågor som rör centrets verksamhetsområde. Utredningen bedömer dock att denna samverkan behöver förtydligas särskilt i fråga om integritetsfrämjande teknik. Ett sådant förtydligande är nödvändigt för att skapa tydliga förutsättningar för uppbyggnad av samverkan och kompetens mellan myndigheterna.

8.5 Finansiering av förvaltningsgemensamma tjänster för integritetsfrämjande teknik

8.5.1 Finansieringsmodeller för offentlig förvaltning

Uppdrag till statliga myndigheter kan i huvudsak finansieras genom anslag, avgifter eller bidrag. Anslag utgör huvudregeln för finansiering av statlig verksamhet. Statskontoret (tidigare Ekonomistyrningsverket) har framfört att anslag ger bättre förutsättningar för långsiktig och stabil hantering av förvaltningsgemensamma digitala tjänster.[33] Anslagsfinansiering stärker också riksdagens och regeringens möjligheter att styra ambitionsnivåer och investeringar och är särskilt lämplig när det är svårt att identifiera betalande målgrupper eller när avgifter riskerar att hämma användningen. Den är även fördelaktig vid investeringar som annars skulle behöva lånefinansieras, eftersom anslag ger säkrare planeringsförutsättningar. Det finns i dag ett antal myndighetsgemensamma digitala lösningar som finansieras via anslag, till exempel Ena, Verksamt.se och Minpension.se.

Enligt Statskontoret kan förvaltningsgemensamma digitala tjänster räknas som anläggningstillgångar. Anläggningstillgångar ska huvudsakligen lånefinansieras i enlighet med 2 kap. 1 § i kapitalförsörjningsförordningen (2011:210). Det innebär att en myndighet inte får hela investeringen i tillgången finansierad direkt via anslag, utan att vissa delar finansieras genom lån från Riksgälden. Regeringen kan dock meddela undantag från krav på lånefinansiering för vissa anläggningstillgångar och medge att investeringen ska finansieras direkt från anslag. Statskontoret anser att sådana undantag även bör gälla för förvaltningsgemensamma digitala verksamhetsinvesteringar, eftersom det kan öka incitamenten för myndigheter att investera i förvaltningsgemensamma digitala lösningar där nyttan inte är tillräckligt stor för den enskilda myndigheten.[34]

Finansiering kan också ske genom avgifter, och vissa statliga verksamheter finansieras helt eller delvis via avgifter. En avgift är en ersättning som betalas för en specifik vara eller tjänst som staten tillhandahåller och varan eller tjänsten utgör en motprestation för ersättningen. Statskontoret har framfört att avgiftsfinansiering kan anses vara en lämplig finansieringsmetod när både tjänst och mål-

[33] Ekonomistyrningsverket, ESV 2020:23, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 10 och 40.
[34] ESV, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 8.

grupp är tydligt identifierade, eftersom den som använder tjänsten då också betalar för den och därmed kan bli mer kostnadsmedveten.[35] Avgiftsfinansiering brukar också anses som lämplig när privaträttsliga verksamheter ska ta del av tjänsterna. Dels för att de ska bidra till finansieringen, dels för att det inte ska påverka konkurrensen i förhållande till företag som tillhandahåller motsvarande tjänster. Avgifter bör vidare särskilt övervägas när användarna är andra utomstatliga aktörer, exempelvis kommuner och regioner, eftersom det är det enda sättet att få dessa att bidra ekonomiskt.[36]

Avgifter kan dock vara olämpliga när bred användning av en tjänst ligger i samhällets intresse, då de riskerar att avskräcka aktörer eller skapa onödiga administrativa kostnader. Det riskerar att minska efterfrågan på tjänsten. Avgiftslösningar innebär dessutom att utvecklingsinsatser måste rymmas inom ändamålen för de deltagande myndigheternas anslag, vilket kan leda till att myndighetsperspektivet prioriteras framför det förvaltningsgemensamma åtagandet.[37]

Vid valet av finansieringsform behöver vissa regelverk beaktas. I detta sammanhang är i första hand upphandlingslagstiftningen, reglerna om statligt stöd samt vissa konkurrensrättsliga bestämmelser av betydelse. Vid prövningen av förenligheten med de nämnda regelverken behöver man beakta vilka aktörer som tjänsterna riktar sig till och den faktiska innebörden av relationerna mellan dessa aktörer. Hur tjänsterna ska finansieras kan även ha betydelse för bedömningarna enligt de aktuella regelverken.

8.5.2 Offentlig upphandling

Av 1 kap. 2 § lagen (2016:1145) om offentlig upphandling, LOU, framgår att lagen gäller för upphandling som genomförs av en upphandlande myndighet. Med upphandling avses åtgärder som vidtas i syfte att anskaffa varor, tjänster eller byggentreprenader genom tilldelning av kontrakt. Med en upphandlande myndighet avses enligt 1 kap. 22 § LOU en statlig eller kommunal myndighet, men även en beslutande församling i en kommun eller region. Enligt samma bestämmelse likställs vissa offentligt styrda organ med en

[35] ESV, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 40 f.
[36] ESV, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 40 f.
[37] ESV, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 40 f.

sådan myndighet, varför exempelvis kommunala bolag omfattas av reglerna om offentlig upphandling.

Anskaffningar mellan statliga myndigheter under regeringen omfattas inte av regelverket eftersom statliga myndigheter ingår i samma juridiska person, nämligen staten.[38] Kommuner och regioner är däremot åtskilda från staten och utgör fristående offentliga aktörer. Upphandlingsreglerna kan därför aktualiseras i förhållandet mellan en statlig myndighet och kommun eller region.

En grundläggande förutsättning för att ett upphandlingsförfarande ska anses föreligga är att det avslutas med tilldelning av ett kontrakt. Ett sådant föreligger om det är fråga om ett skriftligt avtal med ekonomiska villkor som ingås mellan en eller flera upphandlande myndigheter och en eller flera leverantörer och avser leverans av varor, tillhandahållande av tjänster eller utförande av byggentreprenad.[39] För att det ska vara fråga om ett avtal med ekonomiska villkor krävs att den upphandlande myndigheten får en prestation i utbyte mot ekonomisk ersättning.[40] Gåvor eller bidrag utan krav på motprestation faller som huvudregel utanför upphandlingsskyldigheten. Det är alltså fråga om upphandling i de fall en leverantör, i utbyte mot ersättning, tillhandahåller varor, tjänster eller byggentreprenader som är av direkt ekonomiskt intresse för den upphandlande myndigheten.[41]

8.5.3 Statsstöd

I fördraget om Europeiska unionens funktionssätt, EUF-fördraget, finns regler som ska säkerställa en väl fungerande konkurrens på den inre marknaden, däribland reglerna om statligt stöd. Artiklarna 107–109 i fördraget har till syfte att förhindra att konkurrensförhållandena inom unionen snedvrids genom att medlemsstaterna gynnar vissa företag eller viss produktion ekonomiskt. Statsstöd är som utgångspunkt förbjudet men det finns undantag för vissa fall då statsstöd kan vara tillåtet.[42] Den centrala bestämmelsen om statligt stöd finns i artikel 107.1 i EUF-fördraget och lyder enligt följande.

[38] Se HFD 2021 ref. 35.
[39] 1 kap. 15 § lagen (2016:1145) om offentlig upphandling.
[40] Se exempelvis domstolens dom av den 25 mars 2010, Helmut Müller mot Bundesanstalt für Immobilienaufgaben, C-451/08, EU:C:2010:168, p. 48–49.
[41] Prop. 2015/16:195 *Nytt regelverk om upphandling*, s. 933.
[42] Artikel 107.1–3 i fördraget om Europeiska unionens funktionssätt.

> Om inte annat föreskrivs i fördragen, är stöd som ges av en medlemsstat eller med hjälp av statliga medel, av vilket slag det än är, som snedvrider eller hotar att snedvrida konkurrensen genom att gynna vissa företag eller viss produktion, oförenligt med den inre marknaden i den utsträckning det påverkar handeln mellan medlemsstaterna.

EU-domstolen har definierat begreppet stöd enligt följande.

> [Varje åtgärd] varigenom medlemsstaterna för att genomföra sina egna ekonomiska och sociala mål genom ensidiga och självständiga beslut ger företag eller andra rättssubjekt tillgång till medel eller fördelar som skall främja förverkligandet av de eftersträvade ekonomiska eller sociala målen.[43]

Förbudet mot statligt stöd enligt artikel 107.1 i EUF-fördraget förutsätter att fyra rekvisit i artikeln är uppfyllda. Det krävs att

- stödet finansieras av en medlemsstat eller genom statliga medel,
- stödet riktas till vissa företag eller viss produktion,
- konkurrensen snedvrids eller riskerar att snedvridas, samt
- att handeln mellan medlemsstaterna påverkas.

Stöd som riktas till vissa företag

Begreppet företag omfattar enligt EU-domstolens praxis varje enhet som bedriver ekonomisk verksamhet, oavsett enhetens rättsliga form och oavsett hur den finansieras.[44] Domstolen har i domar som rör statligt stöd hänvisat till den innebörd som begreppet har i EUF-fördragets övriga konkurrensregler.[45] Ekonomisk verksamhet utgörs i sin tur av all verksamhet som består i att erbjuda varor eller tjänster på en viss marknad.[46] Det saknar betydelse att verksamheten bedrivs utan vinstsyfte.[47]

EU-domstolen har dock även uttalat att begreppet ekonomisk enhet på statsstödsområdet, vilket är av betydelse för avgränsningen

[43] Domstolens dom av den 27 mars 1980, Amministrazione delle finanze dello stato och Denkavit italiana Srl., C-61/79, EU:C:1980:100, p. 31.
[44] Se t.ex. domstolens dom av den 23 april 1991, Höfner och Elser, C-41/90, EU:C:1991:161, p. 21.
[45] Domstolens dom av den 10 januari 2006, Cassa di Risparmio di Firenze m.fl., C-222/04, EU:C:2006:8, p. 107.
[46] Domstolens dom av den 12 september 2000, Pavlov m.fl., C-180/98 – C-184/98, EU:C:2000:428, p. 75.
[47] Domstolens dom av den 21 september 1999, Albany, C-67/96, EU:C:1999:430, p. 85.

av företagsbegreppet, kan ha en annan innebörd än motsvarande begrepp inom andra områden inom konkurrensrätten.[48] Mot denna bakgrund har statsstödsutredningen bedömt att statsstödsreglernas företagsbegrepp inte nödvändigtvis är samma som det begrepp som är tillämpligt på andra områden inom konkurrensrätten.[49] Bedömningen av om rekvisitet är uppfyllt tar sin utgångspunkt i om den mottagande enheten, eller de aktörer som indirekt gynnas av åtgärden, kan anses bedriva ekonomisk verksamhet.

Kommuners och regioners ekonomiska verksamhet

Även om kommuner och regioner som huvudregel inte bör anses utgöra företag i statsstödsrättslig mening, kan det förekomma att vissa delar av verksamheten har karaktär av ekonomisk verksamhet.

Om den ekonomiska verksamheten är av mycket begränsad omfattning och framstår som tydligt underordnad den huvudsakliga offentliga uppgiften kan hela verksamheten i vissa fall ändå betraktas som icke-ekonomisk och därmed falla utanför statsstödsreglernas tillämpningsområde. Detta förutsätter att den ekonomiska verksamheten är av rent underordnad karaktär, det vill säga att den är direkt knuten till och nödvändig för driften av den icke-ekonomiska verksamheten eller har ett naturligt samband med denna. En sådan underordnad verksamhet kan anses föreligga när den ekonomiska verksamheten utnyttjar samma resurser som den huvudsakliga icke-ekonomiska verksamheten, så som material, utrustning, personal och anläggningstillgångar, och dessutom är begränsad i förhållande till den berörda infrastrukturens kapacitet. Ett exempel på detta kan vara när en icke-ekonomisk forskningsverksamhet i begränsad utsträckning hyr ut utrustning eller laboratorier till externa aktörer.[50] Att den ekonomiska verksamheten är av begränsad omfattning utesluter dock inte i sig att statsstödsreglerna kan vara tillämpliga, utan frågan får bedömas utifrån omständigheterna i det enskilda fallet.

[48] Domstolens dom av den 16 december 2010, AceaElectrabel Produzione SpA mot kommissionen, C-480/09 P, EU:C:2010:787, p. 66.
[49] SOU 2011:69 Olagligt statsstöd, s. 79.
[50] Kommissionens tillkännagivande om begreppet statligt stöd som avses i artikel 107.1 i fördraget om Europeiska unionens funktionssätt, C/2016/2946, p. 207.

Om den ekonomiska verksamheten inte är i begränsad omfattning och tydligt underordnad den icke-ekonomiska verksamheten kan det i stället krävas en tydlig åtskillnad mellan ekonomisk och icke-ekonomisk verksamhet. Det kan exempelvis ske genom separat redovisning och görs för att säkerställa att offentliga medel som avser den icke-ekonomiska verksamheten inte indirekt gynnar den ekonomiska verksamheten genom så kallad korssubventionering. När en och samma enhet bedriver både ekonomisk och icke-ekonomisk verksamhet ska medlemsstaterna således se till att den offentliga finansiering som beviljas för den icke-ekonomiska verksamheten begränsas till att endast täcka de faktiska kostnaderna för den verksamheten. Denna kostnad ska fastställas genom att verksamheterna redovisas tydligt åtskilda från varandra.[51]

8.5.4 Konkurrensrätt

Konkurrensrätten regleras i dag primärt i konkurrenslagen (2008:579) med tillhörande konkurrensförordning (2021:87). I konkurrenslagen regleras även konkurrensbegränsande offentlig säljverksamhet. Från och med den 1 augusti 2026 kommer offentlig säljverksamhet i stället regleras i en ny lag, lagen (2026:578) om offentlig säljverksamhet. Vissa bestämmelser i den nya lagen träder dock i kraft först den 1 januari 2027. Vi har valt att redogöra för bestämmelserna i denna nya lag, eftersom den snart träder i kraft.

Förbud mot otillbörlig offentlig säljverksamhet

Förbudet mot otillbörlig offentlig säljverksamhet gäller för statliga eller kommunala myndigheter, beslutande församlingar i kommuner och regioner, offentliga företag och sammanslutningar av offentliga aktörer. Med säljverksamhet avses en ekonomisk verksamhet som består i att tillhandahålla varor, tjänster eller andra nyttigheter på marknaden, dock inte den delen av verksamheten som består i myndighetsutövning.[52]

[51] Kommissionens tillkännagivande, C/2016/2946, p. 206 och domstolens dom av den 27 juni 2017, Congregación de Escuelas Pías Provincia Betania, C-74/16, EU:C:2017:496, p. 51.
[52] 2 § lagen (2026:578) om offentlig säljverksamhet.

Av lagen framgår att en offentlig aktör inte får bedriva en säljverksamhet eller tillämpa ett förfarande i säljverksamheten som på ett otillbörligt sätt påverkar möjligheterna för privata företag att bedriva verksamhet på marknaden.[53] Med otillbörlig påverkan avses att en offentlig aktör bedriver en verksamhet eller tillämpar ett förfarande som avviker från vad ett privat företag typiskt sett skulle göra, på ett sätt som otillbörligen påverkar privata aktörers möjligheter att bedriva verksamhet. Otillbörligheten består i att den offentliga aktören ges fördelar som ett privat företag saknar, exempelvis tillgång till offentlig finansiering eller andra särskilda förutsättningar som följer av den offentliga ställningen. Bedömningen av om otillbörlig påverkan föreligger ska göras utifrån ett hypotetiskt perspektiv och utgångspunkten är hur ett privat företag normalt skulle påverkas i en jämförbar situation. Det krävs således inte att en privat aktör faktiskt har påverkats eller att det finns privata aktörer som för närvarande är verksamma på den aktuella marknaden.[54]

En säljverksamhet eller ett förfarande som är förenligt med beslut av riksdagen eller regeringen, eller som i övrigt är försvarbart från allmän synpunkt, omfattas inte av förbudet mot otillbörlig offentlig säljverksamhet.[55] Från förbudet undantas således säljverksamhet och förfaranden som grundar sig på eller direkt följer av beslut av riksdagen eller regeringen. Sådana beslut förutsätts vara försvarbara från allmän synpunkt till följd av de särskilda allmänna intressen som motiverar verksamheten.[56] Undantaget omfattar även säljverksamhet och förfaranden som utgör en direkt följd av sådana beslut. Med beslut av regeringen avses exempelvis förordningar som meddelats med stöd av regeringens restkompetens, liksom regeringsuppdrag och regleringsbrev.[57]

När en myndighet ges i uppgift att bedriva säljverksamhet bör det noga övervägas vilka skäl som talar för att staten ska bedriva den aktuella verksamheten. Om det bedöms finnas godtagbara skäl bör det även anges vilken säljverksamhet som myndigheten ska eller får bedriva samt vilka eventuella begränsningar som ska gälla för verksamheten.[58]

[53] 3 § första stycket lagen om offentlig säljverksamhet.
[54] Prop. 2025/26:203 *Nya verktyg för stärkt konkurrens i privat och offentlig verksamhet*, s. 142.
[55] 3 § andra stycket lagen om offentlig säljverksamhet.
[56] Prop. 2025/26:203 s. 71.
[57] Prop. 2025/26:203 s. 143.
[58] Prop. 2025/26:203 s. 71.

8.5.5 En förvaltningsgemensam tjänst för säker flerpartsberäkning bör finansieras genom anslag

Utredningens förslag

Den förvaltningsgemensamma tjänsten för säker flerpartsberäkning bör finansieras genom anslag och tillhandahållas kostnadsfritt till offentlig förvaltning.

Det är möjligt att utforma den förvaltningsgemensamma tjänsten så att anslagsfinansiering är förenligt med upphandlings-, statsstöds- och konkurrensregelverken.

Skälen för utredningens förslag

Anslagsfinansiering är den mest ändamålsenliga finansieringsformen för tjänsten

När det gäller utvecklingen och etableringen av myndighetsgemensamma digitala lösningar har det tidigare framförts kritik mot finansieringsmodeller som bygger på avgifter. Avgiftsfinansiering anses inte vara en tillräckligt förutsägbar, stabil eller långsiktig finansieringsform för att kunna leverera de förväntade resultaten på ett effektivt sätt.[59] Anslagsfinansiering skapar bättre förutsättningar för att hantera förvaltningsgemensamma digitala tjänster på ett långsiktigt och stabilt sätt. Det ökar i sin tur även möjligheterna och incitamenten för att dessa tjänster ska användas på ett sådant sätt som riksdagen och regeringen har avsett.[60] Det finns också utmaningar med att finansiera en uppbyggnad av en verksamhet med avgifter, vilket bland annat it-driftsutredningen har lyft.[61]

Att finansiera en förvaltningsgemensam tjänst för säker flerpartsberäkning genom anslag säkerställer att även små offentliga aktörer ges möjlighet att ta del av tjänsten. Detta minskar risken för att små offentliga aktörer hamnar utanför den datadrivna utvecklingen. Behovet av att tillhandahålla tjänsterna avgiftsfritt till förvaltningens kärnverksamhet har också betydelse för att den samlade samhällsnyttan ska kunna realiseras.

[59] SOU 2017:114 *reboot – omstart för den digitala förvaltningen*, s. 127.
[60] ESV, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 10 och 40.
[61] SOU 2021:97 *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift*, s. 411.

Sammantaget anser utredningen att det är mest ändamålsenligt att kostnaderna för upphandling alternativt utveckling, förvaltning och drift av den föreslagna tjänsten finansieras genom anslag och att tjänsten tillhandahålls till offentliga aktörer kostnadsfritt.

Anslagsfinansiering av tjänsten är förenligt med reglerna om offentlig upphandling

Att tillhandahålla en förvaltningsgemensam tjänst för säker flerpartsberäkning kostnadsfritt till kommuner och regioner innebär inte köp av en tjänst i upphandlingsrättslig mening. Det handlar inte heller om att någon affärsrelation upprättas mellan parterna eller om tilldelning av kontrakt så som avses i lagen om offentlig upphandling. Därför faller en kostnadsfri tjänst utanför lagens tillämpningsområde. Om en förvaltningsgemensam tjänst däremot skulle finansieras genom avgifter är det utredningens uppfattning att det skulle utgöra köp av tjänst och upphandlingsregelverket skulle då vara tillämpligt för kommuner och regioner.

Anslagsfinansiering av tjänsten är förenligt med statsstödsregelverket

En statlig myndighet som tillhandahåller en förvaltningsgemensam tjänst för integritetsfrämjande teknik utgör en del av staten och fullgör i normalfallet offentliga uppgifter. Att verksamheten finansieras genom anslag innebär inte i sig att finansieringen utgör statligt stöd. Den avgörande frågan är i stället om tillhandahållandet av tjänsten ska anses utgöra ekonomisk verksamhet.

Även om den aktuella typen av tjänst i och för sig kan förekomma på en marknad och tillhandahållas av privata aktörer, kan verksamheten i det aktuella sammanhanget bedömas som icke-ekonomisk. Det gäller under förutsättning att den är strikt begränsad till att stödja offentlig förvaltning och myndighetsutövning samt bedrivs utan inslag av försäljning, kommersialisering eller öppen tillgång för privata aktörer. Om tjänsten uteslutande används av statliga myndigheter, kommuner och regioner för fullgörande av offentliga uppgifter och inte bedrivs i konkurrens med privata aktörer, så utgör anslagsfinansiering inte statligt stöd.

Användningen av förvaltningsgemensamma tjänster kan också aktualisera frågan om indirekt statsstöd för de som använder en förvaltningsgemensam tjänst. Statliga myndigheter, kommuner och regioner utgör som utgångspunkt inte företag när de agerar inom ramen för offentlig förvaltning och myndighetsutövning. Deras verksamhet är i regel inte av ekonomisk natur utan de är offentligrättsliga organ med ansvar för att fullgöra lagstadgade uppgifter. Kostnadsfri tillgång till statligt finansierade tjänster för interna eller offentliga ändamål innebär därför normalt inte att dessa aktörer erhåller någon ekonomisk fördel i statsstödsrättslig mening. I den mån en förvaltningsgemensam tjänst för integritetsfrämjande teknik används för uppgifter som är att betrakta som icke-ekonomiska uppkommer således inget indirekt statsstöd. Om tjänsten däremot används i verksamheter som utgör ekonomisk verksamhet, exempelvis kommunal säljverksamhet eller annan marknadsinriktad verksamhet, kan den kostnadsfria tillgången däremot innebära en selektiv ekonomisk fördel och utgöra ett indirekt statsstöd. Kommuner och regioner, som bedriver både ekonomisk och icke-ekonomisk verksamhet, kan ta emot stöd för den icke-ekonomiska verksamheten under förutsättning att finansieringen hålls åtskild så att ingen risk för korssubventionering av den ekonomiska verksamheten föreligger. Däremot görs inte samma bedömning gällande kommunala bolag som bedriver ekonomisk verksamhet eller privata utförare. Dessa omfattas av företagsbegreppet och kan därmed, till skillnad från kommuner och regioner i deras offentligrättsliga roll, inte ges tillgång till tjänster av detta slag avgiftsfritt utan att statsstödsreglerna aktualiseras.

Ett statsstödsrättsligt tillåtet upplägg för en förvaltningsgemensam tjänst för säker flerpartsberäkning förutsätter en tydlig avgränsning av tjänstens ändamål och användning. Tjänsten behöver utformas som en del av statens icke-ekonomiska digitala infrastruktur för offentlig förvaltning, med formellt fastställda användningsvillkor som begränsar tillgången till offentliga aktörer och till användning för offentliga uppgifter. Om regeringen anser att tjänsten ska finansieras med anslag kan det finnas skäl att överväga att anmäla åtgärden till Europeiska kommissionen i enlighet med artikel 108.3 EUF-fördraget, för att säkerställa att tjänsten verkligen utformats på ett tillåtet sätt.

Anslagsfinansiering av tjänsten är förenligt med konkurrensrätten

Tillhandahållandet av en förvaltningsgemensam tjänst för säker flerpartsberäkning utgör en offentlig säljverksamhet, även om det sker kostnadsfritt till den offentliga förvaltningen. Att det sker till följd av ett regeringsuppdrag innebär att det inte träffas av förbudet mot otillbörlig offentlig säljverksamhet.[62] Regeringen behöver dock överväga vilka skäl som finns för att ge ett sådant uppdrag och om de skälen väger tyngre än konkurrensintresset.

Det ligger i samhällets intresse att ha en datadriven offentlig förvaltning som utvecklar digitala tjänster och därigenom underlättar för enskilda och företag samt främjar innovation. Användningen av integritetsfrämjande teknik för att möjliggöra en modern datadelning inom förvaltningen utgör ett medel för att uppnå detta. Mot denna bakgrund bedömer utredningen att det är av vikt för samhället att de förvaltningsgemensamma tjänster som utvecklas också kan användas i så stor omfattning som möjligt.

Användning av säker flerpartsberäkning inom förvaltningen skapar förutsättningar för betydande effektiviseringsvinster och samhällsnyttor inom flera verksamhetsområden. Utredningens samhällsekonomiska analys visar på att tillhandahållandet av en sådan tjänst har potential att frigöra betydande nyttor för samhället i stort och inte enbart för förvaltningen.[63] Nyttorna kan således även komma enskilda och företag till del, såväl direkt som indirekt. Säker flerpartsberäkning möjliggör bland annat mer avancerade databaserade analyser på aggregerad nivå, exempelvis av näringslivs- eller befolkningsdata, utan att enskilda uppgifter behöver röjas. Sådana analyser kan användas som underlag för planering och uppföljning inom områden som infrastruktur, arbetsmarknadspolitik och krisberedskap. Det bidrar till förbättrad samhällsplanering som i sin tur leder till nyttor för samhället i stort.

Inom hälso- och sjukvården kan säker flerpartsberäkning möjliggöra relevanta analyser och jämförelser utan att känsliga patientuppgifter exponeras. Det skapar bättre förutsättningar för en mer kunskapsbaserad och ändamålsenlig vård, där förbättringsområden kan identifieras tidigare och åtgärder vidtas snabbare. Det kan exempelvis vara genom att avvikelser i behandlingsresultat eller vård-

[62] 3 § lagen om offentlig säljverksamhet.
[63] Bilaga 2, *Samhällsekonomisk analys*, s. 71.

processer uppmärksammas i ett tidigt skede. Sammantaget kan detta bidra till både kostnadseffektivitet och ökad nytta för patienterna.

Genom användning av säker flerpartsberäkning kan beslut fattas snabbare och med högre precision utan att mer information än nödvändigt exponeras. För enskilda och företag kan detta innebära kortare handläggningstider och ett minskat behov av att lämna samma uppgifter till flera myndigheter. Det minskar den administrativa bördan, ökar rättssäkerheten och reducerar risken för felaktiga eller motstridiga beslut. För företag frigörs därigenom resurser som kan användas inom deras kärnverksamhet.

Utredningen anser därför att intresset av att främja användningen av en förvaltningsgemensam tjänst för säker flerpartsberäkning, som ett verktyg för en mer datadriven offentlig förvaltning, väger tyngre än konkurrensintresset i detta sammanhang.

8.5.6 Finansiering av framtida förvaltningsgemensamma tjänster bör bedömas för respektive tjänst

Utredningens bedömning

Hur framtida tjänster inom ramen för uppdraget att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik ska finansieras bör bedömas för respektive tjänst.

Skälen för utredningens bedömning

Utgångspunkten bör vara att anslagsfinansiering är den mest ändamålsenliga finansieringen även av framtida förvaltningsgemensamma tjänster för integritetsfrämjande teknik. En sådan finansiering ger långsiktigt stabila förutsättningar för utveckling, förvaltning och användning. Den möjliggör dessutom att tjänsterna kan komma hela förvaltningen till del, oavsett aktörernas storlek eller ekonomiska förutsättningar. Det är en förutsättning för att uppnå avsedd samhällsnytta.

Det går dock inte på förhand att avgöra om alla tjänster som kan komma att erbjudas inom ramen för uppdraget kan finansieras genom anslag och erbjudas kostnadsfritt till förvaltningen. Bedömningen behöver i stället göras för respektive tjänst och beakta den nytta som

den aktuella tjänsten kan tänkas skapa på motsvarande sätt som utredningen har gjort för tjänsten för säker flerpartsberäkning (se avsnitt 8.5.5). Med hänsyn till att den totala samhällsnyttan som användningen av integritetsfrämjande teknik kan skapa bedömer utredningen dock att det bör vara möjligt att finansiera även andra tjänster genom anslag även om en slutlig bedömning behöver göras för respektive tjänst.

8.6 Bearbetning av data i en förvaltningsgemensam tjänst för säker flerpartsberäkning

8.6.1 Beskrivning av användningsprocessen för analyser i en förvaltningsgemensam tjänst

När data bearbetas i en förvaltningsgemensam tjänst för säker flerpartsberäkning kan flera rättsliga frågor aktualiseras. För att identifiera de frågor som kan bli aktuella och för att bedöma dessa, behöver man förstå hur en sådan tjänst kan utformas och hur processen för användning kan se ut.

Utredningen redogör i det följande avsnittet översiktligt för hur en process för användning av den förvaltningsgemensamma tjänsten kan se ut vid en uppföljning och kontroll av utbetalningar från välfärdssystemen. I detta fiktiva exempel har Försäkringskassan identifierat ett behov av att analysera förekomst av samtidig utbetalning av sjukpenning eller bostadsbidrag i kombination med kommunalt ekonomiskt bistånd. Försäkringskassan har uppgifter om utbetalning av sjukpenning samt bostadsbidrag och socialtjänsten i en eller flera kommuner kan bidra med uppgifter om ekonomiskt bistånd enligt socialtjänstlagen (2025:400). Den tekniska beskrivningen har inspirerats av arkitekturbeskrivningen[64] i projektet JOCONDE (se avsnitt 4.4.6).

[64] Se teknisk rapport *JOCONDE D4.1 System Specification and Architecture 1.0* https://cros.ec.europa.eu/joconde (hämtad 2026-03-13).

Identifiering av behov och relevanta datamängder

Det första steget är att identifiera vilken data som behövs för att kunna generera nya insikter eller ta fram förslag på lösningar för det definierade problemet. I detta skede fastställs även vilka aktörer som behöver bidra med data till analysen och en dialog inleds med dessa för att precisera vilka datamängder som är nödvändiga, deras struktur samt på vilket sätt data behöver delas för att möjliggöra en relevant och tillförlitlig analys.

I vårt fiktiva exempel inleds därför en dialog mellan Försäkringskassan och socialtjänsten för att precisera vilka uppgifter som är nödvändiga, exempelvis tidsperioder för utbetalningar, ersättningstyper och hur uppgifterna behöver struktureras för att möjliggöra en relevant och tillförlitlig analys.

Förberedelse inför användning av tjänsten

Innan en förvaltningsgemensam tjänst för säker flerpartsberäkning ska användas behöver de offentliga aktörer som avser att använda tjänsten fastställa vilken beräkning (algoritm) som ska utföras i tjänsten samt vilket kryptografiskt protokoll som ska tillämpas. Det kan exempelvis röra sig om en beräkning som identifierar individer som under samma period uppbär ekonomiskt bistånd från kommunen och sjukpenning från Försäkringskassan, eller där bostadsbidrag kombineras med inkomster som överstiger vissa tröskelvärden.

Därefter identifierar respektive aktör vilka datamängder som ska ingå i beräkningen och gör nödvändiga förberedelser av dessa. För Försäkringskassan kan detta avse uppgifter om utbetalda förmåner och för socialtjänsten uppgifter om beviljade försörjningsstöd.

Respektive aktör krypterar sedan sin data innan överföringen till tjänsten. Efter att krypteringen skett kan krypteringsnycklarna gallras eller raderas, under förutsättning att det är förenligt med arkivlagstiftningen.

Bearbetning av data i tjänsten

Vid den efterföljande beräkningen i den förvaltningsgemensamma tjänsten distribueras data mellan aktörerna på ett sådant sätt att ingen deltagande aktör får tillgång till andra aktörers uppgifter i klartext. Försäkringskassan och socialtjänsten kan därmed delta i samma analys utan att få insyn i varandras uppgifter.

Genom lokala beräkningar och strukturerade meddelandeutbyten genomförs de operationer som krävs för att identifiera exempelvis överlappande ersättningsperioder eller avvikande kombinationer av stöd. Protokollet är utformat så att endast den information som är absolut nödvändig för att föra beräkningen vidare bearbetas i varje steg.

Resultatet av analysen

När alla beräkningssteg är genomförda erhåller respektive aktör en del av resultatet. Dessa resultatdelar kombineras sedan i tjänsten för att skapa det slutliga resultatet. Det innebär att aktörerna kan tillgodogöra sig ett resultat utan att dela sina underliggande data med varandra.

Resultatet, liksom de resultatdelar som hanteras i processen, skyddas genom kryptering. De krypteringsnycklar som krävs för att få tillgång till resultatet tillhandahålls från tjänsten till aktörerna. Åtkomsten till krypteringsnycklarna kan begränsas till specifika funktioner, exempelvis kontroll- eller analysenheter hos Försäkringskassan eller kommunens socialförvaltning. Resultatet från analysen kan därefter användas för att initiera riktade kontroller eller fördjupade granskningar inom respektive aktörs ordinarie verksamhet, i enlighet med gällande regelverk.

8.6.2 Personuppgiftsansvaret i en förvaltningsgemensam tjänst

Utredningens bedömning

Den eller de aktörer som bestämmer ändamål och medel för den behandling som kommer ske i samband med användning av en förvaltningsgemensam tjänst för säker flerpartsberäkning är personuppgiftsansvarig.

Skälen för utredningen bedömning

Bedömningen av personansvaret måste ske utifrån de faktiska omständigheterna

I syfte att beskriva de ställningstaganden som en aktör som vill bearbeta data i en gemensam tjänst behöver göra har utredningen gjort en bedömning av hur personuppgiftsansvaret skulle kunna vara fördelat när en förvaltningsgemensam tjänst för säker flerpartsberäkning används. Vem som är personuppgiftsansvarig för en behandling bedöms utifrån de faktiska omständigheterna.

Ensamt eller gemensamt personuppgiftsansvar

För det förberedande steget av processen ansvarar respektive aktör för sin behandling av personuppgifter. I detta skede behandlas personuppgifterna för respektive aktörs eget ändamål, vilket exempelvis kan vara att genomföra en analys för ett visst syfte eller att lämna ut uppgifter som har begärts.

När uppgifterna sedan överförs till tjänsten för bearbetning, behöver personuppgiftsansvaret bedömas utifrån den aktuella situationen och för vems ändamål som bearbetningen sker. Om de deltagande aktörerna gemensamt har bestämt att den förvaltningsgemensamma tjänsten för säker flerpartsberäkning (medel) ska användas eller tillsammans har ett intresse av resultatet från bearbetningen (ändamål) så talar det för att det föreligger ett gemensamt personuppgiftsansvar. Det är viktigt att de aktörer som vill använda sig av en tjänst för säker flerpartsberäkning noga överväger hur

personuppgiftsansvaret kan komma att bli fördelat och säkerställer att respektive parts ansvar fastställs (se också avsnitt 2.4.2).

Skulle det i stället vara så att endast en aktör har intresse av resultatet och begär uppgifter från andra aktörer till sin analys talar det för att den aktören ensamt bör ses som personuppgiftsansvarig för den bearbetning som sker i den förvaltningsgemensamma tjänsten.

Tillhandahållaren av tjänsten är personuppgiftsbiträde

Den aktör som tillhandahåller tjänsten, i vårt förslag Skatteverket, utför endast en teknisk bearbetning av uppgifterna på uppdrag av de aktörer som vill få bearbetningen utförd. Skatteverket bör därför anses behandla personuppgifter i egenskap av personuppgiftsbiträde.

Utredningen anser inte att det är nödvändigt att särskilt reglera personuppgiftsansvaret för den personuppgiftsbehandling som kommer ske hos Skatteverket. Det är tillräckligt tydligt att det är den eller de aktörer som vill nyttja tjänsten som bestämmer ändamålet för behandlingen och därmed ansvarar för personuppgiftsbehandlingen. Utredningen har konstaterat att behandling av personuppgifter genom integritetsfrämjande teknik är en skyddsåtgärd som syftar till att uppfylla kraven i dataskyddsförordningen. Utredningen har också bedömt att den behandling som sker med teknikerna inte behöver en egen rättslig grund och ett eget ändamål (se avsnitt 7.3.2–7.3.3). Att uppgifterna bearbetas av ett personuppgiftsbiträde (Skatteverket) förändrar inte detta.

8.6.3 Bearbetning i en förvaltningsgemensam tjänst medför att underliggande uppgifter inte röjs

Utredningens bedömning

När data bearbetas under kryptering i en förvaltningsgemensam tjänst för säker flerpartsberäkning röjs inte de underliggande uppgifterna.

Skälen för utredningens bedömning

När en uppgift skyddas av en kryptografisk funktion som hindrar mottagaren att ta del av uppgiftens informationsbärande innehåll, bör den inte betraktas som röjd enligt offentlighets- och sekretesslagen.[65] Som utredningen redogjort för tidigare upplever offentliga aktörer det oklart vad som krävs för att en krypterad datamängd inte ska anses röjd (se avsnitt 6.4.2). En viktig åtgärd för att säkerställa att krypteringen inte bryts, och uppgifterna därigenom röjs, är att krypterade data och krypteringsnycklar inte hanteras under en längre tid än nödvändigt (se avsnitt 7.5.3).

En viktig fråga i sammanhanget är för vilken tid krypteringen behöver skydda uppgifterna. Utredningen anser att en rimlig utgångspunkt är att krypteringens hållbarhet behöver sträcka sig över den tid som den krypterade datamängden ska bearbetas i tjänsten. En bearbetning med säker flerpartsberäkning är inte tänkt att pågå under någon längre tid vilket gör att föråldrade krypteringsalgoritmer sällan bör vara ett problem. Vid en användning av säker flerpartsberäkning kan samtliga datadelande parter på förhand få en uppfattning om hur lång tid som bearbetningen kommer att pågå. Så snart bearbetningen genomförts finns det inget behov av att spara de krypterade uppgifterna och dessa kan raderas från tjänsten. Tidpunkten för när de krypterade uppgifterna ska raderas bör regleras med den som tillhandahåller tjänsten, exempelvis i ett personuppgiftsbiträdesavtal. Det saknas därför skäl att bedöma möjligheterna till att bryta krypteringen senare än vid denna tidpunkt.

Genom samverkan med FRA kan det säkerställas att de krypteringslösningar som väljs för den förvaltningsgemensamma tjänsten har en sådan hållbarhet att de krypterade uppgifterna inte anses röjda under den tid som uppgifterna hanteras i tjänsten.

[65] Prop. 2022/23:97 *Sekretessbrott vid utlämnande för teknisk bearbetning eller teknisk lagring av uppgifter*, s. 7.

8.6.4 Resultatet från en förvaltningsgemensam tjänst är en ny allmän handling

Utredningens bedömning

Analysresultatet från en förvaltningsgemensam tjänst för säker flerpartsberäkning utgör en allmän handling hos den som tagit del av analysresultatet.

Skälen för utredningens bedömning

Med handling avses en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt.[66] En sådan handling är allmän om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos en myndighet.[67] Något förenklat kan sägas att en handling är att anses som inkommen när någon annan har gjort den tillgänglig för myndigheten.[68] En handling är bland annat upprättad, om handlingen inte hänför sig till ett visst ärende, när den har justerats av myndigheten eller färdigställts på annat sätt.[69]

När en säker flerpartsberäkning har genomförts genereras ett analysresultat. Utredningens bedömning är att analysresultatet utgör en allmän handling hos de som deltagit i beräkningen och som faktiskt har tagit del av analysresultatet. Detta följer av att handlingen då får anses både upprättad och förvarad hos respektive aktör i och med att de deltagit i analysen och tar del av resultatet.

Utredningen konstaterar dock att samtliga deltagande aktörer i alla situationer inte kommer ta del av analysresultatet. Situationen kan även vara den omvända, det vill säga att en aktör endast tar del av analysresultatet utan att bidra med data till analysen. En allmän handling uppkommer endast hos den aktör som faktiskt tar del av analysresultatet, antingen som en upprättad eller inkommen handling.

[66] 2 kap. 3 § tryckfrihetsförordningen, TF.
[67] 2 kap. 4 § TF.
[68] 2 kap. 9 § första stycket TF.
[69] 2 kap. 10 § TF.

8.6.5 Befintligt rättsligt skydd är tillräckligt för data i en förvaltningsgemensam tjänst

Utredningens bedömning

De handlingar som överförs till en förvaltningsgemensam tjänst för säker flerpartsberäkning blir inte allmänna handlingar hos Skatteverket.

Framtida förvaltningsgemensamma tjänster bör kunna utformas så att det skydd som finns i verksamhet för teknisk bearbetning och teknisk lagring kan tillämpas.

Skälen för utredningens bedömning

Data i en förvaltningsgemensam tjänst blir inte allmänna handlingar hos Skatteverket

En förvaltningsgemensam tjänst för säker flerpartsberäkning kännetecknas av att den behandlar data som tillhandahålls av flera självständiga parter i syfte att möjliggöra gemensamma beräkningar utan att parterna röjer de underliggande uppgifterna för varandra. Den förvaltningsgemensamma tjänstens funktion är i huvudsak teknisk. Den tar emot och bearbetar krypterade data enligt förutbestämda protokoll, utan att själv kunna tillgodogöra sig innehållet i klartext.

En handling enligt tryckfrihetsförordningen är en framställning i skrift eller bild samt en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt (se avsnitt 8.6.4). Handlingen anses vara allmän om den är förvarad hos en myndighet samt upprättad av eller inkommen hos myndigheten. Som huvudregel anses en upptagning förvarad hos en myndighet om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas eller avlyssnas eller uppfattas på annat sätt.[70] Handlingar som förvaras hos en myndighet enbart som ett led i teknisk lagring eller teknisk bearbetning för annans räkning anses dock inte vara förvarade hos myndigheten.[71] Undantaget tar sikte på situationer där myndigheten endast fungerar som ett tekniskt mellanled, där data

[70] 2 kap. 6 § första stycket TF.
[71] 2 kap. 13 § första stycket TF.

behandlas uteslutande på uppdrag av någon annan och i enlighet med dennes instruktioner.

Den förvaltningsgemensamma tjänsten för säker flerpartsberäkning får anses utgöra ett sådant tekniskt mellanled. I tjänsten behandlas data uteslutande på uppdrag av de deltagande parterna och i enlighet med deras instruktioner. Att tjänsten utgör ett tekniskt mellanled förstärks ytterligare av att uppgifterna är krypterade på ett sätt som innebär att tillhandahållaren av tjänsten inte har möjlighet att rekonstruera eller ta del av det underliggande informationsinnehållet. Den data som överförs är krypterad redan innan den överförs till tjänsten och Skatteverket behöver inte ha tillgång till krypteringsnycklarna. Innehållet i den krypterade datan är inte tillgängligt för Skatteverket på ett sådant sätt att de kan ta del av den.

Att de krypteringsnycklar som krävs för att få tillgång till resultatet tillhandahålls via den förvaltningsgemensamma tjänsten innebär inte att Skatteverket, i rollen som tillhandahållare av tjänsten, får tillgång till dessa nycklar. Eftersom Skatteverket saknar tillgång till nycklarna kan myndigheten inte få tillgång till vare sig resultatet eller underliggande data. Krypteringsnycklar kan visserligen utgöra allmänna handlingar men i många fall omfattas dessa av sekretess eftersom själva syftet med krypteringen annars skulle motverkas. Om den data som har krypterats inför en säker flerpartsberäkning omfattas av sekretess, omfattas även krypteringsnycklar av sekretess.[72] Sekretessen för säkerhets- och bevakningsåtgärder kan också vara tillämplig på krypteringsnycklarna, även om den krypterade datan inte omfattas av sekretess.[73]

Sammanfattningsvis konstaterar utredningen att Skatteverket inte kommer att få tillgång till vare sig resultatet eller underliggande data. Bearbetningen utgör dessutom ett tekniskt mellanled som omfattas av undantaget från allmänna handlingar. Mot denna bakgrund bedömer utredningen att handlingar som förekommer i den förvaltningsgemensamma tjänsten för säker flerpartsberäkning inte kommer utgöra allmänna handlingar hos Skatteverket.

[72] 18 kap. 9 § första stycket offentlighets- och sekretesslagen (2009:400), OSL.
[73] 18 kap. 8 § OSL.

Tillräckligt skydd för framtida tjänster

Utredningen har, av de skäl som redovisas i avsnitt 8.4.3, inte funnit det lämpligt att begränsa uppdraget om förvaltningsgemensamma tjänster till vissa tekniker. Det innebär att vi inte heller föreslår vilka specifika tekniker som det i framtiden bör finnas förvaltningsgemensamma tjänster för. Vilket skydd som behövs för den data som kommer att behandlas i sådana framtida tjänster kommer därför behöva bedömas utifrån omständigheterna i det enskilda fallet.

Utredningen bedömer dock att även framtida förvaltningsgemensamma tjänster bör kunna utformas på ett sådant sätt att undantaget för teknisk lagring eller bearbetning för annans räkning är tillämpligt.[74] Det innebär att den data som behandlas inom ramen för sådana tjänster inte blir allmänna handlingar hos Skatteverket. Uppgifter om en enskilds personliga eller ekonomiska förhållanden, som behandlas inom verksamheten för teknisk lagring och teknisk bearbetning, omfattas även av absolut sekretess.[75]

Utredningen anser således att det befintliga regelverket bör ge ett tillräckligt skydd för de uppgifter som kommer bearbetas även i framtida förvaltningsgemensamma tjänster. Det finns därför inte skäl att föreslå åtgärder i syfte att ytterligare stärka skyddet.

8.7 Fler åtgärder för att öka datadelningen med integritetsfrämjande teknik

8.7.1 Det finns behov av uppdrag för att utforska integritetsfrämjande teknik

I de dialoger som utredningen har fört med representanter för olika offentliga aktörer har det framkommit att många varken har kapacitet eller ambition att ligga i framkant när det gäller att införa och använda ny teknik. Flera av dessa aktörer har vidare uttryckt en önskan om att andra inom förvaltningen ska gå före och visa hur integritetsfrämjande teknik kan tillämpas i praktiken samt vilka nyttor som kan uppnås genom sådan användning.

Även om det finns rättsliga förutsättningar för att offentliga aktörer ska kunna börja använda integritetsfrämjande teknik finns

[74] 2 kap. 13 § första stycket TF.
[75] 40 kap. 5 § OSL.

behov av ett mer aktivt genomförande. Detta kan lämpligen ske genom att vissa myndigheter ges i uppdrag att utforska användningen av sådan teknik. De erfarenheter och insikter som genereras genom sådana uppdrag kan sedan spridas till övriga delar av förvaltningen för att främja användningen.

8.7.2 Regeringsuppdrag att genomföra en samarbetsanalys med säker flerpartsberäkning

Utredningens förslag

Försäkringskassan och Skatteverket bör få i uppdrag att genomföra en samarbetsanalys med säker flerpartsberäkning.

Uppdraget bör ges som ett särskilt regeringsuppdrag.

Skälen för utredningens förslag

Säker flerpartsberäkning kan möjliggöra datadelning som i dag hindras av sekretess

Utredningen har tagit del av en aktuell datadelningssituation mellan Försäkringskassan och Skatteverket som hindras av sekretess. Bakgrunden till den aktuella situationen är att Försäkringskassan fått i uppdrag av regeringen att uppskatta felaktiga utbetalningar av vissa ersättningar. Uppdraget ska redovisas den 5 oktober 2026. I syfte att genomföra kvalitativa omfattningsstudier för uppdraget har Försäkringskassan begärt individuppgifter från Skatteverket. Uppgifterna omfattar en 12-månadersperiod för ungefär 1,3 miljoner personer. Uppgifterna omfattas av absolut sekretess hos Skatteverket.[76] Försäkringskassan har begärt att få del av uppgifterna med stöd av både 10 kap. 27 § och 10 kap. 15 § a OSL. Skatteverket har avslagit begäran.[77] Skälen för Skatteverkets beslut är att uppgifterna inte kommer omfattas av sekretess hos Försäkringskassan och att det vid en intresseavvägning inte är uppenbart att Försäkringskassans intresse väger tyngre än det som sekretessen ska skydda. Vidare anser Skatteverket att behovet av uppgifter för att svara på ett regeringsuppdrag ligger för långt ifrån de syften som finns i 10 kap. 15 a § OSL.

[76] Enligt 27 kap. 1 § OSL.
[77] Skatteverkets beslut, dnr 8-378-180-2025 och 8-82015-2026.

Detta även om analyserna på sikt kan komma att innebära att arbetet med att motverka och förhindra felaktiga utbetalningar förhindras.

Utredningens uppfattning är att den aktuella datadelningen hade kunnat möjliggöras med hjälp av säker flerpartsberäkning. I ett sådant scenario hade uppgifterna kunnat bearbetas under kryptering och Försäkringskassan hade kunnat få insikter om omfattningen utan att få del av de underliggande individuppgifterna. Det hade också varit möjligt att minska den uppgiftsmängd som lämnas ut till Försäkringskassan, så att den endast omfattar personer som faktiskt har fått ersättning från socialförsäkringen under aktuell period och kan antas ha fått felaktiga utbetalningar. Ett sådant resultat skulle Försäkringskassan kunna nyttja både i analysen för regeringsuppdraget och i sin kontrollverksamhet.

Det finns således potential för Skatteverket och Försäkringskassan att öka sin datadelning med hjälp av säker flerpartsberäkning. Det finns visserligen förutsättningar för myndigheterna att på eget initiativ påbörja användningen av integritetsfrämjande teknik. Utredningen bedömer ändå att myndigheterna bör få i uppdrag att genomföra en samarbetsanalys med säker flerpartsberäkning i syfte att testa tekniken och skapa konkret nytta för myndigheterna. Ett sådant uppdrag skulle ställa krav på myndigheterna att faktiskt börja använda integritetsfrämjande teknik för datadelning och ge myndigheterna incitament att hitta nya möjligheter att dela data. Uppdraget bör ges som ett särskilt regeringsuppdrag eftersom det avser en tidsbegränsad insats.

Att just Försäkringskassan och Skatteverket är de myndigheter som ska testa säker flerpartsberäkning har flera fördelar. Båda myndigheterna innehar stora datamängder som kan vara intressanta för andra att ta del av och basera sina insikter på. Det är också myndigheter som har kapacitet att omhänderta ny teknik och nya arbetssätt på ett effektivt sätt. Uppdraget kan även resultera i ett tidigt användningsfall av integritetsfrämjande teknik till den samling med exempel som Digg bör tillhandahålla inom ramen för uppdraget att ge och stöd och vägledning (se avsnitt 8.3.3). När stora myndigheter visar hur ny teknik kan användas och nyttorna med det, kan det inspirera fler offentliga aktörer att börja använda integritetsfrämjande teknik.

Vi har tidigare i detta kapitel föreslagit att Skatteverket ska tillhandahålla en tjänst för säker flerpartsberäkning till offentlig förvaltning. Det här uppdraget ger myndigheten en möjlighet att testa

tekniken i form av en pilot samtidigt som konkret nytta kan uppstå för myndigheterna. Det kan ge värdefulla insikter om vilka behov som en användare av tjänsten kan ha och bidra till att den förvaltningsgemensamma tjänsten får en ändamålsenlig utformning.

Vi anser att det inte finns behov av en särskild skriftlig redovisning av uppdraget. Slutsatser från uppdraget kan i stället inkluderas och redovisas i samband med delredovisningen av Skatteverkets uppdrag att tillhandahålla den förvaltningsgemensamma tjänsten för säker flerpartsberäkning, där bland annat erfarenheter och slutsatser från analys- och pilotfasen bör redovisas (se avsnitt 8.4.6).

8.7.3 Regeringsuppdrag att utforska differentiell integritet inom hälso- och sjukvård

Utredningens förslag

Socialstyrelsen bör få i uppdrag att utforska användningen av differentiell integritet och ett lämpligt spann för den tillåtna nivån av integritetsförlust (epsilon, ε) inom hälso- och sjukvård.

Uppdraget bör genomföras i samverkan med E-hälsomyndigheten, Myndigheten för digital förvaltning, Integritetsskyddsmyndigheten, Statistiska centralbyrån och minst en region.

Uppdraget bör ges som ett särskilt regeringsuppdrag.

Skälen för utredningens förslag

Det behövs kunskap om sektorsspecifik tillämpning av differentiell integritet

Inom hälso- och sjukvårdsområdet finns det stora nyttor som kan realiseras med hjälp av integritetsfrämjande teknik (se avsnitt 6.2.3) och ökad användning av AI. Differentiell integritet kan, utöver att användas när större datamängder ska offentliggöras[78], användas för att skapa träningsdata till en AI-modell. Det är möjligt att använda differentiell integritet både för att avidentifiera data som ska användas för träning och för att skapa syntetiska träningsdata. Inom hälso- och sjukvården kan sådan träningsdata både användas inom en region

[78] Som i Israel, se avsnitt 4.4.6.

för egen AI-träning och delas till andra regioner för träning av deras AI-modeller. Det finns också flera potentiella nyttor av att använda differentiell integritet vid sekundäranvändning av hälsodata, det vill säga för forskning, beslutsfattande och innovation.

För att användningen av differentiell integritet ska öka och nyttorna ska realiseras behöver det finnas specifik vägledning för valet av epsilon både när det används vid differentiell integritet och när det används för att skapa syntetiska data med differentiell integritet. Slutsatserna rörande nivån kan också användas av Digg för att ge vägledning om när teknikerna bör kombineras med varandra. Att tidigt utforska ett område som hanterar integritetskänsliga uppgifter kan också hjälpa Digg att dra slutsatser om lämpliga nivåer för andra sektorer och situationer.

Flera aktörer behöver samverka i uppdraget

Uppdraget bör ges till Socialstyrelsen mot bakgrund av myndighetens statistikansvar för bland annat hälso- och sjukvårdsområdet. Myndigheten ansvarar även för flertalet hälsodataregister. Data som finns hos Socialstyrelsen spänner över ett stort antal områden och mängden av känsliga personuppgifter är stort. Myndigheten har därför behov av att utveckla metoder för att skydda uppgifterna.

Uppdraget bör genomföras i samverkan med E-hälsomyndigheten som ansvarar för att samordna och etablera den nationella digitala infrastrukturen för hälsa, vård och omsorg. Infrastrukturen ska bland annat möjliggöra att dela information tryggt och säkert mellan olika system och aktörer. För att säkerställa att arbetet också ger praktisk nytta bör uppdraget genomföras i samverkan med minst en region.

Samverkan bör också ske med IMY och SCB. Utöver detta bör även samverkan ske med Digg mot bakgrund av myndighetens generella ansvar för stöd och vägledning om integritetsfrämjande teknik. Uppdraget bör ges som ett särskilt regeringsuppdrag eftersom det avser en tidsbegränsad insats.

Skriftlig redovisning av uppdraget kan bidra till förbättrad vägledning

Uppdraget bör redovisas skriftligt till Regeringskansliet, med en utförlig beskrivning av genomförandet och resultaten, så att slutsatser från uppdraget kan användas till att utveckla konkret vägledning vid användningen av differentiell integritet. Det gäller såväl inom hälso- och sjukvård som inom andra områden.

8.7.4 Regeringsuppdrag för att utforska opt-out-lösning

Utredningens förslag

E-hälsomyndigheten och Socialstyrelsen bör få i uppdrag att utforska integritetsfrämjande teknik för att hantera uppgifter om enskilda som har motsatt sig användning av deras hälsodata.

Uppdraget bör ges som ett särskilt regeringsuppdrag.

Skälen för utredningens förslag

Behov av opt-out-lösningar

Inom ramen för det europeiska hälsodataområdet (EHDS) kommer stora mängder personuppgifter behandlas, för såväl primäranvändning (i vård- och omsorgssammanhang) som för sekundäranvändning (för exempelvis forskning eller innovation). Inom primäranvändningen kan medlemsstaterna välja att införa en möjlighet för enskilda att motsätta sig att deras hälsodata tillgängliggörs för andra vårdgivare, så kallad opt-out. Det finns förslag på att en sådan möjlighet ska införas i Sverige och att Socialstyrelsen ska få i uppdrag att utreda formerna för hur en begäran om opt-out ska kunna återtas.[79] E-hälsomyndigheten utvecklar inom ramen för den nationella digitala infrastrukturen för hälsa, vård och omsorg en teknisk lösning för opt-out.[80]

För sekundäranvändningen ska enskilda enligt EHDS-förordningen kunna motsätta sig användningen av deras personuppgifter.

[79] Utredningen med uppdrag att möjliggöra en nationell digital infrastruktur (S 2024:A), Promemoria *Hälsodata ska vara tillgänglig i hela vårdkedjan*, s. 222 ff.
[80] E-hälsomyndigheten, dnr 2025/00346, *Etableringen av en nationell digital infrastruktur i hälso- och sjukvården och för primäranvändningen enligt EHDS-förordningen*, s. 53.

Det ska även finnas möjlighet att motsätta sig att bli underrättad om betydelsefulla upptäckter avseende sin hälsa som sekundäranvändning har lett till.[81] Det ska också vara möjligt att återta en begäran om opt-out avseende sekundäranvändningen. Socialstyrelsen har i uppdrag att förbereda för att bli ansvarigt organ för tillgång till hälsodata för sekundäranvändning (Health Data Access Body). Myndigheten har i sin delredovisning konstaterat att en funktion för hantering av opt-out ingår i de funktioner som ett organ för tillgång till hälsodata behöver utveckla.[82] Det är ännu inte beslutat vilken myndighet som får det nationella ansvaret för en funktion för opt-out.

Det är inte bara inom ramen för EHDS som det finns behov av opt-out-lösningar utan det kan tillämpas i olika situationer inom hela den offentliga förvaltningen. IMY har bland annat lyft möjligheten till opt-out som en åtgärd som kan göra att en vidarebehandling av personuppgifter anses förenlig med ursprungsändamålet.[83] Det kan till exempel vara när personuppgifter ska användas för att träna en AI-modell.

Integritetsfrämjande teknik kan användas för opt-out-lösningar

En utgångspunkt för hanteringen av uppgifter om enskilda som har valt att motsätta sig behandling av deras personuppgifter är att dessa uppgifter bör behandlas i så liten utsträckning som möjligt. Utredningen bedömer att en skyddsåtgärd som kan vidtas för opt-out-lösningar, framför allt inom sekundäranvändningen av hälsodata enligt EHDS, är att använda säker flerpartsberäkning. Det skulle kunna bidra till att stärka integritetsskyddet och minska onödig spridning av personuppgifter. Integritetsfrämjande teknik skulle därmed kunna fungera som ett komplement till andra skyddsåtgärder som vidtas för opt-out-lösningar.

Ett möjligt scenario är att den myndighet som utses till ansvarigt organ för tillgång till hälsodata har ett samlat register över de indi-

[81] Se artikel 58 och 71 i Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847); Socialstyrelsen, 2026, *Förbereda för att bli ansvarigt organ för tillgång till hälsodata enligt EHDS*, delrapport, s. 28 f.
[82] Socialstyrelsen, 2026, *Förbereda för att bli ansvarigt organ för tillgång till hälsodata enligt EHDS*, delrapport, s. 28.
[83] IMY, *Vidarebehandling av personuppgifter i vårdnadsärenden för att träna en AI-modell*.

vider som har valt att utnyttja rätten till opt-out vid sekundäranvändning. Detta register kan krypteras och jämföras med krypterade uppgifter om vilka individer som ingår i en datainnehavares datamängd. Datainnehavaren kan därigenom identifiera vilka individer som ska exkluderas utan att få kännedom om samtliga individer som har utnyttjat rätten till opt-out. På så vis begränsas behandlingen av personuppgifter för de personer som har valt opt-out. Om säker flerpartsberäkning inte används kan uppgifter om vilka enskilda som omfattas av opt-out behöva spridas till berörda datainnehavare, så att dessa kan exkluderas från respektive datamängd. Ett alternativ är att organet med ansvar för tillgång till hälsodata själv exkluderar dessa individer efter att datamängderna har lämnats in för sekundäranvändning. Båda dessa lösningar innebär dock att personuppgifter om individer som motsatt sig behandling för sekundära ändamål behandlas av flera aktörer.

Ett uppdrag för att utforska opt-out med integritetsfrämjande teknik

I syfte att främja användningen av integritetsfrämjande teknik, och inspirera andra aktörer till att använda opt-out-lösningar med integritetsfrämjande teknik, bör E-hälsomyndigheten och Socialstyrelsen få i uppdrag att utforska användningen av integritetsfrämjande teknik för opt-out. Det skulle vara ett sätt för regeringen att särskilt styra mot en ökad användning av integritetsfrämjande teknik inom ramen för det arbete som redan sker i samband med införandet av EHDS.

E-hälsomyndigheten har fått i uppdrag att förbereda för rollen som myndighet för digital hälsa enligt EHDS-förordningen.[84] Myndigheten ska också utreda förutsättningarna för att vara samordnande myndighet för digital hälsa. Socialstyrelsen har fått i uppdrag att förbereda för att bli ansvarigt organ för tillgång till hälsodata för sekundäranvändning enligt EHDS-förordningen. Med hänsyn till myndigheternas föreslagna roller inom EHDS är det sannolikt dessa som kommer att ansvara för att rätten till opt-out enligt EHDS tillgodoses.

Arbetet bör ske i samverkan med Skatteverket, Digg och IMY. Vidare bör uppdraget utgå från de strukturer för samarbete och

[84] Socialdepartementet, S2026/00910, *Uppdrag till E-hälsomyndigheten att förbereda för rollen som myndighet för digital hälsa enligt EHDS-förordningen*.

samverkan som finns inom EHDS med regioner för att fånga in deras perspektiv.

Uppdraget bör inte vara särskilt inriktad på att använda säker flerpartsberäkning för lösningen, eftersom det kan finnas skäl som talar emot att just den tekniken används. Det kan också vara så att andra integritetsfrämjande tekniker, så som nollkunskapsbevis, är mer lämpliga för att lösa behoven. Det kan vidare finnas skäl mot att använda integritetsfrämjande teknik över huvud taget för opt-out-lösningar om andra skyddsåtgärder är mer effektiva och ändamålsenliga. Behovet av att använda integritetsfrämjande teknik kan också skilja sig åt för olika opt-out-lösningar, till exempel vad gäller primär- och sekundäranvändning.

Uppdraget bör ta hänsyn till de pågående uppdrag och den pågående utveckling som sker avseende opt-out enligt EHDS-förordningen, till exempel avseende E-hälsomyndighetens och Socialstyrelsens respektive uppdrag, samt den utredning som har i uppdrag att möjliggöra en nationell digital infrastruktur för hälsodata (S 2024:A).

Skriftlig redovisning av uppdraget kan bidra till spridning av erfarenheter

Utredningen bedömer att uppdraget bör redovisas skriftligt till Regeringskansliet med en utförlig beskrivning av genomförandet och resultaten. De erfarenheter och slutsatser som E-hälsomyndigheten och Socialstyrelsen drar om användningen av integritetsfrämjande teknik för opt-out kan vara användbara för andra delar av den offentliga förvaltningen. Redovisningen kan på så sätt fungera som ett underlag för detta.

9 Konsekvenser

9.1 Inledning

Av förordningen (2024:183) om konsekvensutredningar framgår att kommittéer och särskilda utredare ska redovisa en konsekvensutredning för alla förslag som lämnas i ett betänkande. Konsekvensutredningen ska bland annat redogöra för kostnader och intäkter för staten, kommuner, regioner, företag och andra enskilda. Den ska även redogöra för andra relevanta konsekvenser för dessa aktörer. Det centrala syftet med konsekvensutredningar är att säkerställa att nyttan överstiger kostnaderna för samhället som helhet. Den syftar till att ge en systematisk och objektiv bedömningsgrund som skapar förståelse för de sammanvägda konsekvenserna av olika åtgärdsförslag på samhället och dess aktörer.[1]

Enligt kommittéförordningen (1998:1474) ska kommittéer, om förslagen medför kostnadsökningar eller intäktsminskningar för staten, även föreslå en finansiering som har anknytning till utredningens område och ange skäl för den föreslagna finansieringen. Av våra direktiv framgår att vi särskilt ska beakta att finansieringslösningarna utformas enligt principerna om god budgetdisciplin, hög kostnadseffektivitet och hög samhällsekonomisk effektivitet.

I detta kapitel redogör vi för konsekvenserna av utredningens förslag. Vi beskriver inledningsvis det aktuella problemet som utredningen ska lösa (avsnitt 9.2). Vi beskriver sedan de övergripande konsekvenserna av ett nollalternativ, där inga åtgärder vidtas, samt de åtgärder som utredningen föreslår (avsnitt 9.3 och 9.4). Därefter redogör vi för de möjliga nyttor och andra konsekvenser som vi bedömer att våra förslag har för olika aktörer och utifrån olika perspektiv. Det inkluderar även kostnaderna för våra förslag (avsnitt 9.5–9.10).

[1] https://forum.statskontoret.se/konsekvensutredning/utgangspunkter/verktyg-for-bedomning-och-analys/ (hämtad 2026-05-14).

Vi redogör också för finansieringen av utredningens förslag (avsnitt 9.11). Slutligen beskriver vi tidsplanen för genomförandet av de förslag utredningen lämnar, samt behovet av uppföljning och utvärdering av förslagen (avsnitt 9.12–9.13).

9.2 Integritetsfrämjande teknik är en viktig pusselbit för en förbättrad datadelning

9.2.1 Förutsättningarna för att dela vissa datamängder är i dag begränsade

Data är grunden för digitaliseringen av samhället. Data blir även allt viktigare i takt med utvecklingen av AI, vilket kräver tillgång till stora datamängder för träning. Flera utredningar har betonat vikten av en ökad datadelning för att kunna effektivisera och förbättra kvaliteteten på verksamheter i offentlig förvaltning samt för att skapa en mer sammanhållen och behovsanpassad service till invånare och företag.[2] Ett ökat tillgängliggörande av data anses ha stor nyttopotential när det gäller att bidra till nya lösningar och innovation. Det kan i sin tur kan skapa en ökad konkurrenskraft och tillväxt.[3]

Det pågår för närvarande flera insatser för att möjliggöra en ökad datadelning, såväl inom Sverige som inom EU. Dessa insatser omfattar bland annat förändringar i regelverk och åtgärder för att stärka den grundläggande digitala infrastrukturen för datadelning genom ökad interoperabilitet.[4] Samtidigt förfogar offentliga aktörer över stora mängder data som i dagsläget endast i begränsad utsträckning kan tillgängliggöras och delas inom förvaltningen. En bidragande orsak till detta är att uppgifterna i många fall innehåller personuppgifter. För att säkerställa skyddet för den personliga integriteten finns det rättsliga begränsningar för när uppgifter får behandlas och delas. Dessa begränsningar följer bland annat av dataskyddsförordningen[5] och bestämmelserna i offentlighets- och sekretesslagen (2009:400). Offentliga aktörer har därmed ett ansvar att säkerställa

[2] Se t.ex. SOU 2023:96 *En reform för datadelning*, SOU 2024:33 *Delad hälsodata – dubbel nytta* och SOU 2025:96 *Fler möjligheter till ökat välstånd*.
[3] Se t.ex. SOU 2025:96.
[4] Prop. 2025/26:244 *Nya krav på interoperabilitet vid datadelning inom den offentliga förvaltningen.*
[5] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

att hanteringen av data sker i enlighet med gällande regelverk och med respekt för enskildas rätt till privatliv.[6]

Flera aktörer har framhållit att det finns ett behov av att åstadkomma en bättre balans mellan å ena sidan möjligheterna till ökad datadelning och å andra sidan ett starkt skydd för den personliga integriteten. En sådan balans bedöms vara en förutsättning för att den fulla potentialen i de datamängder som finns i offentlig förvaltning ska kunna tas till vara.[7]

9.2.2 Teknikerna kan möjliggöra en förbättrad datadelning – men kunskapen behöver öka

Integritetsfrämjande teknik har i takt med den tekniska utvecklingen allt oftare lyfts fram som ett viktigt verktyg för att möjliggöra en förbättrad datadelning. Sådana tekniker kan komplettera befintliga regelverk för integritetsskydd och minska riskerna för intrång i den personliga integriteten vid delning av data.[8] Särskilt de moderna teknikerna möjliggör ett förbättrat data- och integritetsskydd vid datadelning, till exempel genom avidentifiering, uppgiftsminimering och skyddad bearbetning.

Inom offentlig förvaltning används moderna integritetfrämjande tekniker i begränsad omfattning. Det innebär att det finns en betydande underutnyttjad potential i form av datamängder som inte kan tillgängliggöras eller delas. Detta gäller i synnerhet inom områden som hanterar stora mängder känsliga uppgifter, till exempel inom hälso- och sjukvård. Samtidigt innebär ökade möjligheter för datadelning mellan offentliga aktörer också större risker för den personliga integriteten. Användningen av integritetsfrämjande teknik kan i detta sammanhang utgöra en skyddsåtgärd för att hantera och minska sådana risker.

Mot denna bakgrund finns ett behov av att i större utsträckning använda integritetsfrämjande teknik, i syfte att möjliggöra en modern datadelning. I dagsläget är kunskapen om teknikerna begränsad. Det gäller bland annat om de rättsliga och tekniska förutsättningarna för

[6] SOU 2025:96, s. 172 f.
[7] Se t.ex. SOU 2025:96, SOU 2025:12 *AI-kommissionens Färdplan för Sverige*, Integritetsskyddsmyndigheten (IMY), IMY-2024-2570, *Integritet och ny teknik 2020–2024*.
[8] Se t.ex. The Royal Society, *From privacy to partnership*, Organisationen för ekonomiskt samarbete och utveckling (OECD), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", *OECD Digital Economy Papers*, No. 351.

att använda teknikerna. Det finns också begränsad kunskap om vilka tekniker som är lämpliga i olika sammanhang samt vilka tillämpnings- och användningsområden som är möjliga. Därtill har offentliga aktörer skilda uppdrag, behov och organisatoriska förutsättningar, vilket påverkar deras möjligheter att tillämpa integritetsfrämjande teknik i praktiken.

För att möta den snabba teknikutvecklingen och det ökade behovet av datadrivna arbetssätt behövs åtgärder som stärker förmågan till datadelning. Att främja en ökad användning av integritetsfrämjande teknik i offentlig förvaltning är en sådan åtgärd.

9.3 Konsekvenser av att inga åtgärder vidtas för att öka användningen (nollalternativet)

Utredningens förslag syftar till att stärka förutsättningarna för datadelning i offentlig förvaltning genom integritetsfrämjande teknik. Det pågår parallellt flera insatser för att möjliggöra en ökad och mer ändamålsenlig datadelning inom Sverige och EU. Denna utveckling kommer att fortgå oberoende av våra förslag och kommer på längre sikt sannolikt bidra till en ökad datadelning.

Utredningens bedömning är att de potentiella nyttorna som följer av en ökad datadelning riskerar att begränsas om inga åtgärder vidtas för att öka användningen av integritetsfrämjande teknik. Nyttorealiseringen riskerar också att försenas och bli mer utdragen över tid. Vilka nyttor som realiseras kan variera för olika offentliga aktörer men innebär i huvudsak förbättrade möjligheter att effektivisera offentliga verksamheter och att förbättra de tjänster som erbjuds till enskilda och företag. Det finns särskilt en risk för att den nyttopotential som finns i de moderna integritetsfrämjande teknikerna inte kommer att realiseras i tillräcklig omfattning, eftersom användningen av just dessa tekniker är så pass begränsad inom förvaltningen. Utvecklingen mot en ökad datadelning och AI-användning kommer också alltmer aktualisera behovet av att skydda den personliga integriteten. Om det inte möts, kan allmänhetens förtroende för förvaltningen på sikt urholkas.

9.3.1 Konsekvenser på kortare sikt

Begränsad och fragmenterad användning av teknikerna

En möjlig konsekvens av att inga åtgärder vidtas för att öka användningen att integritetsfrämjande teknik är att användningen fortsätter att vara begränsad inom förvaltningen. Det gäller främst de moderna teknikerna, men även de etablerade avidentifieringsteknikerna. Det finns framför allt en risk för en fragmenterad och ojämn användning av teknikerna. Det innebär att större offentliga aktörer med resurser och kompetens upphandlar eller utvecklar egna lösningar för integritetsfrämjande teknik. Mindre offentliga aktörer har däremot inte samma möjligheter att använda teknikerna.

En liknande utveckling har tidigare kunnat iakttas inom digitaliseringen av den offentliga förvaltningen, där avsaknaden av sammanhållen och strategisk styrning har bidragit till en fragmenterad och ojämn utveckling. Digitaliseringsinsatserna har i stor utsträckning koncentrerats till vissa större offentliga aktörer. Detta har i sin tur försvårat utvecklingen mot en mer sammanhållen digital förvaltning samt hämmat samverkan och datautbyte inom förvaltningen.[9] En fragmenterad och ojämn användning av teknikerna i offentlig förvaltning kan även begränsa möjligheterna för Sverige att delta i olika datadelningssammanhang på europeisk nivå, exempelvis inom det europeiska hälsodataområdet (EHDS).

En möjlig konsekvens är att teknikerna fortsatt upplevs som alltför avancerade eller kostsamma att tillämpa, vilket begränsar användningen. Vår kartläggning av hur integritetsfrämjande teknik används i offentliga förvaltning visar att offentliga aktörer generellt är tveksamma till att utforska användningen av de moderna och mer avancerade teknikerna och efterfrågar att vissa aktörer agerar som föregångare. Även tidigare utredningar konstaterar att offentliga aktörer överlag är försiktiga när det gäller att tillämpa nya och komplexa digitala lösningar samt att göra digitala investeringar där nyttorna eller riskerna inte är tillräckligt tydliga.[10]

[9] Se t.ex. Myndigheten för digital förvaltning (Digg), dnr 2024-1332, *Ett samhälle i förändring – underlag till regeringens strategiska prioriteringar*, Organisationen för ekonomiskt samarbete och utveckling (OECD), 2019, *Digital Government Review of Sweden: Towards a Data-driven Public Sector*.
[10] Se t.ex. Statskontoret, OOS 51, *Myndigheterna och AI – En studie om möjligheter och risker med att använda AI i statsförvaltningen*, s. 32 f. och SOU 2025:96, avsnitt 4.3.

Utebliven eller mindre säker datadelning

En låg användning av de moderna teknikerna riskerar att begränsa datadelningen mellan offentliga aktörer. Det gäller särskilt inom de områden där det finns en stor mängd personuppgifter eller andra skyddsvärda uppgifter, till exempel inom hälso- och sjukvård och socialtjänst. Skälet till det är att de moderna teknikerna ger utökade möjligheter att säkerställa integritetsskydd och möjliggör datadelning som annars begränsas av sekretess.

Det finns också en risk för att den upplevda rättsliga osäkerheten gällande användningen av teknikerna består eller till och med förstärks i takt med att den tekniska och regulatoriska utvecklingen inom datadelning och AI fortsätter. Detta kan leda till att offentliga aktörer gör en alltför försiktig och strikt tillämpning av regelverken. En konsekvens av detta kan bli att aktörer avstår från att använda integritetsfrämjande teknik och därmed även från att dela vissa datamängder av försiktighetsskäl.[11]

Avsaknaden av stöd och vägledning kan också skapa en bristfällig implementering när teknikerna väl används, exempelvis kan integritetsskyddet bli för svagt. Det kan leda till en osäkrare datadelning.

Minskad möjlighet att påverka och anpassa den tekniska utvecklingen

En begränsad användning av integritetsfrämjande teknik kan minska utrymmet för Sverige att påverka både den tekniska och rättsliga utvecklingen inom området. Vi har tidigare konstaterat att behov och konkreta användarfall i allt högre grad påverkar den fortsatta tekniska utvecklingen av integritetsfrämjande teknik. En mer begränsad användning av teknikerna i förvaltningen försvårar möjligheterna att identifiera lämpliga tillämpnings- och användningsområden där nyttohemtagningen är stor. Det minskar utrymmet för att styra införandet av integritetsfrämjande teknik mot dessa områden, vilket i förlängningen ger en begränsad nyttorealisering. Det kan också skapa sämre förutsättningar för export av tjänster och produkter som utvecklas nationellt.

[11] Se SOU 2025:12, s. 9 f.

9.3.2 Konsekvenser på längre sikt

Uteblivna nyttor av en ökad och förbättrad datadelning

En begränsad användning av integritetsfrämjande teknik innebär att de potentiella nyttorna med en ökad användning av teknikerna riskerar att inte realiseras. Det gäller främst inom områden som omfattar stora mängder känsliga uppgifter så som hälso- och sjukvård, socialtjänst, brottsbekämpning samt skatte- och bidragskontroll. Utredningens samhällsekonomiska analys visar att en del av de potentiella nyttorna av ökad datadelning är direkt beroende av att integritetsfrämjande teknik används i större utsträckning än i dag. Enligt uppskattningar är ungefär 30–50 procent av all ekonomisk potential från datadelning i offentlig förvaltning beroende av att integritetsfrämjande teknik används för att möjliggöra en mer avancerad och rättssäker datadelning. Det motsvarar ekonomiska nyttor om cirka 10–40 miljarder kronor per år.[12]

Utredningens samhällsekonomiska analys har tagit fram olika scenarier för att beskriva nyttorealiseringen av integritetsfrämjande teknik. Scenarierna utgår från olika ambitionsnivåer vad gäller statliga åtgärder för att öka användningen av teknikerna. I ett scenario beskrivs nollalternativet, det vill säga där integritetsfrämjande teknik *inte* etableras som en operativ och strukturell lösning för delning av känsliga uppgifter.[13] Det innebär att den operativa användningen förblir begränsad. Detta scenario beskriver ett försiktigt angreppssätt, där staten främst fokuserar på övergripande vägledning och enstaka tekniska piloter. Vidare introduceras integritetsfrämjande teknik som koncept och prövas i begränsad skala. Genomförandet är dock selektivt och huvudsakligen koncentrerat till ett fåtal statliga myndigheter med hög digital mognad.

I detta scenario går det att realisera en tredjedel av den totala ekonomiska potentialen av datadelning, i huvudsak genom andra reformer så som ökad interoperabilitet, samordning och rättsliga förtydliganden.[14] Vid en sådan begränsad operativ användning av integritetsfrämjande teknik kan dock endast en mycket liten andel (mindre än 10 procent) av värdet av datadelning inom verksamheter

[12] Bilaga 2, *Samhällsekonomisk analys av potentialen för ökad användning av integritetsfrämjande teknik i offentlig förvaltning*, s. 12 f.
[13] Bilaga 2, *Samhällsekonomisk analys*, s. 65 f. I analysen kallas detta för ”Scenario A”.
[14] Bilaga 2, *Samhällsekonomisk analys*, s. 65 f.

med känsliga uppgifter realiseras.[15] Den potentiella nyttorealiseringen av datadelningen sker också relativt långsamt på grund av den begränsade användning av teknikerna. I scenariot nås en realiserad årlig nytta på cirka 2 miljarder kronor efter 10 år.[16] Det finns därmed en risk för att de förväntade nyttorna av ökad datadelning inom förvaltningen inte når sin fulla potential om inte användningen av integritetsfrämjande teknik ökar inom verksamheter som omfattar känsliga uppgifter.

Förtroendet för den offentliga förvaltningen urholkas

En datadriven och AI-baserad utveckling förutsätter tillgång till stora mängder data. En sådan utveckling kräver emellertid att allmänheten känner förtroende för hur den offentliga förvaltningen behandlar personuppgifter och andra skyddsvärda uppgifter. Integritetskyddsmyndigheten (IMY) har konstaterat att det blir allt svårare för individen att värdera känsligheten i att en viss information delas. Det blir därmed svårare att värdera riskerna för den digitala integriteten.[17] Detta gäller särskilt vid utveckling och användning av AI. Där kan bearbetning av omfattande datamängder medföra att information som var för sig inte uppfattas som integritetskänslig sammantaget blir integritetskränkande.[18] Utan tillgång till tillräckligt stor mängd korrekta och representativa data för träning kan AI-modellers resultat samtidigt bli missvisande och i vissa fall leda till diskriminering.[19]

Det finns undersökningar som visar att befolkningens förtroende för hur AI-tjänster hanterar personlig information är relativt lågt. I en undersökning från Insight Intelligence från 2025 har endast 15 procent av de svarande högt förtroende för att AI-tjänster hanterar personlig information på ett säkert sätt.[20]

Integritetsfrämjande teknik skapar förutsättningar för en ökad datadelning och AI-utveckling utan att kompromissa med skyddet

[15] Bilaga 2, *Samhällsekonomisk analys*, s. 66 f.
[16] Bilaga 2, *Samhällsekonomisk analys*, s. 66 f.
[17] IMY definierar digital integritet som rätten till skydd för personuppgifter och privatliv på internet och i andra digitala sammanhang, och i slutändan möjlighet till självbestämmande i det digitala samhället. Digital integritet är en del av den personliga integriteten, se Integritetsskyddsmyndigheten (IMY), rapport 2022:3, *Digital integritet 2022*, s. 9.
[18] IMY, *Digital integritet 2022*, s. 24.
[19] Statskontoret, *Myndigheterna och AI*, s. 33.
[20] Insight intelligence, 2025, *Svenska folket och AI 2025*, s. 26.

för den personliga integriteten. En möjlig konsekvens av att teknikerna endast används i begränsad utsträckning är därför att invånare upplever att offentliga aktörer inte hanterar deras data på ett tillräckligt transparent och säkert sätt. På längre sikt riskerar det att påverka förtroendet för den offentliga förvaltningen.[21] Organisationen för ekonomisk och social utveckling (OECD) har betonat att utvecklingen av en digital förvaltning behöver ske på ett transparent, öppet och säkert sätt för att upprätthålla förtroendet för förvaltningen.[22] Om integritetsskyddet vid datadelning inte säkerställs finns det därmed, enligt vår uppfattning, en risk för att allmänhetens förtroende för den offentliga förvaltningen och dess digitalisering försvagas.

9.4 Utredningens förslag för att öka användningen av integritetsfrämjande teknik vid datadelning

Utredningens övergripande bedömning är att det behövs en tydligare styrning av integritetsfrämjande teknik för att öka kunskapen och användningen av teknikerna i förvaltningen. Denna styrning kan dock utformas på olika sätt. Vi anser att det behövs en kombination av olika åtgärder för att öka användningen på ett effektivt och ändamålsenligt sätt. Förslagen är inriktade på att stärka förmågan att använda teknikerna. Det finns inget egenvärde i att använda teknikerna, utan teknikerna är ett medel för att uppnå nyttorna med modern datadelning. Användningen behöver därför styras av förvaltningens behov och de områden och verksamheter där det finns uppskattade nyttor av att använda teknikerna för datadelning.

I följande avsnitt redogör vi övergripande för våra huvudsakliga förslag och våra bedömningar om alternativa sätt att uppnå en ökad användning av teknikerna.

9.4.1 Förslag om stöd och vägledning

Ett grundläggande steg för att öka användningen av teknikerna i förvaltningen är att förbättra förvaltningens kunskap om teknikerna. Vi föreslår därför att det bör finnas en myndighet med ett

[21] Se även Digg, *Ett samhälle i förändring*, s. 52.
[22] OECD, *Digital Government Review of Sweden*, s. 37 f.

tydligt och långsiktigt ansvar för att stödja och vägleda offentliga aktörer i att tillämpa teknikerna. Det handlar bland annat om att öka kunskapen om de tekniska, organisatoriska och rättsliga förutsättningarna för tillämpningen av teknikerna. Det handlar också om att öka kunskapen om möjliga användningsområden och nyttor. Utredningen föreslår att Myndigheten för digital förvaltning (Digg) får detta uppdrag i samverkan med Skatteverket, IMY, Statistiska centralbyrån (SCB) och Nationellt cybersäkerhetscenter (NCSC) vid Försvarets radioanstalt (FRA) (se avsnitt 8.3).

9.4.2 Förslag om förvaltningsgemensamma tjänster

Utredningen anser att det behövs insatser för att sänka tröskeln för användningen av integritetsfrämjande teknik. Det handlar främst om moderna tekniker som är tekniskt mogna för användning och som har stor potential, men som i dag används i begränsad utsträckning. Vissa av dessa tekniker kan dessutom vara svåra att utveckla eller upphandla för enskilda aktörer. Vi anser därför att en myndighet bör tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik.

I ett första skede finns, enligt vår bedömning, ett särskilt behov av en förvaltningsgemensam tjänst för säker flerpartsberäkning. Det är en teknik som är tekniskt mogen för användning men som endast används i begränsad utsträckning inom förvaltningen och som är svår att utveckla själv. Samtidigt är det en teknik som har stor potential att hantera utmaningarna med delning av känsliga uppgifter. Tjänsten för säker flerpartsberäkning bör vara tillgänglig kostnadsfritt för hela den offentliga förvaltningen och finansieras genom anslag. Detta är viktigt för att främja en bred användning av tjänsten då det finns en risk att avgiftsfinansiering skulle hämma användningen. Anslagsfinansiering underlättar även för regeringen att styra ambitionsnivån för tjänsten, vilket får anses lämpligt i det här fallet då det är svårt att identifiera en tydlig målgrupp (se avsnitt 8.5.1). En förvaltningsgemensam tjänst för säker flerpartsberäkning främjar också en mer rättssäker användning och kostnadseffektiv lösning för förvaltningen, jämfört med om enskilda aktörer skulle utveckla egna lösningar för tekniken.

Vi föreslår att Skatteverket får i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik, i samverkan med Digg, IMY, SCB och NCSC vid FRA (se avsnitt 8.4).

9.4.3 Förslag om särskilda regeringsuppdrag

Utredningen föreslår att regeringen ger riktade och specifika uppdrag för att utforska användningen av integritetsfrämjande tekniker inom olika områden. Dessa uppdrag kan bidra till att tillgodose behoven av kunskap om den praktiska tillämpningen av teknikerna som finns i förvaltningen. Vi föreslår att Skatteverket, Försäkringskassan, E-hälsomyndigheten och Socialstyrelsen tilldelas olika uppdrag som utforskar användningen av teknikerna (se avsnitt 8.7).

9.4.4 Alternativa åtgärder som utredningen har övervägt

Författningsreglerade krav på att använda tekniker och hur de ska användas

Vi har övervägt att föreslå författningskrav om att integritetsfrämjande teknik ska användas i förvaltningen, antingen generellt eller i specifika situationer (se avsnitt 7.4.1). Det skulle bidra till ökad användning av teknikerna i förvaltningen. Utredningen bedömer dock att användningen av teknikerna bör motiveras utifrån behovet i den enskilda situationen. Det finns en risk att författningsreglerade krav på användning gör att teknikerna inte används på ett ändamålsenligt sätt, exempelvis att teknikerna används främst på grund av fastställda krav snarare än på grund av behovet i det enskilda fallet. Krav riskerar också att bli hinder för ökad datadelning eftersom de kan bidra till en ökad administrativ börda, särskilt för mindre aktörer med begränsade resurser.

Vi har även övervägt att införa särskilda författningskrav vid användningen av teknikerna, till exempel krav på samråd med specifika myndigheter (se avsnitt 7.4.2). En fördel med sådana krav skulle vara att de bidrar till tydlighet och förutsägbarhet vid användningen. Vi bedömer dock att det i dagsläget kan bidra till administrativa och tekniska bördor som riskerar att begränsa användningen av tekni-

kerna snarare än att öka den. Det finns även en risk för att sådana krav inte blir proportionerliga i den enskilda datadelningssituationen.

Sammantaget bedömer vi att olika typer av författningsreglerade krav skulle riskera att teknikerna används på ett sätt som inte är behovsanpassat. Det finns även en risk att sådana krav snabbt blir föråldrade, givet den snabba tekniska utvecklingen. Kraven skulle behöva ändras, anpassas och kompletteras när det tillkommer nya användningsområden och nya integritetsfrämjande tekniker. Utredningen bedömer därför att stödjande och vägledande åtgärder är ett mer ändamålsenligt sätt att bidra till tydlighet och förutsägbarhet vid användningen av teknikerna. Det är också ett mer flexibelt styrmedel för att anpassa stödet efter både behoven och den tekniska utvecklingen.

Rådgivning i stället för stöd och vägledning

Utredningen har övervägt olika typer av stödjande åtgärder för att öka kunskapen om och användningen av teknikerna i offentlig förvaltning. Vi har strävat efter att hitta en så effektiv och ändamålsenlig utformning av stödet som möjligt.

Att tillhandahålla rådgivning till förvaltningen är en möjlig åtgärd för att öka användningen av teknikerna. Rådgivning kan exempelvis ske via frågebrevlådor eller telefon. Fördelen med rådgivning är att den är situationsanpassad och svarar mot de specifika behov som uppstår. Rådgivning riskerar samtidigt att bli reaktiv snarare än proaktiv, det vill säga att den främst fokuserar på att möta specifika och uppkomna behov bland aktörerna. Rådgivning ges därför främst till aktörer som efterfrågar den, vilket inte alltid sammanfaller med de datadelningssituationer där nyttopotentialen är som störst.

Vi bedömer att rådgivning riskerar att bli resurskrävande givet bredden på potentiella användningsområden i förvaltningen och den låga kunskapsnivån om teknikerna. Vi anser dessutom att den privata marknaden till viss del täcker in den typen av verksamhetsnära rådgivning som behövs vid tillämpningen av teknikerna (se avsnitt 8.3.1).

Utredningen anser att olika typer av vägledning är ett mer ändamålsenligt sätt att främja användningen av teknikerna än rådgivning. Då kan fokus läggas på användningsområden och tekniker där det

finns störst potentiell nytta. Vägledning gör det möjligt för aktörerna att bygga upp egen kunskap och förmåga så att de själva kan anpassa användningen av teknikerna till respektive användningsområde. Vägledning är också mer tillgängligt för hela förvaltningen än vad rådgivning är, eftersom rådgivning är mer utformat efter specifika situationer. Vi ser samtidigt behov av att komplettera vägledning med ett mer verksamhetsnära och tillämpbart stöd, till exempel i form av metodstöd och anpassade utbildningar (se vidare i avsnitt 8.3.3).

Vår bedömning är att kunskapsspridning om konkreta användningsfall och de nyttor som kan uppnås genom användning av teknikerna utgör en central och möjliggörande faktor för en ökad tillämpning. Det bör därför vara en del av ett stödjande och vägledande uppdrag.

Att inte tillhandahålla förvaltningsgemensamma tjänster

Vi har övervägt en lösning där staten endast tillhandahåller stöd och vägledning, men inte förvaltningsgemensamma tjänster för integritetsfrämjande teknik. Det finns enligt vår bedömning flera nackdelar och risker med en sådan lösning. Flera av de moderna teknikerna är avancerade tekniker som är relativt okända i förvaltningen. Det gäller exempelvis säker flerpartsberäkning som vi föreslår som en första förvaltningsgemensam tjänst. Utredningen har tidigare konstaterat att många statliga myndigheter, regioner och kommuner i dag saknar teknisk och juridisk kunskap om hur integritetsfrämjande teknik kan användas i praktiken. Det gäller särskilt de moderna teknikerna. Utveckling och drift av avancerade integritetsfrämjande tjänster innebär initiala investeringar i teknik, säkerhetsgranskning och kompetensuppbyggnad. För vissa tekniker krävs också en specialistkompetens som i dag är begränsad. Det innebär särskilt en utmaning för mindre offentliga aktörer, till exempel små och medelstora statliga myndigheter och kommuner. Även upphandling av avancerade tekniska lösningar kräver resurser och en viss kompetens. Det innebär att främst större offentliga aktörer skulle ha möjlighet att utveckla eller upphandla en lösning för till exempel säker flerpartsberäkning. Med tanke på den låga kunskapsnivån i förvaltningen finns det även en risk för att det skulle dröja innan tekniker utvecklas eller upphandlas. Vi ser även att det finns

en risk för bristfällig implementering, vilket kan leda till att tillämpningen av tekniken inte ger avsedd effekt.

Att tillhandahålla förvaltningsgemensamma tjänster innebär att flera av dessa risker hanteras. Det innebär en lägre tröskel för användning av tekniken för offentliga aktörer, vilket är centralt för att möjliggöra en förbättrad datadelning. Vår bedömning är därför att stöd och vägledning bör kompletteras med förvaltningsgemensamma tjänster. Det innebär stordriftsfördelar och en möjlighet för förvaltningen att samla relevant spetskompetens.

Generella uppdrag och återrapporteringskrav

Ett annat sätt för regeringen att styra användningen av integritetsfrämjande teknik är att genom mer generella uppdrag eller återrapporteringskrav tydliggöra att statliga myndigheter ska utforska eller använda teknikerna tillsammans med andra myndigheter vid datadelning.

Vår bedömning är att det i dagsläget främst finns behov av mer riktade och specificerade regeringsuppdrag till vissa myndigheter. Skälet till det är bland annat den låga kunskapen om teknikerna i förvaltningen. Det behövs enligt vår bedömning en höjning av kunskapsnivån om teknikerna innan mer generella uppdrag eller återrapporteringskrav kan ges till ett större antal myndigheter. Annars riskerar uppdragen att inte få det genomslag som önskas. Integritetsfrämjande teknik är som tidigare konstaterats inte en enhetlig grupp utan teknikerna har olika syften och användningsområden. Ett generellt uppdrag eller återrapporteringskrav till ett större antal myndigheter är mer lämpligt när kunskapsnivån om tillämpningen av teknikerna har höjts i förvaltningen. Det skulle exempelvis kunna vara aktuellt om den förvaltningsgemensamma tjänsten för säker flerpartsberäkning inte används i tillräcklig utsträckning.

Riktade uppdrag till ett urval av myndigheter ger dessutom regeringen möjlighet att styra arbetet mot de områden där det finns störst nytta och potential för teknikerna. Vår kartläggning visar att bara ett fåtal offentliga aktörer har kapacitet eller ambition att ligga i framkant när det gäller att införa och använda integritetsfrämjande teknik. Några aktörer behöver därför gå först och visa hur integ-

ritetsfrämjande teknik kan tillämpas i praktiken samt vilka nyttor som kan uppnås genom användningen.

9.5 Konsekvenser i form av samhällsekonomiska nyttor

Datadelning är aktuellt för verksamheter inom stora delar av den offentliga förvaltningen. Det innebär att våra förslag för att öka användningen av integritetsfrämjande teknik potentiellt påverkar hela den offentliga förvaltningen, även om teknikerna är mer relevanta för de verksamheter som behandlar stora mängder känsliga uppgifter. I förlängningen bedöms våra förslag både direkt och indirekt ha betydelse för stora delar av samhället. De som berörs direkt är offentliga aktörer. Förslagen berör dock även enskilda individer vars personuppgifter behandlas och delas samt företag.

I följande avsnitt redovisas de samhällsekonomiska nyttorna av datadelning med integritetsfrämjande teknik ur ett makroperspektiv. Därefter redogör vi för de konkreta konsekvenser som vi har identifierat för enskilda och företag samt för offentliga aktörer (avsnitt 9.6–9.10). Dessa konsekvenser omfattar såväl nyttor som risker och kostnader.

9.5.1 Nyttopotentialen vid datadelning med teknikerna

Den samhällsekonomiska analys som utredningen har låtit genomföra visar att det, även vid försiktiga antaganden, finns en betydande potential i form av nyttor vid användning av teknikerna. En förbättrad datadelning med hjälp av integritetsfrämjande teknik kan bland annat leda till ökad effektivitet, kvalitet och säkerhet i den offentliga förvaltningens verksamheter. Det kan också leda till förbättrad service till enskilda och företag. Teknikerna kan även underlätta olika typer av förebyggande arbete och hantering av komplexa samhällsutmaningar som brottsförebyggande arbete och folkhälsa. Vidare kan teknikerna bidra till innovativa nya lösningar.

Den samhällsekonomiska analysen fokuserar i huvudsak på ekonomiska nyttor i form av effektiviseringar och kostnadsbesparingar för verksamheter inom offentlig förvaltning. Det är där som de direkta nyttorna av teknikerna uppstår vilket gör kvantifierbara beräkningar

mer tillförlitliga. Det bör dock understrykas att åtgärder som leder till effektiviseringar och ökad kvalitet inom förvaltningen även genererar betydande nyttor för enskilda och företag. Dessa kan dock vara svårare att kvantifiera.

Uppskattningar av de samhällsekonomiska nyttorna

Utredningens samhällsekonomiska makroanalys uppskattar den ekonomiska potentialen av ökad och förbättrad datadelning inom förvaltningen till cirka 30–80 miljarder kronor per år. Av detta bedöms ungefär 10–40 miljarder kronor årligen vara direkt beroende av att integritetsfrämjande teknik används, i den meningen att dessa tekniker möjliggör datadelning som annars inte hade varit möjlig eller genomförbar på ett rättssäkert och integritetfrämjande sätt.[23]

Utredningens mikroanalyser pekar samtidigt på att potentialen inom vissa områden kan vara ännu större. I dessa analyser uppskattas den ekonomiska potentialen av datadelning med integritetsfrämjande teknik till 19–42 miljarder kronor per år för de tillämpningsområden som bedöms ha den största nyttopotentialen för offentlig förvaltning.[24] Skillnaderna mellan makro- och mikroanalyserna avspeglar olika antaganden om användningsgrad och sektoriell spridning. Mikroanalyserna fokuserar också särskilt på utvalda tillämpningsområden och användningsfall där nyttan av datadelning med integritetsfrämjande teknik bedöms vara stor. Dessa områden är hälso- och sjukvård, socialtjänst, omsorg och bistånd samt skatte- och bidragskontroller. Inom dessa områden finns det flera studier och rapporter som innehåller försök att specificera och kvantifiera nyttorna. Det finns emellertid även andra områden där de potentiella samhällsnyttorna kan vara betydande (se avsnitt 6.2.3).

De lägre beloppen i de angivna spannen bygger på antagandet att integritetsfrämjande teknik används i vissa prioriterade områden men att det saknas en bred, samordnad och systematisk tillämpning i hela den offentliga förvaltningen. De högre beloppen i spannen förutsätter att teknikerna används generellt och långsiktigt i stora delar av förvaltningen. De förutsätter också att relevanta verksam-

[23] Bilaga 2, *Samhällsekonomisk analys*, s. 12.
[24] Bilaga 2, *Samhällsekonomisk analys*, s. 46.

hetsprocesser, styrmodeller och tekniska infrastrukturer anpassas för att möjliggöra lösningar i större skala.

Nyttopotentialen av utredningens förslag

Utredningens förslag bör ses som inledande och nödvändiga steg för att successivt uppnå de omfattande samhällsekonomiska nyttorna av datadelning med stöd av integritetsfrämjande teknik. Att realisera den fulla potentialen förutsätter dock ett systematiskt och långsiktigt arbete. Regeringen och statliga myndigheter behöver tydligare styra mot en förbättrad datadelning med teknikerna över tid, både genom stöd och vägledning samt genom att tillhandahålla tekniska lösningar. I den samhällsekonomiska analysen presenteras olika scenarier som motsvarar olika ambitionsnivåer vad gäller åtgärder för att öka användningen av teknikerna. Ett av dessa scenarier motsvarar satsningar som överensstämmer med utredningens förslag.[25] I scenariot införs integritetsfrämjande tekniker främst i vissa prioriterade områden där behoven och nyttan av teknikerna uppskattas att vara större. I ett sådant scenario ökar nyttorealiseringen gradvis vilket innebär att det efter 5 år finns en uppskattad årlig nyttorealisering om cirka 3 miljarder kronor och efter 7 år cirka 6 miljarder kronor. Efter 10 år uppskattas den årliga nyttorealiseringen till cirka 11 miljarder kronor.[26]

Utredningens bedömning är att satsningen i detta scenario realiserar en betydande del av den identifierade nyttopotentialen och att satsningen är proportionerlig. I vilken utsträckning förvaltningen på sikt kan närma sig den fulla nyttopotentialen beror dock i hög grad på regeringens och offentliga aktörers ambitionsnivå samt på vilka andra åtgärder som vidtas framöver.

Potentialen är störst inom områden som har sämre förutsättningar för datadelning

Den samhällsekonomiska analysen visar att nyttopotentialen är särskilt stor inom områden som i dag har begränsade förutsättningar för datadelning, exempelvis där det saknas tydliga uppgiftsskyldig-

[25] Bilaga 2, *Samhällsekonomisk analys*, s. 67 f. I analysen kallas detta för ”Scenario B”.
[26] Bilaga 2, *Samhällsekonomisk analys*, s. 68 f.

heter eller tillämpliga sekretessbrytande bestämmelser. Ett sådant område är hälso- och sjukvården, där den uppskattade nyttopotentialen av integritetsfrämjande teknik uppgår till totalt cirka 12–26 miljarder kronor per år.[27] I dessa verksamheter kan teknikerna i särskilt hög grad möjliggöra sekundäranvändning av hälsodata för analys, uppföljning och beslutsstöd, samtidigt som en hög skyddsnivå för den personliga integriteten upprätthålls (se vidare i avsnitt 6.2.2).

9.6 Konsekvenser för enskilda

Vi bedömer att våra förslag i huvudsak leder till positiva konsekvenser för enskilda. En ökad användning av integritetsfrämjande teknik vid datadelning kan bidra till att förenkla administrativa processer och förkorta handläggningstider inom förvaltningen. Därigenom kan enskilda i större utsträckning få snabbare tillgång till beslut, ersättningar och andra offentliga tjänster. Teknikerna kan vidare möjliggöra en mer sammanhållen och ändamålsenlig användning av digitala lösningar. Det leder till att offentliga tjänster kan göras mer tillgängliga, behovsanpassade och effektiva ur individens perspektiv. Det kan också bidra till att stärka förtroendet för den offentliga förvaltningen.[28]

En ökad användning av integritetsfrämjande teknik bidrar till att skyddet för enskildas uppgifter stärks vid datadelning. För den enskilde kan detta innebära en ökad upplevd trygghet i hur personuppgifter samlas in, delas och används. Det kan stärka medborgarnas tillit till att deras personliga information hanteras ansvarsfullt och i enlighet med gällande regelverk.

Vidare kan användningen av teknikerna vid datadelning bidra till att höja kvaliteten i offentliga verksamheter, vilket också får direkta effekter för enskilda. Exempelvis kan förbättrade beslutsstöd och mer underbyggda bedömningar leda till mer träffsäkra beslut i ärenden som rör enskildas rättigheter och behov. Inom hälso- och sjukvården kan detta innebära både förbättrad hälsa och ökad patientsäkerhet. Ett illustrativt exempel är användningen av AI-baserade kliniska beslutsstöd. När integritetsfrämjande teknik används i sådana lösningar kan de bidra till en mer ändamålsenlig användning av vårdens

[27] Bilaga 2, *Samhällsekonomisk analys*, s. 37.
[28] Se OECD, *Digital Government Review of Sweden,* s. 37 f.

resurser och till minskade kostnader. Samtidigt kan patienter få en säkrare och snabbare diagnos. Detta möjliggör i sin tur tidigare och mer träffsäkra vårdinsatser, vilket är av stor betydelse för den enskildes hälsa och livskvalitet.[29]

9.6.1 Den personliga integriteten

Det rättsliga skyddet för den enskildes personliga integritet kommer till uttryck i flera regelverk. Skyddet regleras bland annat i regeringsformen (RF) och dataskyddsförordningen. Sverige har därutöver anslutit sig till ett flertal internationella konventioner på området.

Förslagen bidrar till att färre personuppgifter behandlas vid datadelningstillfället

Utredningen lämnar inga författningsförslag avseende användningen av integritetsfrämjande teknik vid datadelning. Förslagen innebär inte heller att offentliga aktörer åläggs nya eller utökade skyldigheter att behandla personuppgifter. Däremot lämnar vi ett antal förslag som syftar till att stärka den offentliga förvaltningens förmåga att dela data genom ökad användning av integritetsfrämjande teknik. En ökad datadelning inom offentlig förvaltning kan medföra ökade risker för den personliga integriteten.

Mot bakgrund av den breda definitionen av personuppgiftsbehandling kommer de åtgärder som vidtas vid användningen av teknikerna att utgöra personuppgiftsbehandlingar. Inom ramen för utredningens förslag om en förvaltningsgemensam tjänst kommer personuppgifter att behandlas i flera led, bland annat vid identifiering av relevanta datamängder och vid förberedelser inför användningen av tjänsten. Även när respektive aktör tar del av resultatet kan en behandling av personuppgifter komma att äga rum.

En ökad användning av integritetsfrämjande teknik kan därför generellt förväntas leda till att personuppgifter i större utsträckning än i dag behandlas hos de aktuella aktörerna *inför* en delning av data. Det övergripande syftet med att bearbeta data med integritetsfrämjande teknik innan den delas är dock att stärka integritetsskyddet vid datadelningen. Även om en ökad användning av integritets-

[29] Bilaga 2, *Samhällsekonomisk analys*, s. 26 f.

främjande teknik kan innebära att personuppgifter i större utsträckning behandlas hos berörda aktörer inför en datadelning, kan alltså teknikerna bidra till att färre personuppgifter behandlas vid själva delningstillfället.

I vilken utsträckning den ökade användningen av integritetsfrämjande teknik sammantaget leder till en mer omfattande personuppgiftsbehandling är svårt att bedöma. Eftersom teknikerna kan möjliggöra datadelning i situationer där sådan delning i dag inte är möjlig, är dock utredningens bedömning att förslagen kan leda till fler datadelningstillfällen. Dessa datadelningstillfällen kommer att ske med ett stärkt skydd för den personliga integriteten.

Förslagen leder inte till ökade integritetsrisker utan kan förväntas stärka skyddet för enskildas integritet

Den personuppgiftsbehandling som följer av våra förslag bidrar till att skyddet för uppgifterna kan upprätthållas även vid en mer omfattande datadelning. Förslagen innebär inte heller att andra personuppgifter än de som redan i dag behandlas ska få behandlas eller delas. Förslagen innebär inte heller att personuppgifterna kommer att få behandlas för andra ändamål än de som redan gäller för respektive aktör inom offentlig förvaltning. Integritetsfrämjande teknik minskar dessutom behovet av att dela eller lagra stora mängder data, vilket reducerar exponeringen av känsliga uppgifter. Säkerheten kan också förbättras genom att data i större utsträckning kan bearbetas lokalt med vissa tekniker. Det minskar behovet av dataöverföring och därmed risken för obehörig åtkomst.

Det kan dock noteras att integritetsfrämjande teknik kan uppfattas som en enkel lösning för att stärka integritetsskyddet vid datadelning. Det finns därför en risk att teknikerna används på ett felaktigt sätt, vilket kan leda till en ökad datadelning med otillräckligt skydd. Utredningens förslag om stöd och vägledning samt förvaltningsgemensamma tjänster innebär dock att denna risk minskas och bidrar till att teknikerna används på ett korrekt sätt inom förvaltningen.

Vår samlade bedömning är att våra förslag inte medför en förhöjd risk för intrång i den personliga integriteten. Tvärtom förväntas förslagen kunna bidra till ett stärkt skydd för den personliga integriteten vid datadelning. Vi bedömer inte heller att personupp-

gifter kommer att få en större spridning än i dag. Genom en ökad användning av integritetsfrämjande teknik förbättras i stället förutsättningarna för uppgiftsminimering även vid en ökad datadelning.

Det innebär att den ökade personuppgiftsbehandling som offentliga aktörer kan förväntas utföra inför en delning är förenlig med kraven på skydd mot oacceptabla intrång i den enskildes personliga integritet. Den är också nödvändig och tillåten enligt dataskyddsregelverket. Den samlade effekten av våra förslag bedöms därför vara positiva för enskilda genom att skyddet för den personliga integriteten stärks.

9.6.2 Barn och andra särskilt skyddsvärda grupper

Utredningens förslag kan få särskilt positiva effekter för barn och andra skyddsvärda grupper, till exempel personer med funktionsnedsättning, äldre med nedsatt kognitiv förmåga eller individer i beroendeställning. Dessa grupper kan ha större svårigheter att förutse riskerna med att lämna ut uppgifter, förstå vilket skydd de har för sina personuppgifter samt påverka hur uppgifterna behandlas. Integritetsfrämjande teknik kan i detta avseende fungera som ett förstärkt skydd genom att minska behovet av att lämna ut personuppgifter i identifierbar form. De kan också begränsa åtkomsten till känsliga uppgifter samt möjliggöra datadriven verksamhetsutveckling utan att den enskildes uppgifter exponeras i onödan.

För barn innebär detta att datadelning i större utsträckning kan ske i former som är förenliga med den grundläggande principen om barnets bästa i barnkonventionen.[30] På motsvarande sätt kan våra förslag bidra till ett ökat skydd för andra särskilt skyddsvärda grupper. För barn och andra personer som har svårare att utöva kontroll över sina uppgifter kan en ökad användning av integritetfrämjande teknik minska risken för otillbörlig spridning eller obehörig åtkomst av uppgifter. Förslagen kan även bidra till att motverka maktobalans mellan den enskilde och myndigheter eller andra aktörer som behandlar uppgifter, genom att utformningen av datadelningen i högre grad sker med ytterligare skyddsåtgärder.

Våra förslag bedöms sammantaget bidra till att barn och andra särskilt skyddsvärda grupper ges ett mer robust och likvärdigt skydd,

[30] Artikel 3 i Förenta nationernas konvention den 20 november 1989 om barnets rättigheter.

oberoende av deras individuella förutsättningar att själva tillvarata sina rättigheter. Det innebär att våra förslag inte enbart har generella positiva effekter för den personliga integriteten, utan även kan bidra till att stärka skyddet specifikt för grupper som annars löper en förhöjd risk för integritetsintrång.

9.6.3 Jämställdhet och likabehandling

En ökad användning av integritetsfrämjande teknik kan bidra till ökad jämställdhet och minskad risk för diskriminering, särskilt vid användning av AI-baserade system i offentlig verksamhet. Detta eftersom integritetsfrämjande teknik kan möjliggöra tillgång till större och mer representativa datamängder för analys och modellträning, utan att personuppgifter exponeras. Det kan förbättra kvaliteten i beslutsunderlag och minska risken för snedvridna eller diskriminerande utfall till följd av bristfälliga eller skeva data. Vi bedömer vidare att en ökad tillgång till data kommer att underlätta uppföljning och analys av eventuella diskriminerande mönster i offentlig förvaltning.

Utredningen konstaterar samtidigt att integritetsfrämjande teknik inte i sig eliminerar risker för diskriminering. För att de positiva effekterna ska realiseras krävs att tekniken används inom ramen för tydlig styrning, transparens, konsekvensbedömning och mänsklig kontroll. Detta gäller särskilt vid automatiserat beslutsfattande. Sammantaget bedöms dock våra förslag kunna bidra till minskad risk för diskriminering i offentlig förvaltning.

9.7 Konsekvenser för företag

Utredningen bedömer att förslagen medför huvudsakligen positiva konsekvenser för företag i Sverige. Vi bedömer att en effektivisering av offentlig förvaltning även kan medföra flera potentiella nyttor för företag. Integritetsfrämjande teknik kan exempelvis effektivisera handläggningen av beslut som avser företag, skapa mer sammanhållna kontakter utifrån företagens behov och minska uppgiftslämningen för företag. Det kommer i förlängningen minska den administrativa bördan för företag, vilket stärker förutsättningarna för ökad tillväxt och konkurrens.

Våra förslag innebär en satsning på integritetsfrämjande teknik i offentlig förvaltning och bygger på att den privata marknadens kompetens bör tillvaratas. De företag som i första hand berörs av utredningens förslag är företag verksamma inom området för integritetsfrämjande teknik (privacy tech). Detta omfattar såväl större som mindre företag. Inom ramen för denna satsning har företag en viktig roll att bidra med kunskap och erfarenhet. Satsningen bedöms kunna bidra till att svenska företags position inom området stärks. Det kan i förlängningen öka deras möjligheter att påverka den internationella utvecklingen av integritetsfrämjande teknik samt bidra till stärkt konkurrensförmåga även utanför Sverige.

Utredningens förslag om stöd och vägledning om integritetsfrämjande teknik kan bidra till ökad legitimitet för och ökad medvetenhet om sådana tekniska lösningar. Detta bedöms kunna leda till en ökad efterfrågan såväl inom offentlig sektor som inom privat sektor. Det kan i sin tur kan skapa nya affärsmöjligheter för företag som tillhandahåller produkter och tjänster relaterade till teknikerna.

När det gäller förvaltningsgemensamma tjänster konstaterar utredningen att det finns en hög kompetens hos privata aktörer i Sverige och Europa när det gäller integritetsfrämjande teknik. Antalet aktörer är dock fortfarande begränsat och för vissa tekniker saknas i dag färdigutvecklade tjänster som kan upphandlas (se avsnitt 4.3.2). Detta skiljer sig exempelvis från AI-området där den privata marknaden är mer etablerad. Utredningens förslag om förvaltningsgemensamma tjänster för integritetsfrämjande teknik kan bidra till teknikutvecklingen. Detta gäller särskilt när den sker med stöd av den kompetens och kunskap som finns inom den privata sektorn. Det är därför angeläget att förvaltningsgemensamma tjänster i så stor utsträckning som möjligt utvecklas med stöd av privata aktörer.

Enligt utredningens bedömning bör förvaltningsgemensamma tjänster för offentlig förvaltning inledningsvis fokusera på säker flerpartsberäkning. För just denna teknik kan efterfrågan från offentliga aktörer på produkter och kompetens från privata aktörer minska, i den mån offentliga aktörer i stället väljer att använda den förvaltningsgemensamma tjänsten. Samtidigt är säker flerpartsberäkning en komplex och kostsam teknik att utveckla, vilket innebär att det inte framstår som realistiskt att ett större antal offentliga aktörer på egen hand upphandlar eller utvecklar sådana tjänster.

9.8 Konsekvenser som är gemensamma för offentlig förvaltning

9.8.1 Offentliga aktörer som använder teknikerna

Våra förslag innebär inte någon skyldighet för statliga myndigheter, kommuner eller regioner att använda integritetsfrämjande teknik vid datadelning. För merparten av offentliga aktörer medför dock användningen av sådan teknik en initial kostnad för att kunna generera och ta del av de nyttor som beskrivits i avsnitt 9.5. Dessa kostnader utgörs i huvudsak av användnings- och anpassningskostnader snarare än rena utvecklingskostnader. Det rör sig exempelvis om kostnader för juridiska analyser, tekniska anpassningar samt åtgärder för att säkerställa tillgång till nödvändiga resurser och relevant kompetens. Kostnadsnivån påverkas av verksamhetens storlek och komplexitet.[31]

Vår bedömning är att våra föreslag bidrar till att de initiala kostnaderna för att använda integritetsfrämjande teknik blir avsevärt lägre än vad som annars hade varit fallet. Tillgång till vägledning och stöd bedöms exempelvis förenkla de rättsliga bedömningarna samt underlätta användningen av sådan teknik generellt. Att löpande sprida kunskap och erfarenheter mellan de offentliga aktörer som använder teknikerna, till exempel genom utbildningar och nätverk, kan också bidra till att förenkla och minska kostnader för användningen över tid. Den förvaltningsgemensamma tjänsten för säker flerpartsberäkning innebär vidare att kostnader i första hand uppstår i form av tekniska anpassningar hos berörda aktörer, i stället för mer omfattande anskaffnings- och utvecklingskostnader.

[31] Bilaga 2, *Samhällsekonomisk analys*, s. 51 f.

Tabell 9.1 Kostnader för att använda teknikerna efter genomförande av förslagen

Aktör	Storlek	Initial kostnad	Årlig kostnad
Kommuner	Liten	0,8–1,5 mkr	0,3–0,6 mkr
	Mellan	1,5–3 mkr	0,6–1,2 mkr
	Stor	3–5 mkr	1,2–2 mkr
Regioner	Liten	2–4 mkr	1–1,5 mkr
	Mellan	4–7 mkr	1,5–2,5 mkr
	Stor	7–12 mkr	2,5–4 mkr
Statliga myndigheter	Liten	1–2 mkr	0,5–0,9 mkr
	Mellan	2–4 mkr	0,9–1,5 mkr
	Stor	4–7 mkr	1,5–3,0 mkr

Källa: Bilaga 2, *Samhällsekonomisk analys*, s. 58 f.

9.8.2 Digitaliseringen av offentlig förvaltning

Tillgången till data är avgörande för digitalisering eftersom den möjliggör analys, automatisering samt utveckling av datadrivna tjänster och beslut. Utan relevanta data begränsas offentliga aktörers förmåga att skapa innovation, effektivisera processer och dra nytta av AI. Våra förslag om stöd och vägledning bidrar till ökad rättslig och teknisk förutsebarhet vid användning av integritetsfrämjande teknik i offentlig förvaltning. Genom att klargöra hur sådan teknik kan tillämpas minskar osäkerheten avseende tillåtna användningsområden, ansvarsfördelning och riskhantering. Detta skapar bättre förutsättningar för modern datadelning samt för utveckling och användning av datadrivna arbetssätt hos offentliga aktörer.

Integritetsfrämjande teknik kan vidare, genom att bidra till en ökad datadelning och samverkan mellan offentliga aktörer, möjliggöra en mer sammanhållen digitalisering av den offentliga förvaltningen. Det möjliggör bland annat en digital förvaltning som är organiserad efter livs- eller företagshändelser i stället för organisationsindelningar och förvaltningsnivåer. Enligt internationella jämförelser har digitaliseringen av den offentliga förvaltningen i Sverige inte varit tillräckligt sammanhållen och användarorienterad.[32]

Sammantaget anser vi att våra förslag har en positiv effekt för digitaliseringen eftersom vägledning och förvaltningsgemensamma

[32] Digg, *Ett samhälle i förändring*, s. 68.

tjänster för integritetsfrämjande teknik utgör viktiga verktyg för att möjliggöra ökad och mer ändamålsenlig tillgång till data. Detta är en förutsättning för en rättssäker och effektiv digitalisering av offentlig förvaltning som allmänheten har förtroende för.

9.8.3 Effektiviteten i offentlig förvaltning

Våra förslag kan förväntas ha en positiv påverkan på effektiviteten i offentlig förvaltning eftersom de kan leda till en förbättrad tillgång till data. Förvaltningsgemensamma tjänster kan minska behovet av att enskilda offentliga aktörer upphandlar eller utvecklar egna tekniska lösningar och gör separata tolkningar av gällande regelverk. Detta kan leda till minskad resursåtgång, kortare utvecklings- och införandetider samt lägre kostnader för såväl utveckling som förvaltning av tekniska lösningar. En mer enhetlig utformning av tekniska och organisatoriska lösningar kan vidare underlätta samverkan mellan statliga myndigheter, regioner och kommuner. Det förbättrar förutsättningarna för ett effektivt informationsutbyte.

På längre sikt bedöms användningen av integritetsfrämjande teknik kunna bidra till ökad grad av automatisering och förbättrad kvalitet i beslutsprocesser, genom att fler relevanta datakällor kan utnyttjas på ett säkert och kontrollerat sätt. Detta kan ge bättre beslutsunderlag, minska behovet av manuell hantering och frigöra resurser för mer värdeskapande verksamhet.

En stor del av effektiviseringspotentialen bedöms finnas inom hälso- och sjukvård, socialtjänst och omsorg. I vår samhällsekonomiska analys uppskattas det exempelvis att integritetsfrämjande teknik kan bidra till att underlätta prioriteringar och förbättra resursplanering. Det kan bland annat ske genom att vårdpersonal får mer sammanhållen tillgång till patientinformation över organisationsgränser.[33] Teknikerna kan även bidra till att förbättra samordningen av olika typer av stöd och insatser till enskilda, såväl inom en kommuns olika förvaltningar som mellan kommuner, myndigheter och regioner. Det gäller till exempel inom socialtjänstens område där det kan bidra till minskade utrednings- och handläggningstider.[34]

[33] Bilaga 2, *Samhällsekonomisk analys*, s. 23 f.
[34] Bilaga 2, *Samhällsekonomisk analys*, s. 37 f.

Sammantaget bedömer utredningen att de föreslagna åtgärderna kommer att stärka effektiviteten i offentlig förvaltning.

9.8.4 Informationssäkerheten i offentlig förvaltning

Våra förslag bidrar till att stärka informationssäkerheten hos offentliga aktörer genom att exponeringen av känsliga data vid delning och analys minskar. Genom en ökad användning av integritetsfrämjande teknik kan risken för obehörig åtkomst och informationsläckage minska vid datadelning inom förvaltningen. Det innebär att teknikerna kan bidra både till att minska risken för incidenter och till att begränsa konsekvenserna av dem.

Samtidigt medför användning av integritetsfrämjande teknik en ökad teknisk komplexitet vilket ställer högre krav på styrning, kompetens och förvaltning. Bristande införande eller otydliga ansvarsförhållanden kan annars ge upphov till nya sårbarheter. Sammantaget bedöms dock våra förslag bidra till en förstärkt och mer robust informationssäkerhet vid datadelning.

9.8.5 Förpliktelser som följer av EU-rätten

Det finns flera förordningar på EU-nivå som styr mot användningen av integritetsfrämjande teknik, så som dataförordningen och dataförvaltningsförordningen (se avsnitt 5.2.1). Integritetsfrämjande teknik har också ett nära samband med skyddet av personuppgifter vilket i huvudsak regleras genom dataskyddsförordningen. Integritetsfrämjande teknik kan utgöra sådana tekniska och organisatoriska åtgärder (skyddsåtgärder) som säkerställer en lämplig säkerhetsnivå för personuppgifter i samband med datadelning. Teknikerna kan därför användas i syfte att säkerställa att kraven i förordningen uppfylls (se avsnitt 7.3). Eftersom förslagen främjar användningen av sådana skyddsåtgärder bedömer vi att de föreslagna åtgärderna är förenliga med dataskyddsförordningen samt med andra förpliktelser som Sverige har åtagit sig inom EU.

9.9 Konsekvenser för kommuner och regioner

Våra förslag skapar förbättrade förutsättningar för kommuner och regioner att dela data och skapa en mer datadriven verksamhetsutveckling. Det kan bland annat bidra till ökad effektivitet och kvalitet i dessa verksamheter. Som vi tidigare har konstaterat finns flera av områdena med störst potential för en ökad datadelning med integritetsfrämjande teknik inom kommunal och regional verksamhet.

9.9.1 Betydande nyttor för kommuner och regioner

Utredningens samhällsekonomiska analys visar att ökad datadelning med stöd av integritetsfrämjande teknik har en betydande nyttopotential för kommuner och regioner. Den samlade samhällsekonomiska nyttopotentialen av förbättrad datadelning för kommunerna bedöms uppgå till cirka 15–25 miljarder kronor per år.[35] Av denna nyttopotential bedöms en relativt stor andel (cirka 30–50 procent) vara beroende av användningen av integritetsfrämjande teknik vid datadelning. Nyttan finns främst i individnära verksamheter så som ekonomiskt bistånd, socialtjänst, arbetsmarknadsinsatser samt kommunal hälso- och sjukvård och omsorg. Teknikerna bedöms kunna bidra till förbättrad samordning inom och mellan kommuner samt mellan kommuner, regioner och statliga myndigheter. Det minskar dubbelutredningar, förkortar handläggningstider, förbättrar träffsäkerheten i stödinsatser och reducerar felaktiga utbetalningar.[36]

För regionerna uppskattas nyttopotentialen av förbättrad datadelning till omkring 10–20 miljarder kronor årligen.[37] En väsentlig del av regionernas nyttor bedöms kunna realiseras inom hälso- och sjukvården.[38] Även här bedöms en betydande andel (40–60 procent) av nyttopotentialen vara beroende av integritetsfrämjande teknik. Regionernas verksamhet präglas av höga integritets- och sekretesskrav vilket i dag begränsar möjligheterna till storskalig analys och samverkan mellan regioner samt sekundäranvändning av hälsodata. Integritetsfrämjande teknik möjliggör exempelvis federerade analyser,

[35] Bilaga 2, *Samhällsekonomisk analys*, s. 16.
[36] Bilaga 2, *Samhällsekonomisk analys*, s. 16.
[37] Bilaga 2, *Samhällsekonomisk analys*, s. 15.
[38] Bilaga 2, S*amhällsekonomisk analys*, s. 15.

säkra kliniska beslutsstöd och tvärregional uppföljning utan individexponering.[39]

9.9.2 Inga ökade kostnader för kommuner och regioner

Utredningens förslag innebär inte några krav eller skyldigheter för kommuner eller regioner att dela data eller att använda integritetsfrämjande teknik. Förslagen bedöms därmed inte ge upphov till några direkta kostnader för kommuner och regioner. Förslagen bedöms inte heller medföra ökade intäkter för kommuner och regioner.

9.9.3 Det kommunala självstyret

Det kommunala självstyret är reglerat i regeringsformen och kommunallagen (2017:725). En inskränkning i den kommunala självstyrelsen bör inte gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett den.[40] Eftersom förslagen inte medför nya krav eller skyldigheter för kommuner eller regioner är utredningens bedömning att förslagen inte medför en inskränkning i det kommunala självstyret.

9.10 Konsekvenser för statliga myndigheter

9.10.1 Betydande nyttor för statliga myndigheter

Vi bedömer att det finns en betydande nyttopotential även för statliga myndigheter vid datadelning med integritetsfrämjande teknik. Den samlade nyttopotentialen för statliga myndigheters förbättrade datadelning bedöms uppgå till 15–25 miljarder kronor per år. Av detta bedöms 30–50 procent vara direkt beroende av att integritetsfrämjande teknik används. Dessa nyttor är främst en följd av bland annat förbättrad regelefterlevnad inom skatte- och avgiftsområdet, minskade felaktiga utbetalningar samt kortare handläggningstider och lägre administrativa kostnader. Integritetsfrämjande teknik är

[39] Bilaga 2, *Samhällsekonomisk analys*, s. 15 f.
[40] 14 kap. 3 § regeringsformen.

främst en möjliggörare i de verksamheter där det krävs kontinuerlig, automatiserad och myndighetsövergripande analys.[41]

9.10.2 Förslagen medför ökade kostnader för statliga myndigheter

Utredningens förslag bedöms medföra indirekta och direkta kostnader för statliga myndigheter. *Indirekta* kostnader avser den kostnad som följer av användningen av integritetsfrämjande teknik (se avsnitt 9.8.1). *Direkta* kostnader avser kostnaderna för de statliga myndigheter som vi föreslår tilldelas uppdrag avseende integritetsfrämjande teknik. Här bedöms kostnaderna vara störst för Skatteverket och Digg givet att vi föreslår ett mer omfattande och löpande ansvar för dessa myndigheter.

De direkta kostnaderna för våra förslag uppgår totalt till cirka 165–198 miljoner kronor för perioden 2027–2030. Merparten av dessa kostnader avser uppdraget att tillhandahålla den förvaltningsgemensamma tjänsten för säker flerpartsberäkning, vilken ska utvecklas, testas och tas i produktion under denna period (se avsnitt 9.10.5). Från och med 2031 beräknas de direkta kostnaderna vara löpande och uppgå till cirka 67–70 miljoner kronor per år. Vi beskriver de direkta kostnaderna för statliga myndigheter närmare i avsnitt 9.10.4–9.10.10.

9.10.3 Förslagens kostnader har vägts mot nyttorna med ökad användning av teknikerna

Utredningen bedömer att de kostnader som följer av förslagen är nödvändiga för att det ska vara möjligt att realisera de potentiella nyttorna av en förbättrad datadelning med integritetsfrämjande teknik. Enligt vår samhällsekonomiska analys finns en risk att nyttorealiseringen uteblir om satsningarna blir alltför begränsade, vilket sammantaget kan innebära att de positiva konsekvenserna på det stora hela taget uteblir. Det handlar såväl om effektivitetsvinster och kostnadsbesparingar som höjd kvalitet i offentliga verksamheter och offentlig service.[42] Vi bedömer därför att det inte räcker

[41] Bilaga 2, *Samhällsekonomisk analys*, s. 13 f.
[42] Bilaga 2, *Samhällsekonomisk analys*, s. 69.

med enbart stöd och vägledning. Det krävs även en investering i förvaltningsgemensamma tjänster för att kunna realisera nyttorna.

Utredningen bedömer att den direkta kostnaden bör betraktas som en investering för staten eftersom vår samhällsekonomiska analys visar att de potentiella ekonomiska nyttorna vida överstiger kostnaderna. Enligt analysen förväntas en betydande del av de potentiella nyttorna realiseras inom en 5–10-årsperiod (se avsnitt 9.5.1). De ekonomiska nyttorna förväntas överstiga kostnaderna redan efter cirka 2 år.[43] För att säkerställa att dessa nyttor realiseras behöver dock användningen av teknikerna följas över tid. Likaså behöver effekterna och nyttorna utvärderas (se vidare i avsnitt 9.13).

Åtgärder för att begränsa kostnaderna för förslagen

För att de potentiella nyttorna ska kunna realiseras har våra förslag utformats så att de är tillräckligt genomgripande för att möjliggöra en relativt skyndsam och mer omfattande användning av teknikerna (se avsnitt 9.5.1). Vi har vägt detta mot behovet av kostnadseffektiva och proportionerliga åtgärder. Med det menas att vi har övervägt såväl mindre som mer omfattande åtgärder och vägt dessa mot de potentiella kostnader respektive nyttor de skapar.

Vi har exempelvis övervägt att enbart tillhandahålla stöd och vägledning till förvaltningen och inte en förvaltningsgemensam tjänst (se avsnitt 9.4.4). Enligt vår bedömning skulle det riskera att leda till en mer begränsad användning av moderna integritetsfrämjande tekniker och därmed en mer begränsad nyttorealisering. Vi har utgått ifrån att användningen av integritetsfrämjande teknik bör styras av de behov och potentiella användningsområden som finns i förvaltningen, snarare än att införa olika typer av generella krav på användningen. Det innebär att resurser riktas mot områden där det finns störst nyttopotential, i stället för till verksamheter där användningen och nyttan av teknikerna är mer begränsad. Utredningen har också strävat efter att lämna förslag som utnyttjar förvaltningens samlade expertis och kompetens, i stället för att samla och bygga upp ny kompetens hos en myndighet. Det innebär en mer effektiv användning av förvaltningens resurser och kompetens. Vidare anser utredningen att den offentliga förvaltningen bör till-

[43] Bilaga 2, *Samhällsekonomisk analys*, s. 66 f.

varata de lösningar och den kompetens om integritetsfrämjande teknik som finns på den privata marknaden, vilket kan bidra till ett mer kostnadseffektivt arbete.

9.10.4 Kostnader för Digg

Vi föreslår att Digg får i uppdrag att ta fram stöd och vägledning om integritetfrämjande teknik (avsnitt 8.3.2). I detta uppdrag ingår samverkan med Skatteverket, IMY, SCB och NCSC vid FRA.

Digg har uppskattat att kostnaden för uppdragen uppgår till cirka 9,5 miljoner kronor per år under de två första åren. Av detta avser 6–7 miljoner kronor personalkostnader, motsvarande cirka tre årsarbetskrafter. Därutöver tillkommer kostnader för bland annat konsulter med särskild expertkompetens samt för informationsinsatser. För det tredje året uppskattas kostnaden minska till cirka 8,5 miljoner kronor.

Vi bedömer att de uppskattade kostnadsökningarna inte ryms inom ramen för myndighetens nuvarande finansiering. Vi anser därför att kostnaderna bör finansieras genom att medel tillförs Diggs förvaltningsanslag, vilket vid sammanslagningen med Post- och telestyrelsen (PTS) förs över till förvaltningsanslaget för PTS (se vidare i avsnitt 9.11.1).

9.10.5 Kostnader för Skatteverket

Vi föreslår att Skatteverket får i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik (avsnitt 8.4.2). Tjänsterna ska utvecklas i samverkan med Digg, IMY, SCB och NCSC vid FRA. Den första tjänsten som ska tas fram inom ramen för uppdraget är en förvaltningsgemensam tjänst för säker flerpartsberäkning (se avsnitt 8.4.4).

Skatteverket uppskattar att kostnaden för den inledande analysfasen uppgår till cirka 46 miljoner kronor. I denna fas avser Skatteverket att utvärdera och genomföra en pilot. Analysfasen omfattar bland annat uppbyggnad av kompetens, marknadsdialog, anskaffningsförberedelser, utveckling av teknisk plattform och arkitektur, juridiska analyser, arbete med informationssäkerhet samt säkerhetstestning.

Kostnaden för den efterföljande etableringsfasen uppskattas av Skatteverket till minst 72–92 miljoner kronor beroende på ambitionsnivån gällande användbarhet. Denna fas omfattar produktionssättningen av tjänsten för säker flerpartsberäkning. När tjänsten väl är i bruk har Skatteverket uppgett att den årliga kostnaden för drift och förvaltning uppskattas till cirka 57 miljoner kronor.

Vi bedömer att de uppskattade kostnadsökningarna inte ryms inom ramen för myndighetens nuvarande anslag, utan förutsätter att medel tillförs myndigheten (se vidare i avsnitt 9.11.2).

9.10.6 Kostnader för IMY

Vi föreslår att IMY får i uppdrag att samverka med Digg och Skatteverket inom ramen för deras respektive uppdrag (avsnitt 8.3.5 och 8.4.5). Detta innebär att IMY behöver avsätta resurser för denna samverkan. IMY har uppskattat att kostnaden för detta kommer att uppgå till cirka 1,5 miljoner kronor per år, vilket motsvarar en årsarbetskraft.

IMY är bland annat tillsynsmyndighet enligt dataskyddsförordningen.[44] Tillsynsmyndigheterna ska vara oberoende i utförandet av sina uppgifter och utövandet av sina befogenheter i enlighet med dataskyddsförordningen. Detta innebär att medlemsstaterna ska säkerställa att tillsynsmyndigheterna bland annat förfogar över personal och finansiella resurser som behövs för att myndigheten ska kunna utföra sin tillsynsverksamhet.[45]

Utredningens bedömning är att de kostnader som IMY har för att samverka med Digg och Skatteverket inte bör hanteras inom nuvarande finansiering eftersom det skulle innebära att en del av befintligt förvaltningsanslag används till annat än tillsynsverksamhet. Kostnaderna bör därför finansieras genom att ytterligare medel tillförs IMY:s förvaltningsanslag.

[44] 2 a § förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten.
[45] Artikel 52.1 och 52.4 i dataskyddsförordningen.

9.10.7 Kostnader för SCB

Vi föreslår att SCB får i uppdrag att medverka i viss samverkan med andra myndigheter. Samverkan ska ske med Digg inom ramen för Diggs uppdrag att ta fram vägledning om integritetsfrämjande teknik (avsnitt 8.3.5) och med Skatteverket inom ramen för deras uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik (avsnitt 8.4.5). I båda dessa fall ska SCB:s medverkan begränsas till sådana integritetsfrämjande tekniker där myndigheten har etablerad erfarenhet genom sin statistikverksamhet, i första hand olika former av avidentifieringstekniker. Därutöver föreslås SCB bidra som samverkanspart i Socialstyrelsens uppdrag att utforska användningen av differentiell integritet inom hälso- och sjukvården (avsnitt 8.7.3).

SCB har bedömt att utredningens förslag kommer att medföra ökade årliga kostnader om cirka 400 000–800 000 kronor, vilket motsvarar 0,25–0,5 årsarbetskrafter. Kostnadsökningen hänför sig främst till behovet av att avsätta personalresurser för deltagande i samverkansaktiviteter i de aktuella uppdragen.

Utredningen bedömer att de tillkommande kostnaderna för SCB är begränsade och av sådan karaktär att de bör kunna hanteras inom myndighetens befintliga anslag. Det finns exempelvis överlappningar mellan de uppdrag vi föreslår och SCB:s roll som behörigt organ för dataförvaltningsförordningen samt med uppdraget att förbereda inrättandet av en funktion för främjande av datahantering.

9.10.8 Kostnader för NCSC vid FRA

Vi föreslår att NCSC vid FRA får i uppdrag att medverka i viss samverkan med Digg inom ramen för Diggs uppdrag att ta fram vägledning om integritetsfrämjande teknik (avsnitt 8.3.5). Vidare föreslås NCSC delta i samverkan med Skatteverket inom ramen för myndighetens uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik (avsnitt 8.4.5). I båda dessa sammanhang ska NCSC:s medverkan vara avgränsad till sådana integritetsfrämjande tekniker där myndigheten har särskild kompetens, i första hand tekniker som baseras på kryptografi.

NCSC har på grund av sin känsliga verksamhet inte kunnat lämna några kostnadsberäkningar men utredningen bedömer att omfatt-

ningen motsvarar den för SCB, det vill säga cirka 0,5 årsarbetskrafter. Sammantaget bedöms därför de föreslagna samverkansuppdragen att medföra ökade årliga kostnader om cirka 400 000–800 000 kronor. Kostnadsökningen avser främst behovet av att avsätta personalresurser för deltagande i samverkansaktiviteter, inklusive kompetensstöd, rådgivning och löpande medverkan i de aktuella uppdragen.

Utredningen bedömer att de tillkommande kostnaderna för NCSC är begränsade och av sådan karaktär att de bör kunna hanteras inom myndighetens befintliga anslag. NCSC har exempelvis redan en uppgift att samverka och utbyta information med privata och offentliga aktörer i frågor som rör cybersäkerhet.[46]

9.10.9 Kostnader för E-hälsomyndigheten

Vi föreslår att E-hälsomyndigheten får i uppdrag att tillsammans med Socialstyrelsen utforska möjligheten att använda integritetfrämjande teknik för en så kallad opt-out-lösning inom EHDS (avsnitt 8.7.4). E-hälsomyndigheten ska också samverka med Socialstyrelsen inom ramen för Socialstyrelsens uppdrag att utforska användningen av differentiell integritet inom hälso- och sjukvården (avsnitt 8.7.3).

E-hälsomyndigheten har bedömt att utredningens förslag kommer att medföra tillfälliga kostnader om cirka 3 miljoner kronor, vilket motsvarar två årsarbetskrafter.

De tillkommande kostnaderna bedöms vara begränsade och behovet av opt-out-lösningar följer redan av de krav som ställs genom EHDS-förordningen[47]. E-hälsomyndigheten ansvarar också för etableringen av den nationella digitala infrastrukturen för hälsa, vård och omsorg som utgör en central förutsättning för utbytet av hälsodata och genomförandet av kraven som följer av EHDS-förordningen. Utredningen bedömer därför att kostnaderna bör kunna hanteras inom E-hälsomyndighetens befintliga anslag.

[46] 2 § förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.
[47] Europaparlamentets och rådets förordning (EU) 2025/327 av den 11 februari 2025 om det europeiska hälsodataområdet och om ändring av direktiv 2011/24/EU och förordning (EU) 2024/2847.

9.10.10 Kostnader för Socialstyrelsen

Vi föreslår att Socialstyrelsen får i uppdrag att utforska användningen av differentiell integritet inom hälso- och sjukvården (avsnitt 8.7.3). I uppdraget ingår bland annat samverkan med E-hälsomyndigheten, Digg, IMY, SCB och minst en region. Socialstyrelsen föreslås även få ett uppdrag att tillsammans med E-hälsomyndigheten utforska möjligheten att använda integritetfrämjande teknik för en så kallad opt-out-lösning inom EHDS (avsnitt 8.7.4).

Socialstyrelsen har bedömt att utredningens förslag kommer att medföra tillfälliga kostnader om cirka 3 miljoner kronor, vilket motsvarar två årsarbetskrafter. Myndighetens uppskattning av kostnaderna gäller uppdraget att utforska differentiell integritet, eftersom myndigheten bedömer att kostnaderna för uppdraget om opt-out redan omfattas av nuvarande finansiering.

Utredningen bedömer att de tillkommande kostnaderna för uppdragen är begränsade. Behovet av opt-out-lösningar följer redan av de krav som ställs genom EHDS-förordningen. Det finns även synergier med Socialstyrelsens uppdrag att förbereda för rollen som ansvarigt organ för tillgång till hälsodata för sekundäranvändning enligt EHDS-förordningen. Det finns också synergier med Socialstyrelsens statistikansvar för den officiella statistiken inom bland annat hälso- och sjukvård och socialtjänst, där myndigheten löpande behöver utveckla säkra metoder för att skydda känsliga uppgifter. Utredningen bedömer därför att kostnaderna bör kunna hanteras inom Socialstyrelsens befintliga anslag.

9.11 Finansiering av utredningens förslag

9.11.1 Stöd och vägledning för integritetsfrämjande teknik

När det gäller Diggs uppdrag om stöd och vägledning bedömer vi att medel bör tillföras myndighetens förvaltningsanslag, det vill säga anslaget 2:6 Myndigheten för digital förvaltning. I samband med avvecklingen av Digg och inordnandet av myndighetens uppgifter i PTS i januari 2027 förs anslagsmedel över till anslaget 2:1 Post- och telestyrelsen.[48] Vår bedömning är att stöd och vägledning om teknikerna behöver vara ett långsiktigt uppdrag och att det där-

[48] Prop. 2025/26:1 *Budgetpropositionen för 2026*, utgiftsområde 22, s. 135.

med behövs en långsiktig finansiering. Genom att tillföra medel till myndighetens förvaltningsanslag ges Digg, och framöver Digitaliseringsmyndigheten, långsiktiga förutsättningar för att bygga upp en stödjande och vägledande verksamhet för integritetsfrämjande teknik. På så sätt finns också möjligheter att hitta synergier med Digitaliseringsmyndighetens övriga främjande och stödjande uppgifter inom närliggande områden.

Vad gäller medlen till IMY bedömer utredningen att även dessa bör tillföras IMY:s förvaltningsanslag, anslaget 6:3 Integritetsskyddsmyndigheten. Samverkan med Skatteverket och Digg om integritetsfrämjande teknik är enligt vår uppfattning ett viktigt och långsiktigt åtagande för IMY, givet deras uppdrag om integritetsskydd.

9.11.2 Den förvaltningsgemensamma tjänsten för säker flerpartsberäkning

Utredningen föreslår att den förvaltningsgemensamma tjänsten för integritetsfrämjande teknik ska utgöra en komponent i den nationella digitala infrastrukturen Ena. Finansieringen av Ena sker inom anslag 2:7 Digital förvaltning (Utgiftsområde 22). Villkoren för anslag 2:7 och anslagspost 1 Förvaltningsgemensam digital infrastruktur anger att anslagsposten får användas för utveckling och förvaltning av förvaltningsgemensam digital infrastruktur samt för bidrag till statliga myndigheter, kommuner och regioner.[49] Det innebär att Digg, som disponerar anslaget, kan fördela bidrag till andra offentliga aktörer vid utveckling och förvaltning av komponenter i Ena. Det sker exempelvis när det gäller drift och förvaltning av den digitala fullmaktstjänsten Mina ombud, som Bolagsverket ansvarar för. Det sker också när det gäller infrastrukturen för ärendeåterkoppling (Mina ärenden) som drivs av Skatteverket.[50]

Vi bedömer att det är lämpligt att även finansieringen av utvecklingen av den förvaltningsgemensamma tjänsten för säker flerpartsberäkning sker genom att medel tillförs anslag 2:7. Myndigheter som anskaffar anläggningstillgångar som finansieras av medel från anslag 2:7 medges undantag från kravet på lånefinansiering i kapitalförsörjningsförordningen (2011:210). Ett sådant undantag är lämp-

[49] Regeringens beslut, Fi2026/00587, *Regleringsbrev för budgetår 2026 avseende Myndigheten för digital förvaltning*, s. 4 f.
[50] Myndigheten för digital förvaltning (Digg), 2025-09125, *Årsredovisning 2025*, s. 77.

ligt om regeringen beslutar att finansieringen av den förvaltningsgemensamma tjänsten för säker flerpartsberäkning sker direkt genom anslag 2:7.[51] Även framtida integritetsfrämjande tekniker skulle därmed kunna finansieras genom bidrag från anslaget.

Det bör i villkoren för anslag 2:7 vara tydligt angivet att medlen ska användas för utveckling av den förvaltningsgemensamma tjänsten för säker flerpartsberäkning så att Skatteverket får fungerande planeringsförutsättningar. Det kan göras genom att lägga till en särskild anslagspost som specificerar att de tillhörande medlen får användas av Skatteverket för att genomföra uppdraget att utveckla tjänsten. Ett annat alternativ är att inom ramen för anslagspost 1 specificera att ett visst belopp får användas för Skatteverkets uppdrag att utveckla tjänsten.

Vad gäller drift och förvaltning av den förvaltningsgemensamma tjänsten för säker flerpartsberäkning bedömer vi att den bör finansieras genom att medel tillförs Skatteverkets förvaltningsanslag, anslag 1:1 Skatteverket (Utgiftsområde 3).

9.11.3 Finansiering av kostnaderna för förslagen

Vi har övervägt flera möjligheter till finansiering för kostnaderna för våra förslag (se avsnitt 8.5). Som tidigare konstaterats innebär utredningens förslag en betydande nyttopotential för hela den offentliga förvaltningen. Därför finns det inte ett givet utgifts- eller politikområde, med tillhörande anslag, där den främsta nyttohemtagningen kan förväntas ske. Vår bedömning är att det inte finns utrymme för att använda befintlig finansiering inom anslag 2:6–2:7 (Utgiftsområde 22), anslag 6:3 (Utgiftsområde 1) och anslag 1:1 (Utgiftsområde 3). Det innebär att medel behöver tillföras dessa anslag genom en omprioritering av medel från andra anslag.

Utredningens förslag skulle kunna finansieras genom en omfördelning av medlen från anslag 1:1 Utveckling av statens transportinfrastruktur (Utgiftsområde 22) till anslag 2:6–2:7 inom samma utgiftsområde, samt till anslag 6:3 Integritetsskyddsmyndigheten (Utgiftsområde 1) och till anslag 1:1 Skatteverket (Utgiftsområde 3). Dessa omfördelningar skulle endast i liten omfattning påverka möj-

[51] Ekonomistyrningsverket (ESV), 2020:23, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 19 f.

ligheterna att uppfylla syftena med anslag 1:1 Utveckling av statens transportinfrastruktur, eftersom de investeringskostnader som anslaget bland annat ska täcka är svårprognosticerade både i tid och medelsåtgång.[52]

På längre sikt finns det dock ett behov av att tydligare följa upp och utvärdera nyttorna av ökad datadelning genom integritetsfrämjande teknik. Då kan områden och verksamheter där det finns realiserade nyttor identifieras. I dagsläget finns det ingen mekanism för att realisera de ekonomiska nyttor som förvaltningsgemensamma tjänster ger upphov till, exempelvis i form av effektiviseringar och besparingar. Det innebär att de eventuella effektiviseringar och besparingar som följer av våra förslag inte kommer att återföras till statsbudgeten. I stället kommer dessa nyttor att uppstå i de olika verksamheter som använder teknikerna för datadelning, till exempel genom att resurser frigörs för annan verksamhet eller att kvaliteten i en verksamhet stärks. Nyttorna kommer också att vara externa, det vill säga tillfalla enskilda och företag. Att nyttorna ofta är förvaltningsgemensamma och externa innebär generellt en utmaning för hur finansieringen av förvaltningsgemensamma tjänster ska utformas.[53]

Digg har föreslagit att det i en långsiktig finansieringsmodell för den nationella digitala infrastrukturen Ena bör ingå att identifiera realiserbara besparingar av Ena. Dessa besparingar bör i sin tur fördelas inom ramen för regeringens budgetprocess, genom att en tredjedel tillfaller den myndighet som genomfört effektiviseringen, en tredjedel tillförs statskassan och en tredjedel används för att finansiera fortsatt utveckling av Ena. Förslaget förutsätter dock en förbättrad nyttorealisering och uppföljning hos berörda myndigheter av digitala utvecklingsprojekt.[54] En sådan fördelningsmekanism skulle erbjuda en möjlighet att synliggöra och omfördela de besparingar som görs med hjälp av integritetsfrämjande teknik. Den skulle därmed även potentiellt kunna täcka framtida kostnader för utveckling av nya förvaltningsgemensamma tjänster för integritetsfrämjande teknik.

[52] För liknande resonemang, se SOU 2021:97 *Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift*, s. 413 och SOU 2023:96, s. 293.
[53] ESV, *Styrning och finansiering av förvaltningsgemensam digital infrastruktur*, s. 9.
[54] Myndigheten för digital förvaltning (Digg), dnr 2024–4511, *Förslag till långsiktig utveckling och förvaltning av Ena, bilaga Långsiktig finansiering av Ena*, s. 7 f.

9.12 Tidsplan för uppdragen

Det kommer att ta 5–10 år innan utredningens förslag har fått fullt genomslag och omfattande nyttor kan realiseras. Den investeringskostnad som förslagen innebär kommer dock kunna täckas inom en kortare tid än så. Mot denna bakgrund bedömer utredningen att åtgärderna bör genomföras skyndsamt. I följande avsnitt redovisas ett förslag till tidsplan för genomförandet av respektive åtgärd.

9.12.1 Uppdragen som avser stöd och vägledning

Stöd och vägledning om integritetfrämjande teknik

Den vägledning och det stöd som föreslås tas fram av Digg är av komplex karaktär eftersom dessa behöver omfatta flera olika aspekter, såväl rättsliga som tekniska. Uppdraget bedöms därmed vara både resurs- och tidskrävande. Mot denna bakgrund bör regeringen ge Digg i uppdrag att ta fram vägledning om integritetsfrämjande teknik i myndighetens regleringsbrev för 2027. Inom ramen för uppdraget bör Digg även utarbeta en tidsplan för arbetet med att ta fram vägledningar för olika integritetsfrämjande tekniker. Tidsplanen bör avse perioden 2027–2030.

Skatteverket, IMY, NCSC vid FRA och SCB föreslås få i uppdrag att samverka med Digg vid framtagandet av stöd och vägledning (se avsnitt 8.3.5). Uppdragen bör ges i respektive myndighets regleringsbrev för 2027.

Första inriktningen för stöd och vägledning

Enligt våra förslag ska Digg initialt ta fram stöd och vägledning om differentiell integritet, syntetiska data samt metoder för att utvärdera risken för återidentifiering vid användning av avidentifieringstekniker (se avsnitt 8.3.4). Uppdraget bör anges i regleringsbrevet för 2027 och vägledningen bör vara färdigställd och publicerad inom 18 månader. Inom denna tid bör även andra stödjande insatser för att komplettera vägledningen utformas.

Differentiell integritet i hälso- och sjukvården

Socialstyrelsen föreslås få i uppdrag att undersöka användningen av differentiell integritet samt att analysera vilket spann för tillåten nivå av integritetsförlust (epsilon, ε) som kan vara lämpligt inom hälso- och sjukvård (se avsnitt 8.7.3). Uppdraget bör pågå parallellt med Diggs arbete med vägledning om differentiell integritet, men inledas först efter att Digg har kommit längre i detta arbete. Mot denna bakgrund bör uppdraget ges under hösten 2027. Eftersom uppdraget är avgränsat till sin omfattning bör det slutredovisas inom sex månader.

9.12.2 Uppdragen som avser förvaltningsgemensamma tjänster för integritetsfrämjande teknik

Tillhandahålla förvaltningsgemensamma tjänster

Utredningen bedömer att utvecklingen av förvaltningsgemensamma tjänster för integritetsfrämjande teknik är förenad med relativt lång genomförandetid. Mot denna bakgrund bör arbetet med att etablera sådana tjänster inledas så snart som möjligt. Skatteverket bör därför ges i uppdrag att tillhandahålla förvaltningsgemensamma tjänster för integritetsfrämjande teknik i myndighetens regleringsbrev för 2027.

Digg, IMY, NCSC vid FRA och SCB föreslås få i uppdrag att samverka med Skatteverket vid framtagandet av förvaltningsgemensamma tjänster (se avsnitt 8.4.5). Uppdragen bör ges i respektive myndighets regleringsbrev för 2027.

En förvaltningsgemensam tjänst för säker flerpartsberäkning

Skatteverket föreslås tillhandahålla en tjänst för säker flerpartsberäkning som första förvaltningsgemensamma tjänst för integritetsfrämjande teknik (se avsnitt 8.4.4). Uppdraget bör anges i regleringsbrevet för 2027.

Skatteverket har uppskattat att det kommer ta cirka 30 månader att genomföra en analysfas bestående av analys och pilotgenomförande. Denna fas sträcker sig från och med januari 2027 till och med juni 2029. Resultatet av denna analysfas, inklusive en mer detaljerad kostnadsanalys, bör delredovisas till regeringen, som därefter

kan fatta beslut om tilldelning av medel för genomförandefasen. Skatteverket kan påbörja genomförandefasen, det vill säga produktionssättning av tjänsten, från och med sommaren 2029. Tjänsten beräknas vara i bruk senast i början av 2031.

Uppdraget att testa en samarbetsanalys med säker flerpartsberäkning

Skatteverket och Försäkringskassan föreslås få i uppdrag att genomföra en samarbetsanalys med säker flerpartsberäkning (se avsnitt 8.7.2). Tidpunkten för när uppdraget bör ges är till viss del beroende av när Skatteverket är redo för pilotgenomförande. Mot denna bakgrund bedömer utredningen att uppdraget bör ges med start tidigast hösten 2028.

9.12.3 Uppdraget att utforska en opt-out-lösning med integritetsfrämjande teknik

Socialstyrelsen och E-hälsomyndigheten föreslås få i uppdrag att utforska om integritetsfrämjande teknik kan användas för att hantera uppgifter om enskilda som har motsatt sig användning av deras hälsodata, så kallad opt-out (avsnitt 8.7.4). En nationell opt-out-lösning behöver utvecklas inom ramen för EHDS innan mars 2029. Uppdraget bör därför påbörjas och avslutas under 2027, så att utvecklingen av en sådan tjänst kan genomföras under 2028.

9.13 Uppföljning och utvärdering

9.13.1 Uppföljning av teknikernas användning

Det finns skäl att särskilt följa utvecklingen av användningen av integritetsfrämjande teknik inom offentlig förvaltning. Detta eftersom området är relativt nytt och att användningen hittills varit begränsad. En sådan uppföljning är viktig för att kunna bedöma om användningen av teknikerna ökar och sker i en rimlig takt.

Uppföljningen kan med fördel ske inom ramen för Diggs uppgift att årligen följa digitaliseringen av den offentliga förvaltningen.[55] Denna årliga uppföljning genomförs genom undersökningar riktade till statliga myndigheter samt, sedan 2025, även till kommuner och regioner. I 2024 års undersökning låg fokus bland annat på i vilken utsträckning den offentliga förvaltningen är datadriven och hur artificiell intelligens används i verksamheterna.[56]

Genom att analysera resultaten från sådana undersökningar kan det gå att dra slutsatser om faktorer som bidrar till en lägre respektive högre användning av teknikerna, till exempel vad gäller olika organisatoriska och tekniska förutsättningar hos offentliga aktörer. Detta kan i sin tur underlätta att identifiera vilka åtgärder som regeringen, Digg och andra aktörer behöver genomföra för att öka användningen. En sådan uppföljning kan även bidra till att utveckla Diggs stödjande och vägledande uppdrag, bland annat genom att tydliggöra inom vilka verksamhetsområden, för vilka tekniker eller hos vilka aktörer det finns ett särskilt behov av stöd.

9.13.2 Utvärdering av genomförda åtgärder

Utredningen bedömer att det också bör genomföras en utvärdering av de åtgärder som har vidtagits i syfte att öka användningen av integritetsfrämjande teknik inom offentlig förvaltning. En sådan utvärdering bör omfatta såväl regeringens styrning av området som berörda myndigheters genomförande av tilldelade uppdrag, däribland Diggs stödjande och vägledande roll samt användningen av förvaltningsgemensamma tjänster.

Syftet med utvärderingen bör vara att bedöma om vidtagna åtgärder har varit tillräckliga och om de har lett till avsedda effekter. Detta gäller exempelvis i vilken utsträckning användningen av integritetsfrämjande teknik har ökat och om detta har bidragit till en mer effektiv och säker datadelning inom förvaltningen. Det kan i detta sammanhang vara relevant att analysera i vilken mån integritetsfrämjande teknik har möjliggjort ökad datadelning av personuppgifter och andra skyddsvärda uppgifter samt för vilka ändamål och inom vilka verksamhetsområden sådan datadelning har skett. Vi

[55] 2 § i förordning (2018:1486) med instruktion för Myndigheten för digital förvaltning.
[56] Myndigheten för digital förvaltning (Digg), dnr 2024-7510, *Uppföljning av statliga myndigheters digitalisering 2024 – om data och AI. En enkätundersökning.*

bedömer att en sådan utvärdering är motiverad mot bakgrund av den betydande nyttopotential som integritetsfrämjande teknik bedöms ha när det gäller att möjliggöra en förbättrad datadelning inom offentlig förvaltning.

Utvärderingen bör genomföras 3–5 år efter att de föreslagna åtgärderna har genomförts för att åtgärderna ska ha haft möjlighet att få genomslag. Utvärderingen bör lämpligen genomföras inom ramen för ett regeringsuppdrag till Statskontoret, i syfte att säkerställa att granskningen genomförs av en myndighet som inte är direkt involverad i genomförandet av åtgärderna. I uppdraget bör även ingå att lämna förslag till eventuella fortsatta åtgärder.

Kommittédirektiv 2025:64

Integritetsbevarande metoder för en mer datadriven och samverkande förvaltning

Beslut vid regeringssammanträde den 19 juni 2025.

Sammanfattning

En särskild utredare ska analysera förutsättningarna för den offentliga förvaltningen att använda integritetsbevarande metoder vid datadelning och föreslå åtgärder som kan främja användningen av sådana metoder. Syftet är att öka den offentliga förvaltningens förmåga att dela data samtidigt som skyddet för uppgifterna upprätthålls.

Utredaren ska bl.a.

- analysera förutsättningarna för myndigheter och andra aktörer i den offentliga förvaltningen att använda integritetsbevarande metoder vid datadelning och föreslå hur användningen kan förbättras,
- bedöma om det finns behov av att införa särskilda krav vid användning av integritetsbevarande metoder och i så fall lämna förslag på hur kraven bör regleras,
- analysera om en eller flera myndigheter bör ges i uppdrag att utveckla och tillhandahålla gemensamma tekniska tjänster, testmiljöer, testbäddar eller plattformar för integritetsbevarande metoder för datadelning,
- bedöma och lämna förslag på hur en funktion för rådgivning till den offentliga förvaltningen om datadelning och användning av integritetsbevarande metoder kan utformas och organiseras, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 30 juni 2026.

Uppdraget att analysera förutsättningarna för användning av integritetsbevarande metoder vid datadelning

Statliga myndigheter och andra aktörer inom den offentliga förvaltningen, inklusive kommuner, regioner, privata utförare, kommunalförbund och kommunala bolag, producerar, inhämtar och förvaltar stora mängder data. Om data delades i större utsträckning skulle detta kunna utveckla den offentliga förvaltningen till att bli mer datadriven och samverkande, samtidigt som innovation och förenkling för såväl människor som företag skulle kunna främjas ytterligare. Därutöver underlättar datadelning för uppföljningen och utvärderingen av olika typer av statliga insatser.

Förutsättningarna för att dela uppgifter styrs av bl.a. dataskyddsregelverket, offentlighets- och sekretesslagen (2009:400) och olika registerförfattningar. Detta innebär att alla data inte kan delas. Datadelningen inom den offentliga förvaltningen skulle dock kunna öka inom befintliga rättsliga ramar om aktörerna skulle använda s.k. integritetsbevarande metoder (i internationell litteratur kallade Privacy-Enhancing Technologies, PET). Användandet av sådana metoder skulle vidare kunna öka tillgängliggörandet av data för vidareutnyttjande för t.ex. innovation.

Integritetsbevarande metoder är metoder, bl.a. tekniska metoder, som syftar till att göra delning av data möjlig utan att personuppgifter eller andra skyddsvärda uppgifter, exempelvis företagshemligheter, röjs. Exempel på sådana metoder är anonymisering, generalisering och randomisering.

Användningen av integritetsbevarande metoder skulle kunna skapa förutsättningar för en ökad datadelning och därigenom en mer innovativ och samverkande offentlig förvaltning, utan att skyddet för den personliga integriteten eller andra skyddsvärden äventyras. Det kan bidra till att myndigheter utvecklar nya funktioner för bl.a. bekämpning av välfärdsbrott och en förenklad och mer behovsanpassad service till individer och företag. Användningen av integritetsbevarande metoder kan även bidra till en mer sömlös upplevelse för användarna i en gemensam digital ingång till den offentliga förvaltningen, i enlighet med ett delmål i Sveriges digitaliseringsstrategi 2025–2030 (Fi2025/01181). Datadelning där integritetsbevarande metoder används kan också främja verksamhetsutveckling, innovation och utvecklingen av artificiell intelligens (AI). AI-kommissionen har i sitt slutbetänkande AI-

kommissionens Färdplan för Sverige angett att användandet av integritetsbevarande metoder är avgörande för att förena innovation och integritet (SOU 2025:12).

Kapitel II i Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsförordningen) reglerar bl.a. hur myndigheter kan använda integritetsbevarande metoder för att kunna tillgängliggöra vissa kategorier av data för vidareutnyttjande. Förordningens regler om vidareutnyttjande är dock som huvudregel inte tillämpliga när myndigheter delar data med varandra.

Trots att det finns tekniska förutsättningar används integritetsbevarande metoder endast i begränsad omfattning av myndigheter och andra aktörer inom den offentliga förvaltningen.

I Sverige saknas det bestämmelser om hur den offentliga förvaltningen får använda integritetsbevarande metoder för att dela data med varandra. Det medför en osäkerhet om de rättsliga förutsättningarna för att använda sådana metoder. Vidare innebär det bl.a. osäkerhet i fråga om vilka krav som en aktör bör förhålla sig till vid användningen av integritetsbevarande metoder, exempelvis vilka metoder som är lämpliga att använda för olika typer av data. Mot denna bakgrund kan det finnas behov av att reglera användningen, genom att exempelvis ställa vissa minimikrav.

Utredaren ska därför

- analysera förutsättningarna för myndigheter och andra aktörer i den offentliga förvaltningen att använda integritetsbevarande metoder vid datadelning och föreslå hur användningen kan förbättras,
- bedöma om det finns behov av att införa särskilda krav vid användning av integritetsbevarande metoder och i så fall lämna förslag på hur kraven bör regleras,
- föreslå åtgärder i övrigt som kan främja en rättssäker, effektiv och ändamålsenlig användning av integritetsbevarande metoder för datadelning inom den offentliga förvaltningen, och
- lämna nödvändiga författningsförslag.

I forskningsverksamhet vid universitet och högskolor bedrivs redan i dag ett omfattande arbete för datahantering, bl.a. genom datahanteringsplaner och principer för att göra forskningsresultat sökbara, tillgängliga, kompatibla och återanvändningsbara, s.k. FAIR-princi-

per. Utredningen ska därför inte analysera eller lämna förslag som påverkar verksamheten vid universitet och högskolor.

Uppdraget att föreslå organisatoriska och infrastrukturella lösningar för gemensamt stöd

För att integritetsbevarande metoder ska kunna användas effektivt av alla aktörer inom den offentliga förvaltningen krävs det tillgång till en ändamålsenlig teknisk infrastruktur. En sådan infrastruktur bör inkludera gemensamma tekniska tjänster för integritetsbevarande metoder och kräver en tydlig ansvarsfördelning mellan berörda aktörer.

Redan i dag finns det digital infrastruktur, Ena, den nationella digitala infrastrukturen, som samordnas av Myndigheten för digital förvaltning (Digg). Ena kopplar samman olika system och kan bl.a. komma att utgöra den tekniska grunden för en gemensam digital ingång till den offentliga förvaltningen. Ena bör kunna vidareutvecklas för att också främja att den offentliga förvaltningen använder integritetsbevarande metoder.

I fråga om sådana integritetsbevarande metoder som kan användas för att tillgängliggöra data för vidareutnyttjande är Digg och Statistiska centralbyrån (SCB) behöriga organ enligt dataförvaltningsförordningen att ge stöd till andra myndigheter. Det behövs dock stödfunktioner som erbjuder rådgivning om användning av integritetsbevarande metoder i fall där myndigheter delar data med varandra.

Även om det finns viss digital infrastruktur och visst stöd för tillgängliggörande av data för vidareutnyttjande i dag, saknas det ett gemensamt stöd för att använda integritetsbevarande metoder inom offentlig förvaltning. Avsaknaden begränsar förmågan att fullt ut dra nytta av de möjligheter som tekniken erbjuder.

Utredaren ska därför

- analysera om en eller flera myndigheter bör ges i uppdrag att utveckla och tillhandahålla gemensamma tekniska tjänster, testmiljöer, testbäddar eller plattformar för integritetsbevarande metoder för datadelning,
- utifrån analysen, vid behov, lämna förslag på en eller flera sådana myndigheter,

- bedöma och lämna förslag på hur en funktion för rådgivning till den offentliga förvaltningen om användning av integritetsbevarande metoder för datadelning kan utformas och organiseras,
- lämna förslag på vilken befintlig myndighet eller vilka befintliga myndigheter som bör ansvara för en sådan funktion,
- föreslå eventuella ytterligare åtgärder som kan möjliggöra ett gemensamt stöd för användning av integritetsbevarande metoder inom offentlig förvaltning, och
- lämna nödvändiga författningsförslag.

Utredaren ska särskilt beakta Ena och de befintliga uppdrag som myndigheter har för att ge stöd i användningen av integritetsbevarande metoder.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för myndigheter, regioner och kommuner. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. Förslagen och deras finansieringslösningar ska utformas enligt principerna god budgetdisciplin, hög kostnadseffektivitet och hög samhällsekonomisk effektivitet. Vidare ska andra relevanta konsekvenser för myndigheter, kommuner och regioner analyseras, exempelvis behov av tekniska investeringar, organisatoriska förändringar eller ökad administration. Övriga samhällsekonomiska konsekvenser ska också redovisas.

Utredaren ska även bedöma konsekvenserna för privata aktörer, särskilt om förslagen kan påverka deras rättigheter, skyldigheter eller konkurrensförhållanden. Vad gäller konsekvenser för enskilda ska särskilt skyddet av den personliga integriteten bedömas.

Om något av förslagen i betänkandet påverkar den kommunala självstyrelsen ska en konsekvensanalys samt de avvägningar som har lett fram till förslaget särskilt redovisas.

Kontakter och redovisning av uppdraget

Utredaren ska föra en dialog med berörda statliga myndigheter, kommuner och regioner samt med företrädare för näringsliv, universitet och högskolor och andra relevanta aktörer. Vidare ska utredaren hämta in synpunkter från Digg, SCB och Integritetsskyddsmyndigheten i frågor som rör myndigheternas expertområden. Utredaren ska därutöver hämta in synpunkter från Nationellt cybersäkerhetscenter i frågor som rör informations- och cybersäkerhet. Utredaren ska vidare hålla sig informerad om och beakta relevant EU-rättslig utveckling och tillämpning, särskilt i fråga om dataskyddslagstiftningen, dataförvaltningsförordningen och andra EU-rättsakter som är relevanta för datadelning, säkerhet och skydd för personuppgifter.

Uppdraget ska redovisas senast den 30 juni 2026.

(Finansdepartementet)

Samhällsekonomisk analys av potentialen för ökad användning av integritetsfrämjande teknik i offentlig förvaltning

RISE - Underlag till Utredningen om integritetsfrämjande teknik i förvaltningen (Fi 2025:07)

Författare: Håkan Cavenius, RISE
Jie Li, RISE
Rickard Brännvall, RISE
Claus Popp Larsen, RISE

Stockholm, maj 2026

RISE RESEARCH INSTITUTES OF SWEDEN
Box 857, 501 15 Borås
info@ri.se


RI.
SE
Research Institutes
of Sweden

Sammanfattning

Denna rapport utgör en bilaga till betänkandet av Utredningen om integritetfrämjande teknik i förvaltningen (Fi 2025:07) och omfattar en samhällsekonomisk analys av de potentiella *nyttor* och *kostnader* som ett ökat införande och användning av s.k. integritetsfrämjande tekniker *(Privacy Enhancing Technologies, PET)* i svensk offentlig förvaltning skulle innebära.

Analysen omfattar statliga myndigheter, regioner och kommuner samt centrala tillämpningsområden såsom hälso- och sjukvård, socialtjänst och omsorg, skatte- och bidragskontroller samt tvärgående datadelning. Utgångspunkten för analysen är att digitalisering och datadelning är grundläggande förutsättningar för ökad effektivitet, kvalitet och innovation i offentlig sektor, samtidigt som krav på skydd för individens integritet och efterlevnad av dataskyddsregler sätter tydliga ramar för hur data får användas. Integritetsfrämjande tekniker utgör i detta sammanhang en viktig möjliggörare genom att de tillåter analys och samverkan kring data utan att exponera personuppgifter, vilket i praktiken kan undanröja centrala juridiska och organisatoriska hinder för datadelning. Detta innebär att en stor del av de mest avancerade och värdeskapande tillämpningarna – särskilt inom verksamheter som hanterar känsliga uppgifter – förutsätter att sådana tekniker används.

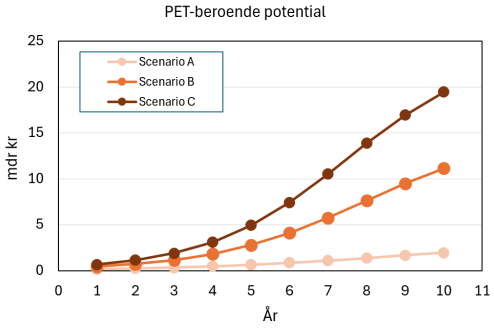
Analysen visar att de största nyttorna kan realiseras inom hälso- och sjukvården, där en ökad användning av PET möjliggör sammanhållen informationshantering, förbättrad diagnostik och mer effektiv resursanvändning. Den samlade nyttopotentialen inom detta område uppskattas till cirka 12,3–25,6 miljarder kronor per år. Nyttorna uppstår genom bland annat minskade dubbelundersökningar, kortare vårdtider, färre vårdskador samt förbättrade beslutsstöd baserade på artificiell intelligens. Även möjligheten till säker sekundäranvändning av hälsodata för forskning och innovation utgör en betydande del av potentialen.

Inom socialtjänst, omsorg och bistånd bedöms nyttopotentialen uppgå till cirka 4,0–9,6 miljarder kronor per år. Här är de centrala effekterna kopplade till förbättrad samordning av individstöd, tidigare identifiering av riskindivider samt ökad automatisering av kontroller och beslutsprocesser. Detta leder till kortare handläggningstider, minskad administration och ökad träffsäkerhet i stödinsatser. För skatte- och bidragskontroller uppskattas nyttopotentialen till cirka 2,9–6,4 miljarder kronor per år. PET gör det möjligt att genomföra avancerad och kontinuerlig analys av uppgifter mellan olika aktörer utan att rådata behöver delas, vilket bidrar till minskade felaktiga utbetalningar, förbättrad regelefterlevnad och effektivare bekämpning av välfärdsbrott.

Sammanvägt visar analysen ur flera tillämpningsperspektiv (mikroestimat) att nyttopotentialen i Sverige uppgår till cirka 19–42 miljarder kronor per år (efter ca 10 år vid en etablerad användning av PET), vilket ligger i samma härad som makroestimatet för den PET-beroende delen av datadelningens samhällsekonomiska värde. Det bör också nämnas att det finns ytterligare nyttopotential inom fler tillämpningsområden, men dessa har vi bedömt vara av mindre omfattning än de ovanstående, och omfattas ej av beräkningarna.

De kostnader som är förknippade med införandet av PET består dels av nationella investeringar i gemensam infrastruktur och stödjande funktioner, dels av lokala anpassningskostnader hos användande aktörer. På aktörsnivå är kostnaderna generellt begränsade och domineras av personella insatser för juridisk analys, verksamhetsanpassning och systemintegration.

För att belysa hur nyttor och kostnader utvecklas över tid har tre scenarier analyserats. *Scenario A* beskriver en låg ambitionsnivå där PET endast införs i begränsad omfattning, vilket leder till en relativt liten nyttorealisering över tid. *Scenario B* utgör ett mer balanserat alternativ där PET etableras som en operativ förmåga inom prioriterade områden och där en betydande del av nyttopotentialen kan realiseras. *Scenario C* representerar ett mer ambitiöst och transformativt angreppssätt där PET införs brett i offentlig förvaltning, vilket skapar förutsättningar för att realisera huvuddelen av den identifierade nyttopotentialen. Analysen visar att nyttorealiseringen följer en gradvis utveckling över tid, där effekterna initialt är begränsade men ökar i takt med att tekniken implementeras, standardiseras och integreras i verksamheterna. Diagrammet nedan visar utvecklingskurvorna för nyttopotentialen i de tre olika scenarierna:



Figur 1: Utvecklingen av nyttopotentialen i tre olika scenarier.

Rapportens samlade slutsatser är att integritetsfrämjande teknik har en central roll för att möjliggöra en mer effektiv, rättssäker och datadriven offentlig förvaltning. Den *potentiella samhällsekonomiska nyttan bedöms tydligt överstiga kostnaderna*, särskilt vid en mer omfattande och strukturerad implementering. Det konstateras slutligen att PET är en riskreducerande, men inte riskeliminerande, teknik. För att säkerställa en ändamålsenlig användning krävs därför fortsatt utveckling av styrning, metodstöd och kompetens.

Research Institutes of Sweden

Sammantaget visar analysen att en långsiktig och strategisk satsning på integritetsfrämjande teknik kan skapa betydande samhällsekonomiska värden, samtidigt som individens integritet och tilliten till offentlig förvaltning stärks.

RISE

Stockholm, maj 2026

RI.SE
Research Institutes of Sweden

Innehållsförteckning

Sammanfattning 3
1 Bakgrund 8
2 Metodik 10
3 Nyttopotential: Makroperspektivet 12
4 Nyttopotential ur statliga myndigheters, regioners och kommuners perspektiv 13
4.1 Statliga myndigheter 13
4.2 Regioner 15
4.3 Kommuner 16
5 Nyttopotential: Mikroperspektivet 18
5.1 Tillämpningsområde: Hälso- och sjukvård 19
5.1.1 Uppskattningar av den potentiella nyttan 20
5.2 Tillämpningsområde: Socialtjänst, omsorg och bistånd 37
5.2.1 Uppskattningar av den potentiella nyttan 38
5.3 Tillämpningsområde: Skatte- och bidragskontroller 41
5.3.1 Uppskattningar av den potentiella nyttan 42
5.4 Tillämpningsområde: Tvärgående tillämpningar 44
5.5 Summering av nyttopotentialen - Mikroperspektivet 46
6 Investerings- och kostnadsanalys 47
6.1 Skatteverket 47
6.2 Digg (Myndigheten för digital förvaltning) 49
6.3 IMY 50
6.4 SCB 50
6.5 NCSC/FRA 50
6.6 E-hälsomyndigheten 51
6.7 Socialstyrelsen 51
6.8 Lokala kostnader för de användande aktörerna 51
6.8.1 Grundläggande antaganden 51
6.8.2 Övergripande beräkningslogik för lokala kostnader 52
6.8.3 Lokala kostnadskomponenter 53
6.8.4 Beräkning för olika aktörstyper 55
6.8.5 Segmentsvisa schabloner 57

6.8.6 Aggregerade lokala kostnader per segment 61
6.9 Sammanställning av investerings- och kostnadsestimat 61
7 Scenarioanalys: Nyttopotential och kostnader 62
7.1 Investeringar och kostnader 62
7.2 Förväntad nyttorealisering 63
7.3 Scenarioanalysens beräkningsmodell 63
7.4 Scenario A 65
7.5 Scenario B 67
7.6 Scenario C 69
8 Slutsatser och reflektioner 71
9 Källförteckning 72

1 Bakgrund

Digitalisering är en central möjliggörare för ett välfungerande och hållbart samhälle på såväl nationell som regional, kommunal och individuell nivå. Dess betydelse förväntas fortsätta öka inom områden som framtidens sjukvård och omsorg, administration, rättsväsende, bistånd, forskning och kompetensförsörjning. För att digitaliseringens potential och samhällsnytta ska kunna realiseras krävs god tillgång till kvalitativa data. I många fall skapas ytterligare värde genom att data delas och används mellan flera olika aktörer och sektorer.

En central utgångspunkt är också att all databehandling ska ske i enlighet med gällande regelverk, särskilt dataskyddsförordningen (GDPR). Skyddet av individers personuppgifter och den personliga integriteten en grundläggande förutsättning för ett demokratiskt och tillitsbaserat samhälle. Det är därför avgörande att databehandling och dataanalys kan genomföras på ett säkert och ansvarsfullt sätt. Integritetsfrämjande teknik (*Privacy Enhancing Technologies*, PET) utgör en viktig del i detta arbete. PET omfattar metoder och tekniker som syftar till att skydda känsliga uppgifter vid insamling, lagring och behandling av data, samtidigt som potentialen och nyttan av datadelning och analys kan tillvaratas. Genom användning av sådana tekniker kan exempelvis mängden personuppgifter som behöver behandlas minska och skyddet för individers integritet stärkas.[1]

Behovet av integritetsskydd blir särskilt tydligt i samband med avancerad dataanalys och användning av maskininlärning och AI. Exempelvis används stora mängder medicinska och beteenderelaterade data för att identifiera samband, förbättra vårdinsatser eller upptäcka cyberhot. Eftersom dessa datamängder ofta innehåller känsliga personuppgifter, såsom hälsodata, finns risker kopplade till obehörig åtkomst, missbruk och intrång i den personliga integriteten. Sådana risker kan i förlängningen påverka rättssäkerhet, samhällstillit och ekonomisk stabilitet. Därutöver behöver offentliga och privata aktörer förbereda övergången till kvantsäkra system, mot bakgrund av den snabba utvecklingen inom kvantteknik och de framtida cyberhot som kvantdatorer kan innebära.

RISE har fått i uppdrag av Utredningen om integritetsfrämjande teknik (Fi 2025:07) att som ett separat underlag till betänkandets konsekvensutredning genomföra en samhällsekonomisk analys som består av följande delar:

- Beskrivning, analys, resonemang och beräkningar av *potentiella nyttoeffekter* (kvantitativt, monetärt och kvalitativt) exempelvis i form av ökad effektivisering, förbättrade tjänster, ökad servicenivå och ökade möjligheter till innovation, för de målgrupper och prioriterade teknologier som berörs av förslagen.

- Beskrivning, analys, resonemang och beräkning av kostnaderna för de målgrupper och prioriterade teknologier som berörs. Leveransen ska även behandla om/hur förslagen och konsekvenserna samspelar med andra satsningar och förslag, exempelvis inom AI.

[1] Läs mer om vilka tekniker som utgör integritetsfrämjande tekniker i kapitel 4 i betänkandet.

- Dessutom appliceras några olika scenarion för att beskriva potential- och kostnadsutvecklingen över tid för de prioriterade målgrupperna och tillämpningarna.

Avgränsningar och fokus för denna analys

Fokus för RISE analysuppdrag är följande[2]:

1. Primära **användare och målgrupper** (mottagande, användande aktörer):
    a. Statliga myndigheter
    b. Regioner
    c. Kommuner

2. Primära **tillämpningsområden**:
    a. Hälso- och sjukvård
    b. Socialtjänst, omsorg och bistånd
    c. Skatte- och bidragskontroller
    d. Tvärgående tillämpningsområden (där datadelning kan ske över sektorer och tillämpningsområden)

3. Primära **integritetsfrämjande tekniker** (*Privacy Enhancing Technologies, PET)* att implementera och nyttja är dessa:
    a. Differentiell integritet *(Differential Privacy, DP)*
    b. Federerad inlärning *(Federated Learning, FL)*
    c. Säker flerpartsberäkning *(Secure Multi-Party Computation, SMPC/MPC)*
    d. Syntetiska data *(Synthetic Data, SD)*

Notera: I rapporten används i många fall de engelska förkortningarna ovan (t.ex. PET), i syfte att förkorta och förenkla texter eller tabeller.

Såväl nationella (statliga) tjänster för integritetsfrämjande teknik som lokalt implementerade och nyttjade stöd omfattas av analysen.

[2] Inriktningen för analysen har tagits fram i dialog med sekretrariatet för utredningen.

2 Metodik

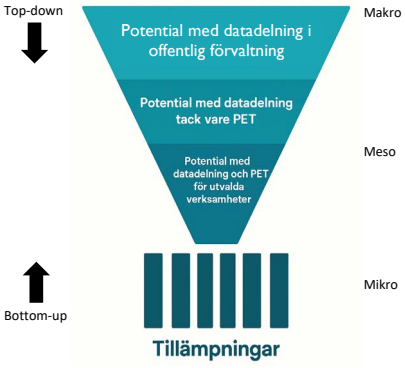
I vårt analysarbete har vi i huvudsak utgått från sekundärdata, mestadels rapporter och studier (svenska och internationella). Därefter har vi testat våra antaganden, hypoteser och preliminära resultat med forskarkollegor på RISE som har stor erfarenhet att arbeta med offentliga aktörer och datadelning, i såväl teori som praktik. Analysens tyngdpunkt ligger på de potentiella nyttorna med datadelning vid nyttjandet av integritetsfrämjande tekniker, men även investerings- och kostnadssidan berörs. Med *datadelning* avses här sådan teknisk och organisatorisk samverkan mellan offentliga aktörer som möjliggör bättre informationsunderlag för beslut, uppföljning, kontroll och samordning. Med *PET-beroende nytta* avses den del av nyttan som inte kan realiseras genom traditionell datadelning, regeländringar eller manuella processförbättringar, utan som kräver andra tekniska lösningar som möjliggör analys och matchning av data utan överflödig exponering av individuppgifter.

Vi har analyserat *nyttopotentialen* med ett ökat användande av integritetsfrämjande tekniker (PET) från två håll: ”top-down” / makronivå (t.ex. i andelstermer av BNP) och ”bottom-up” / mikronivå (per tillämpning) för att identifiera och kvantifiera de potentiella nyttor som genereras och som är av olika natur:

a) Effektiviserande / tids- eller kostnadsbesparande
b) Riskreducerande / säkerhetshöjande
c) Kvalitets- och servicenivåhöjande
d) Innoverande / nyskapande

Dessa beräkningar av nyttopotentialen ur såväl makro- som mikroperspektiv har sedan utgjort en samlad bild av den totala potentialen, för att ringa in nyttopotentialen från olika håll och med hjälp av olika uppskattningar (*triangulering)*. Vi har sedan lagt större tyngdpunkt på resultatet från mikroanalysen, tack vare dess högre detaljupplösning och robusthet när det kommer till summeringen av de olika tillämpningarnas nyttobidrag, när vi beräknat utfallet i de olika scenariona (se kapitel 7).

Nedan visas en principskiss hur vi har arbetat för att ringa in de potentiella nyttor som bedöms kunna genereras:



Figur 2: Principskiss för analysens metodik

De identifierade potentiella nyttorna beskrivs *kvalitativt (med beskrivande text)*, *kvantitativt* och *monetärt*.

Därefter har vi analyserat de uppskattade *initiala investeringar och löpande kostnader* som går att knyta till ovanstående nyttor och satsningar. Dessa investeringar och kostnader härstammar från de föreslagna satsningar som görs i utredningen, och de berörda aktörernas kostnadsestimat, samt en uppskattning av de kostnader som också uppstår på de mottagande aktörernas sida, d.v.s. användarna av PET (målgrupperna/segmenten: statliga myndigheter, regioner och kommuner).

Slutligen tillämpar vi tre olika *utvecklingsscenarier* för att uppskatta nyttopotentialens och kostnadernas utveckling över tid, beroende på ambitionsnivå, hur mycket som investeras, och när. Utgångspunkten för beräkningarna i de olika scenarierna är den nyttopotential som uppskatttats ur mikroperspektivet, tillsammans med investerings- och kostnadsestimaten.

Det sista kapitlet i rapporten sammanfattar våra slutsatser och reflektioner.

3 Nyttopotential: Makroperspektivet

OECD konstaterar att förbättrad datadelning i offentlig förvaltning kan generera mellan 0,1 % och 1,5 % av BNP i positiva årliga samhällsekonomiska effekter[3]. Om vi applicerar detta på Sverige (med en BNP på ca 6 500 mdkr 2025) ger det en nyttopotential på 7–98 miljarder kronor per år.[4]

Några andra internationella jämförelser (OECD, EU) visar att en effektivisering på 3–7 % är realistiskt att anta vid mogen datadelning.[5] Offentlig förvaltning i Sverige omsätter grovt 1 500 mdkr/år, vilket ger en effektiviseringspotential genom förbättrad datadelning i offentlig förvaltning på ca 45–100 mdkr/år.[6]

Sammanvägt ger ett flertal bedömningar, inkl ovanstående, att potentialen med *datadelning* i svensk offentlig förvaltning bör kunna ligga i intervallet ca 40–100 mdkr/år. Detta intervall återkommer i flera oberoende modeller och ligger i linje med jämförbara länder. Om vi för säkerhets skull gör en något *försiktigare* uppskattning så hamnar vi i vår studie i intervallet 30–80 mdkr/år (eftersom vi har gjort en viss avgränsande prioritering av verksamheter och tillämpningar).

Hur stor del som är PET-beroende av denna potential är en sammanvägd bedömning med input från flera olika källor, t.ex. OECD, WEF, Royal Society, G20, EU, DAMVAD/ Lantmäteriet[7]. Utifrån diverse forskning och uppskattningar ger detta att ca 30–50 % av all ekonomisk potential från datadelning i offentlig förvaltning är beroende av PET[8], d.v.s. ca **10–40 miljarder kr per år** (alternativt 12–50 mdkr/år vid den högre uppskattningen av datadelningspotentialen), som en utgångspunkt för makropotentialen (på nationell nivå) med PET i Sverige.

Det förekommer även uppskattningar med högre belopp. Dessa avviker dock från majoriteten av uppskattningarna genom att de har andra avgränsningar. Mot denna bakgrund har dessa inte inkluderats i analysen.

[3] Enhancing Access to and Sharing of Data, OECD, 2019.

[4] SCB. Nationalräkenskaper – BNP, löpande priser. Senaste tillgängliga utfall och prognoser för 2025–2026.

[5] OECD. Digital Government Review of Sweden: Towards a Data-Driven Public Sector, 2020. European Commission. Assessing the Economic Impacts of Open Data. Publications Office of the European Union, Luxembourg, 2020.

[6] Statistikmyndigheten SCB. Offentlig förvaltning – utgifter och konsumtion, 2025.

[7] OECD. Enhancing Access to and Sharing of Data, 2019; OECD/G20. Compendium on Data Access and Data Sharing. OECD Publishing, 2024. OECD. Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches. OECD Publishing, 2023. World Economic Forum. The Impact of Privacy-Enhancing Technologies on Data Collaboration, 2023. The Royal Society. From Privacy to Partnership: The Role of Privacy-Enhancing Technologies in Data Governance, London, 2023. DAMVAD Analytics & Lantmäteriet. The Economic Value of Open and Shared Data in Sweden, Stockholm, 2019.

[8] RISE bedömning baserad på OECD (2021; 2022; 2024) samt DAMVAD/Lantmäteriet (2019). Bedömningen att cirka 30–50 % av potentialen är PET-beroende baseras på en uppdelning av datadelningsnyttor i (a) sådana som kan realiseras med öppna data eller enklare informationsdelning, samt (b) sådana som kräver analys av känsliga personuppgifter över organisationsgränser.

4 Nyttopotential ur statliga myndigheters, regioners och kommuners perspektiv

För att öka nyttan med datadelning inom offentlig förvaltning finns flera parallella möjligheter som alla kräver säkrare och mer förutsägbar datadelning – framför allt i hälso- och sjukvården där t.ex. sekretess och patientdatalagen sätter ramarna. PET är ofta den saknade byggstenen som gör att man kan använda känsliga data utan att behöva flytta rådatan och kan därmed möjliggöra många av de initiativ som gör att värdet av datadelning för statliga myndigheter, regioner och kommuner kan realiseras.

Detta kapitel redovisar en samlad (och grov) bedömning av den samhällsekonomiska nyttan av förbättrad datadelning inom offentlig förvaltning, med särskilt fokus på de nyttor som förutsätter användning av integritetsfrämjande tekniker. Analysen omfattar segmenten *statliga myndigheter*, *regioner* samt *kommuner* och avser återkommande, strukturella effektiviserings- och kvalitetsvinster snarare än engångseffekter.

Notera att uppskattningarna i detta kapitel gällande nyttopotentialen av *datadelning* i offentlig förvaltning samt hur stor del av dessa som är *beroende av PET* är schematiska. I nästa kapitel (kapitel 5) görs en mer detaljerad analys och uppskattningar av nyttopotentialen för olika huvudsakliga tillämpningar som rör de tre segmenten, och som ger ett mer finfördelat och robust underlag.

4.1 Statliga myndigheter

Sverige har hög digital mognad men låg realiserad produktivitetsvinst bland vissa statliga myndigheter, främst p.g.a. stuprör, rättsosäkerhet och bristande tekniska skydd för känsliga individdata.[9] Det finns även en brist hos många offentliga aktörer att arbeta datadrivet, långsiktigt och hållbart, samt att kunna hantera data så de blir återanvändningsbara. Användandet av integritetsfrämjande tekniker är här en etablerad och internationellt rekommenderad lösning för att möjliggöra laglig, säker och skalbar datadelning. Internationellt används PET redan av bl.a. skatteförvaltningar, arbetsmarknads-myndigheter, statistikproduktion och brottsbekämpning (i regulatoriskt godkända former).

För staten innebär detta mindre rättslig fragmentering och större förutsägbarhet. Det rör sig ofta om strukturella hinder, som ger till effekt att datadelning sker för sent eller inte alls, trots lagstöd. GDPR och sekretess tolkas restriktivt och olika mellan myndigheter. Analys av data kräver idag ofta en central (eller lokal) hantering av persondata, alternativt omfattande manuella processer. Resultatet blir onödigt dubbelarbete, sämre beslutsunderlag, misstro mellan myndigheter och lägre produktivitet än jämförbara länder. För statliga myndigheter är de tydligaste nyttorna med PET följande:

- Effektivare kärnprocesser

[9] Digg. Uppföljning av statliga myndigheters digitalisering, 2023, 2024. Riksrevisionen, Statliga strategiska digitaliseringsprojekt – stora gemensamma utmaningar (RiR 2025:8), 2025. Vetenskapsrådet. Digitalisering i offentlig sektor: Nyttor, kostnader och mätbarhet, 2025.

- Mindre manuell handläggning, effektivare administration
- Automatisk faktakoll mellan myndigheter
- Minskade ledtider i tillstånd, ersättningar och tillsyn
- Minskade felutbetalningar
- Minskade bedrägerier
- Bättre styrning, prognoser och beredskap

OECD och Digg pekar samstämmigt på att en relativt låg datadelningsmognad, svag styrning och bristande tekniska möjliggörare för effektiv datadelning är den avgörande flaskhalsen för nästa steg i svensk statsförvaltning. I vägledningarna inom Diggs ramverk för öppna och delade data betonar man delning över gränser och interoperabilitet.[10] PET gör det möjligt även när data är skyddade (”delade data” med villkor), inte bara öppna data.

Ur primärt ett statligt perspektiv är PET en möjliggörare för att analysera och samverka kring data utan att tvingas dela rå persondata, uppfylla GDPR-principer redan i det initiala skedet då en tjänst skapas (inte som efterhandskontroll), samt minska behovet av undantag, samtycken och specialavtal.

Den samlade årliga nyttopotentialen för statliga myndigheters förbättrade datadelning bedömer vi uppgå till 15–25 miljarder kronor.[11] Denna nytta härrör främst från effektivare hantering av transfereringssystem, förbättrad regelefterlevnad inom skatte- och avgiftsområdet, minskade felaktiga utbetalningar samt kortare handläggningstider och lägre administrativa kostnader. En betydande del av dessa effektivitetsvinster är möjliga att uppnå genom generell digitalisering, förbättrade arbetssätt och utökad lagreglerad informationsdelning.

Vi bedömer att en relativt stor del (30–50 %) av den totala nyttan ovan är beroende av ett nyttjande av PET.[12] Denna del av nyttan avser framför allt sådana tillämpningar där kontinuerlig, automatiserad och myndighetsövergripande analys krävs, exempelvis avancerad riskklassning, löpande inkomst- och ersättningsmatchning samt realtidsbaserade avvikelselarm. Utan tekniskt säkerställd integritet och möjlighet till säker analys utan rådatadelning bedöms dessa nyttor inte kunna realiseras i praktiken.

[10] OECD, Digital Government Review of Sweden: Towards a Data-Driven Public Sector, OECD Publishing, 2019. OECD, Digital Government Index 2023 – Country results for Sweden, OECD Public Governance Directorate, 2023. Digg. Uppföljning av statliga myndigheters digitalisering 2024, (publicerad 2025). Digg, Vägledning om skyddade data, inom Öppna och delade data, 2026.
[11] RISE uppskattning baserad på OECD (2019; 2021), Digg (2024) och Riksrevisionen (2025). Bedömningen utgår från uppskattad total potential för datadelning i offentlig förvaltning samt en proportionering av statens andel och typiska effektområden såsom transfereringar, regelefterlevnad och administration.
[12] RISE bedömning baserad på OECD (2021; 2022; 2024). Bedömningen om att cirka 30–50 % av nyttan är PET-beroende baseras på en sammanvägd analys av vilka användningsfall som kräver tekniskt säkerställd datadelning (t.ex. kontinuerlig myndighetsövergripande analys, realtidsmatchning och avancerad riskklassning). Bedömningen baseras på en klassificering av identifierade användningsfall i sådana som kan realiseras med *konventionell datadelning* respektive sådana som kräver *integritetsbevarande analys* (PET) enligt OECD:s ramverk för datadelning.

4.2 Regioner

Regionerna hanterar stora mängder data i olika sammanhang och tillämpningar, t.ex. mycket känsliga patientdata, och de största nyttovinsterna uppstår där PET låser upp datadelning som annars är juridiskt blockerad – särskilt klinisk AI och sekundäranvändning. Regiongemensam hälsodatahantering har stor potential att skapa olika typer av samhälleliga nyttor, såväl för verksamheterna själva som för medborgarna. Regionernas samlade potential bedöms som hög – både produktivitetsvinster och kvalitetsförbättringar – när datadelning sker med PET och i linje med EHDS[13]. Regionernas datalager kan knytas samman för uppföljning och analys på nationell nivå. PET ger det integritets- och tekniklager som behövs för att köra gemensamma analyser utan central rådataflytt.

Genom att använda tekniken *federerad inlärning* så kan man utnyttja den stora potenialen med AI inom vården, det ger förbättrade beslutsstöd och diagnostik utan centraliserad bearbetning av känsliga patientdata. Sverige har redan börjat bygga upp en erfarenhet av federerad inlärning inom vården, vilket innebär att det redan finns inhemsk kompetens som det då finns en möjlighet att skala upp.

Vid kliniska tillämpningar (primäranvändning av data) så kan ett användande av PET möjliggöra färre dubbelundersökningar, snabbare behandlingsbeslut, trygg överföring mellan vårdgivare (av exempelvis patientdata via Nationell patientöversikt, NPÖ) – tack vare att datadelning kan göras säkert och enhetligt.

Vid uppföljning och analys (sekundäranvändning av data) kan PET åstadkomma samordnad uppföljning och kvalitetsanalys över regioner utan rådataflytt, bättre kapacitetsplanering och förbättrade vårdresultat. PET kan också åstadkomma säker åtkomst till hälsodata för forskning via etablering av ett nationellt organ för sekundäranvändning av data, HDAB[14], och federerade lösningar, med stark integritetsgaranti.

För regionsektorn, i huvudsak hälso- och sjukvård, bedömer vi att den årliga nyttopotentialen av förbättrad datadelning uppgår till 10–20 miljarder kronor.[15] Nyttan uppstår genom minskade vårdskador, färre onödiga eller duplicerade vårdkontakter, effektivare vårdlogistik samt bättre besluts- och uppföljningsunderlag. Även effektivisering av administrativa processer och kliniska arbetsflöden bidrar till nyttan.

Av denna potential bedömer vi att en relativt stor andel (ca 40–60 %) är beroende av PET för att kunna realiseras.[16] Regionernas verksamhet präglas av höga integritets- och sekretesskrav, vilket i dag kraftigt begränsar möjligheterna till storskalig analys och samverkan mellan regioner samt sekundäranvändning av vårddata. PET möjliggör exempelvis federerade

[13] Europeiska hälsodataområdet, *European Health Data Space, EHDS.*
[14] *Health Data Access Body, HDAB.*
[15] RISE bedömning baserad på OECD (2019; 2022; 2024) om nyttor av hälsodatadelning, EU/EHDS konsekvensanalyser av produktivitets- och kvalitetsvinster samt nationella kostnads- och effektstudier av vårdprocesser.
[16] RISE uppskattning baserad på OECD (2021; 2022; 2024) om behov av tekniska skydd för avancerad analys EU/EHDS om sekundäranvändning och federerad analys samt en uppdelning av användningsfall i konventionell datadelning vs integritetsberoende analys.

analyser, säkra kliniska beslutsstöd och tvärregional uppföljning utan individexponering. Utan dessa tekniska lösningar bedöms merparten av de strukturella nyttorna inom vård och hälsa inte kunna realiseras.

4.3 Kommuner

Även kommuner hanterar mycket känsliga individdata (barn/elevhälsa, socialtjänst, LSS, äldreomsorg etc). Lagstiftning (t.ex. GDPR), sekretess, osäkerhet kring ”ändamålsglidning” samt resurs- och kunskapskrävande manuella processer gör att nödvändig samverkan ofta uteblir eller sker manuellt. Målet med förbättrad datadelning är att skapa effektiva, rättssäkra och datadrivna arbetssätt utan att behöva centralisera persondata (nationellt).

Många kommuner är också små och har också relativt begränsade IT-resurser och organisatoriska resurser, trots ett brett ansvar och en bred verksamhet. Dessutom är man i hög grad beroende av samverkan inom kommunen, mellan kommuner, samt med samverkan med statliga myndigheter och regioner.

PET ger kommunerna en ökad möjlighet att utöva en laglig och effektiv samverkan. Först då kan man skapa effektiva, rättssäkra och datadrivna arbetssätt utan att centralisera känsliga persondata. Juridisk och organisatorisk trygghet är då ofta den största vinsten som man uppnår, samt en tydligare ansvarsfördelning och minskad oro för enskilda tjänstemän att göra fel. PET ersätter inte laglig grund men möjliggör dataminimering och ändamålsbegränsning i praktiken (GDPR-principer), samt ger lägre riskklassning jämfört med centraliserad samkörning av persondata.

Kommunsektorns årliga nyttopotential av förbättrad datadelning bedömer vi uppgå till 15–25 miljarder kronor.[17] Nyttan är främst kopplad till individnära verksamheter såsom ekonomiskt bistånd, socialtjänst, arbetsmarknadsinsatser samt vård och omsorg. Effektivare samordning mellan kommuner och mellan kommun och stat bedöms kunna minska dubbelutredningar, förkorta handläggningstider, förbättra träffsäkerheten i stödinsatser och reducera felaktiga utbetalningar.

Av denna nyttopotential bedöms en relativt stor del (ca 30–50 %) vara beroende av PET.[18] Denna del av nyttan avser framför allt automatiserad och kontinuerlig samordning mellan kommunala och statliga system, säker matchning av individstöd samt tidig identifiering av risker och felaktigheter. Utan PET begränsas kommunerna till manuella, punktvisa och resurskrävande kontroller, vilket kraftigt reducerar möjligheterna till storskalig effektivisering.

[17] RISE bedömning baserad på OECD (2019; 2022; 2024) om produktivitetsvinster från datadelning, studier om offentlig sektors effektivisering samy nedbrytning av total datadelningspotential (30–80 mdkr/år) till kommunsektorn baserat på verksamhetsandel och användningsområden.
[18] RISE uppskattning baserad på OECD (2021; 2022; 2024) om behov av tekniska skydd för avancerad analys samt klassificering av användningsfall i kommunsektorn (manuella vs automatiserade/flödesbaserade).

Beroendet av privata utförare i kommunal och regional verksamhet

I många kommunala och regionala verksamheter och tillämpningar så återfinns en eller flera privata utförare (t.ex. inom hemtjänst, äldreomsorg, primärvård, HVB-hem), och för att potentialen med datadelning skall kunna nås så krävs att samverkan kring känsliga data som dessa aktörer hanterar också omfattas. PET kan naturligtvis användas även i dessa situationer men det ökar komplexiteten och kräver då att de privata aktörerna inkluderas i implementeringen och processerna för datadelning med hjälp av PET.

5 Nyttopotential: Mikroperspektivet

För de prioriterade tillämpningsområdena gör vi i detta kapitel en analys av nyttorna (kvalitativt och kvantitativt) för statliga myndigheter, regioner och kommuner, som vi därefter aggregerar (och vid behov extrapolerar) till nationell makronivå. Varje kvantifiering av en tillämpning är baserad på offentligt tillgänglig statistik, dataunderlag från rapporter samt en eller flera uppskattningar/antaganden av effekten av att använda sig av PET.

Notera att de uppskattningar av nyttopotentialen som görs för de identifierade tillämpningarna bygger på att PET tillför de mekanismer som gör att en nytta kan realiseras fullt ut, men i viss mån skulle detta också kunna ske med hjälp av andra metoder och förbättrade arbetssätt. Dessa metoder och faktorer tar vi ej hänsyn till i denna analys.

Effekterna kan vara av olika natur:

a) Effektiviserande / tids- eller kostnadsbesparande
b) Riskreducerande / säkerhetshöjande
c) Kvalitets- och servicenivåhöjande
d) Innoverande / nyskapande *(svårare att uppskatta)*

Såväl OECD som Produktivitetskommissionen påtalar att Sverige generellt sett har en relativt hög digital mognad men en låg realiserad produktivitetsvinst i offentlig förvaltning p.g.a. stuprör, juridisk osäkerhet och bristande datadelning.[19] Man pekar också på att *fragmenterade datalager* är en viktig orsak till låg offentlig produktivitet trots en relativt hög *generell* digital mognad. Riksrevisionen och Digg pekar på utmaningar inom offentliga verksamheter med exempelvis[20]:

- Dubbeldokumentation och dubbelarbete
- Manuella, riskfyllda och bristande kontroller (t.ex. av utbetalningar av olika bidrag)
- Onödiga, ineffektiva parallella IT-system implementeras
- Bristande samordning mellan stat, region och/eller kommun

En betydande del av datadelningens potential blockeras idag av rättsliga och etiska begränsningar, som just PET adresserar. Ett flertal aktörer och analyser pekar på att dagens datadelning inte når sin potential, p.g.a. att lagrum (t.ex. GDPR) sätter käppar i hjulen för datadelning. Detta medför ofta en stor återhållsamhet i analys och beslutsfattande p.g.a. rättsliga osäkerheter och brist på pålitliga dataskydd. Dessutom saknas många gånger processer, kompetens och förmåga att effektivt hantera och dela data på ett säkert sätt hos offentliga aktörer, inte minst hos regioner och kommuner.

[19] OECD. Digital Government Review of Sweden: Towards a Data-Driven Public Sector. OECD Publishing, 2020. SOU 2025:96 Fler möjligheter till ökat välstånd.
[20] Riksrevisionen. Samverkan mellan myndigheter – hinder och möjligheter i individärenden (RiR 2020:22). Stockholm, 2020. Riksrevisionen. Ändrade förhållanden – ineffektiv hantering i socialförsäkringen (RiR 2026:4). Stockholm, 2026. Myndigheten för digital förvaltning, Digg. Stuprör, juridik och teknik – hinder för datadelning i offentlig förvaltning, 2023.

Genom att på ett ordnat vis införa och öka användningen av olika PET så kan man uppnå exempelvis säkra databehandlingar och beräkningar utan att exponera rådata, analyser utan att behöva identifiera enskilda individer och ge en ändamålsenlig och kontrollerad insyn utan att parterna behöver ha full åtkomst till alla data. PET krävs i delar av offentlig förvaltning som hanterar känsliga uppgifter för att över huvud taget få använda och dela data (t.ex. inom vård, socialförsäkring, rättsväsende). PET möjliggör alltså ”samkörning” mellan olika aktörer utan att behöva dela data på ett traditionellt sätt.

Till de offentliga aktörerna skall även läggas de *privata aktörer* som i många fall agerar utförare av regioners och kommuners verksamheter (t.ex. hemtjänst, äldreomsorg, HVB-hem), och även här behövs datadelning för att skapa ytterligare nytta. De privata aktörerna inkluderas ej i denna analys.

G20/OECD beskriver datadelning som ett av de största outnyttjade värdeskapande verktygen i offentlig förvaltning, och lyfter primärt fram dessa nyttor[21]:

- Effektivare styrning
- Minskad duplicering
- Bättre policyträffsäkerhet
- Bättre resursallokering

Nedan följer en analys av de tre verksamhetsindelade *tillämpningsområdena* som vi analyserat kvalitativt, kvantitativt och monetärt vad gäller nyttopotentialen, samt ett fjärde mer generiskt tillämpningsområde, som är mer verksamhetsneutralt och tvärgående till sin natur.

5.1 Tillämpningsområde: Hälso- och sjukvård

Hälsodata är till karaktären av känslig natur, ofta med en mycket hög andel personuppgifter och med stor påverkan av dataskyddsbestämmelser. Ett ökat användande av PET är sannolikt en förutsättning för en effektivare datadelning inom detta tillämpningsområde och för möjligheten att åstadkomma ökad nytta. Exempelvis kan man träna AI-modeller för förbättrade beslutsstöd och diagnostik utan centraliserad bearbetning av känsliga patientdata. Träningen av AI-modeller sker då lokalt i varje region, endast själva uppdateringen och förbättringen av modellen aggregeras och delas med bidragande parter, t.ex. olika regioner. Passar exempelvis bilddiagnostik, triagering, riskprediktion och språkmodeller baserade på klinisk text.

De viktigaste tillämpningarna och nyttorna som identifierats inom hälso- och sjukvård är:

1. **Sammanhållen vårdinformation**, som exempelvis ger
   a) Färre dubbelundersökningar
   b) Minskade risker för fel

[21] OECD, G20 Compendium on Data Access and Sharing Across the Public Sector and with the Private Sector for Public Interest, OECD Publishing, 2024. OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463.

c) Kortare vårdtider
d) Bättre prioritering och resursplanering
a) Säkrare överföring av patientdata mellan vårdgivare.

2. **Klinisk AI och beslutsstöd**, som exempelvis ger
   a) Ökad precision i bilddiagnostik
   b) Mer träffsäker prediktion av vårdbehov
   c) Bättre personal- och resursplanering
   d) Snabbare behandlingsbeslut.

3. **Sekundäranvändning av data**, som exempelvis ger
   a) Förbättrade förutsättningar för forskning och utveckling (t.ex. av behandlingsmetoder och läkemedel) utan risk för individexponering
   b) Säker åtkomst till hälsodata för forskning via en nationell roll som *Health Data Access Body* (HDAB) och federerade lösningar – med stark integritetsgaranti
   c) Samordnad uppföljning och analys över olika regioner utan att behöva flytta och centralisera rådata.

4. **Nationella kvalitetsregister och förbättrad statistik,** som exempelvis ger
   a) Förbättrade möjligheter till gemensam uppföljning, baserad på många källor utan risk för individexponering
   b) Gemensamma analyser/matchningar (t.ex. kvalitetsuppföljning mellan regioner) utan att någon ser andras rådata
   c) Förbättrade möjligheter till kvalitativ, publicerbar statistik och testresultat utan exponering av identifierbara individer.

5. **Kris och smittspårning,** som exempelvis ger
   a) Snabbare analys och möjlighet till tidigare insatser (prevention)
   b) Övervakning och följsamhet utan risk för individexponering.

6. **Förbättrad datadelning inom EU baserad på EHDS,** som exempelvis ger
   a) Produktivitets- och kvalitetsvinster
   b) Ökad primäranvändning av EU-gemensamma hälsodata
   c) Ökad sekundäranvändning av EU-gemensamma hälsodata.

5.1.1 Uppskattningar av den potentiella nyttan

Nedan följer ett flertal beskrivningar på hur vi har uppskattat den *potentiella nyttan* (i kvalitativa, kvantitativa och monetära termer) för de ovanstående tillämpningarna inom hälso- och sjukvård. Dessa uppskattningar baseras på relativt *försiktiga antaganden* som en utgångspunkt.

För varje tillämpning gör vi därefter en summerande uppskattning uttryckt i ett *intervall* baserad på de antaganden och beräkningar av nyttopotential som redovisats, för att generera såväl en *konservativ* som en mer *progressiv* uppskattning av nyttan i monetära termer.

Den ekonomiska nyttoberäkningen följer i flertal fall en ekonomisk analysmodell bestående av tre huvudsakliga steg:

1. Identifiering av nyttodrivare: För varje nyttokategori definieras relevanta händelser som kan påverkas positivt av PET, exempelvis antalet dubbelundersökningar, förekomsten av medicinska fel eller genomsnittligt antal vårddygn.
2. Volymuppskattning: För varje händelsetyp uppskattas a) antal patienter per år, b) antal händelser per patient och c) andelen händelser där PET gör skillnad. Detta skapar en kvantitativ grund för att beräkna den potentiella nyttan.
3. Monetär värdering: Relevant kostnad per händelse fastställs, baserat på etablerade enhetskostnader inom svensk hälso- och sjukvård. Exempel på kostnadsparametrar:

    - Vårddygn: 10 000 - 18 000 kr
    - Labbprov: 50 - 500 kr
    - MR-undersökning: 4 000 - 8 000 kr
    - Läkemedelsrelaterad skada: 50 000 - 200 000 kr

Total monetär nytta beräknas generellt enligt formeln:

Årsnytta = Volym före PET × Kostnad per händelse × Påverkansgrad i %

Uppskattningar av påverkansgraden är baserade på internationella studier (som ofta visar på minst 5–10 % förbättring vid ändmålsenlig ”dataintegration” (samkörning) vid användning av PET, samt olika pilotstudier med förbättrad samordning mellan regioner (10–25 % förbättring).[22] De angivna intervallen 5–10 % respektive 10–25 % utgör inte exakta punktestimat utan sammanvägda intervall baserade på internationella studier, policyanalyser och pilotresultat. De lägre nivåerna avser bred implementering under normala förutsättningar, medan de högre nivåerna främst observerats i avgränsade piloter och i samband med strukturell förbättrad samordning mellan organisationer.

1. Sammanhållen vårdinformation

Införandet av PET för att möjliggöra säker och *sammanhållen vårdinformation* har en betydande potential att generera stora ekonomiska och kvalitativa nyttor. Bland de största effekterna återfinns i reducerad vårdtid, minskade dubbelundersökningar och färre medicinska fel, som i sin tur ger minskat lidande för patienter och anhöriga. Studier visar att bristande informationsdelning mellan vårdgivare leder till dubbelprovtagning och dubbel

[22] OECD. Enhancing Access to and Sharing of Health Data: Reconciling Privacy, Security and Public Interest. OECD Publishing, 2021; OECD. Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches. OECD Publishing, Paris (2023); McKinsey Global Institute. The next normal in R&D productivity. McKinsey & Company, 2020; OECD. Digital Government Review of Sweden: Towards a Data-Driven Public Sector. OECD Publishing, 2020; European Commission. Assessing the Economic Impacts of Open Data. Publications Office of the European Union, Luxembourg, 2020.

bilddiagnostik, särskilt radiologi. Effekterna av delade journalsystem och informationsutbyte på minskad dubbelundersökning är väldokumenterad.

1a) Färre dubbelundersökningar

Bristfällig eller otillgänglig information leder ofta till att undersökningar upprepas i onödan.[23] Genom förbättrad informationsdelning via PET kan dessa undvikas (nedanstående antaganden bedöms vara konservativa).[24]

Estimerad nyttopotential:

- Volym röntgenundersökningar: 2 000 000 undersökningar/år[25]
- Antagande: Andel dubbelundersökningar p.g.a. bristande informationsdelning: 8–10 %[26]
- Genomsnittlig kostnad per undersökning: 1 500 kr[27]
- Undvikbara undersökningar: 2 000 000 × 0,08/0,10 = 160 000 – 200 000

Årsnytta: **240 – 300 mkr**

1b) Minskade medicinska fel och risker

Tillgång till korrekt, aktuell och relevant information minskar sannolikheten för felaktiga medicinordinationer, diagnoser eller behandlingar.[28] Sådana informationsrelaterade brister är en välkänd orsak till medicinska fel i slutenvården, särskilt vid vårdövergångar och komplexa vårdsituationer.[29] PET möjliggör detta samt tillgång till relevant vårdinformation över organisationsgränser utan att kompromissa med patientens integritet.[30]

[23] Ayabakan, S., Bardhan, I., Zheng, Z. E., & Kirksey, K. (2017). The impact of health information sharing on duplicate testing. MIS Quarterly, 41(4), 1083–1103.
[24] Rome, B. N., et al. (2020). Effect of shared electronic health records on duplicate imaging after hospital transfer. Journal of General Internal Medicine, 35(5), 1617–1619. EIT Health & Swedish Medtech. (2023). Implementing the European Health Data Space in Sweden.
[25] Strålsäkerhetsmyndigheten. (2025). Fem års rapportering om röntgenstatistik – utmaningar och utvecklingsbehov (SSM Rapport 2025:07).
[26] Ayabakan, S., et al. (2017). The impact of health information sharing on duplicate testing. MIS Quarterly, 41(4), 1083–1103. Steinkamp, J., Kantrowitz, J. J., & Airan-Javia, S. (2022). Prevalence and sources of duplicate information in the electronic medical record. JAMA Network Open, 5(9), e2233348.
[27] Vårdgivarguiden / Region Stockholm. (2025). Prislista för radiologiska undersökningar – fullbetalande patienter. Evidia Sverige, 2024. Prislista radiologiska undersökningar.
[28] Chimbo, B., & Motsi, L. (2024). The effects of electronic health records on medical error reduction. JMIR Medical Informatics, 12, e54572. Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. Saudi Medical Journal, 38(12), 1173–1180.
[29] Sergi, C. M. (2024). Medical errors can cost lives. Archives of Medical Science, 20(4), 1378–1383.
[30] 1177 Vårdguiden, 2024. Sammanhållen journalföring – så skyddas och hanteras dina uppgifter.

Estimerad nyttopotential:

- Ca 600 000 slutenvårdstillfällen per år[31]
- Konservativ uppskattning (1 %): 6 000 informationsrelaterade fel/år[32]
- Antagande kostnad per fel: Den genomsnittliga samhällsekonomiska kostnaden per vårdrelaterat fel har i internationell och nordisk litteratur ofta uppskattats till omkring 100 000 kr per händelse, baserat på förlängd vårdtid, kompletterande behandlingar och ökad resursåtgång.[33]
- Antagande: PET minskar felfrekvensen med 10–20 %. Studier av elektronisk informationsdelning och sammanhållna journalsystem visar att tillgång till korrekt information kan minska frekvensen av medicinerings- och behandlingsfel med cirka 10–20 %, särskilt i slutenvård och vid akuta situationer.[34]

Årsnytta: **60 – 120 mkr**

1c) Kortare vårdtider

Försenade beslut, fördröjd informationsåtkomst och fragmenterade patientdata bidrar till längre vårdtider, särskilt i akuta vårdflöden där kliniska beslut måste fattas snabbt och ofta med begränsad information.[35] Bristande tillgång till tidigare journaluppgifter, provsvar och läkemedelslistor leder till väntetider, dubbelarbete och onödiga förseningar i både akutmottagning och efterföljande slutenvård.[36] Initiativ som NDI (Nationell digital infrastruktur) för hälsa, vård och omsorg ökar möjligheten att dela information tryggt och säkert mellan olika system och aktörer, och i detta sammanhang kan ett ökat användande av PET möjliggöra snabbare och mer effektiva arbetsflöden. Det sker genom att vårdpersonal får tillgång till relevant patientinformation över organisationsgränser, vilket minskar flaskhalsar och underlättar tidigare beslut om diagnostik, behandling och inläggning.

[31] Socialstyrelsen, 2026. Statistik om sjukdomar behandlade i sluten vård. Statistikmyndigheten SCB. (2025). Sjukdomar i sluten vård.
[32] Sveriges Kommuner och Regioner (SKR), 2024. Skador inom somatisk vård 2013–2023.
[33] Durand, M., et al. (2024). Evaluating the costs of adverse drug events in hospitalized patients. Health Economics Review, 14, 11. Ranasinghe, S., et al. (2024). Calculating the cost of medication errors. BMJ Open Quality, 13(2), e002570.
[34] Office of the National Coordinator for Health Information Technology. (2025). Health Information Exchange – Benefits. Holmgren, A. J., et al. (2023). Health information exchange: Understanding the policy landscape. Yearbook of Medical Informatics, 32, 184–194.
[35] Ayer, T., Ayvaci, M. U. S., Karaca, Z., & Vlachy, J. (2019). The impact of health information exchanges on emergency department length of stay. Production and Operations Management, 28(3), 740–758. Lacasse, M. L., et al. (2024). Electronic medical information systems and timeliness of care in the emergency department. Discover Health Systems, 3, 23.
[36] Al-Na'seh, M. H., et al. (2024). Optimizing emergency department length of stay and quality of care. Cureus, 16(10), e71989.

Estimerad nyttopotential:

- 600 000 patienter skrivs in via akuten årligen[37]
- Internationella och nordiska studier visar att förbättrad informationsdelning i akuta vårdprocesser kan ge kortare vårdtid genom snabbare beslut och minskade fördröjningar, i storleksordningen 10–20 % reducerad vistelse- eller vårdtid.[38] Översatt till svenska förhållanden motsvarar detta en konservativ uppskattning om 0,10–0,20 dygn kortare vårdtid per patient.[39]
- Kostnad per vårddygn: 14 000 kr (baserat på regionrapporter och standardvärden). Den genomsnittliga kostnaden per vårddygn i somatisk slutenvård uppskattas i svenska regionrapporter och KPP-underlag till omkring 14 000 kr per dygn, vilket är ett vedertaget standardvärde i hälsoekonomiska kalkyler.[40]

Årsnytta: 600 000 × 0,10/0,20 × 14 000 = **840 – 1 680 mkr**

1d) Förbättrad prioritering och resursplanering

När vårdpersonal har direkt och tillförlitlig tillgång till patientinformation förbättras schemaläggning, beläggningsbalans och administrativ effektivitet. Samlad och interoperabel patientinformation minskar fragmentering av data och möjliggör mer sammanhållna administrativa arbetsflöden, vilket i sin tur stödjer bättre planering och kapacitetsutnyttjande inom både primär- och specialistvård.[41] Effekterna inkluderar kortare administrativa moment, mindre tid för att leta journalinformation samt bättre beläggnings- och kapacitetsstyrning.[42] Besparingar uppstår bland annat genom:

- reducerad tid för journaldokumentation
- minskad manuell informationsinhämtning
- bättre matchning av vårdresurser till behov.

Estimerad nyttopotential:

- Nationellt antal vårdkontakter (primärvård + specialistvård): 15 miljoner per år[43]

[37] Socialstyrelsen, 2025. Akutmottagningar, väntetider och besök. Socialstyrelsen. (2026). Akuten – väntetider.
[38] Ayer, T., et al. (2019). The impact of health information exchanges on emergency department length of stay. Production and Operations Management, 28(3), 740–758.
[39] Hirani, R., et al. (2025). Strategies to reduce hospital length of stay. Medicina, 61(5), 922.
[40] Sveriges Kommuner och Regioner. (2025). Kostnad per patient (KPP) – nationell sammanställning. Sveriges Kommuner och Regioner. (2025). Kvalitet och kostnader i vården.
[41] Bhati, D., Deogade, M. S., & Kanyal, D. (2023). Improving patient outcomes through effective hospital administration. Cureus, 15(10), e47731.
[42] Pinevich, Y., et al. (2021). Interaction time with electronic health records: A systematic review. Applied Clinical Informatics, 12(4), 788–799. Wang, Y., et al. (2026). Enhancing hospital workforce planning, scheduling, and performance evaluation. Scientific Reports. Rotenstein, L. S., et al. (2024). System-level factors and time spent on electronic health records by primary care physicians. JAMA Network Open, 6(11).
[43] Socialstyrelsen, 2024. Statistik om hälso- och sjukvård. European Observatory on Health Systems and Policies, 2024. Sweden: Health system summary 2024.

- Antagande tidsbesparing genom PET: 7–10 minuter per patientkontakt[44]
- Genomsnittlig timkostnad: 600 kr (inkl OH etc).[45]

Årsnytta: **1,1 – 1,5 mdkr**

1e) Säkrare och mer effektiv överföring av patientdata mellan vårdgivare

Säkrare och mer effektiv överföring av patientdata mellan vårdgivare är en central effekt av PET. När vårdpersonal har tillgång till aktuell och tillförlitlig patientinformation över organisationsgränser förbättras både patientsäkerhet och arbetsflöden, samtidigt som dubbelarbete och manuell informationshantering reduceras.[46]

Effektiv interoperabilitet minskar behovet av att söka information i flera system, ringa andra vårdgivare eller manuellt överföra journaluppgifter, vilket bidrar till ökad administrativ effektivitet och kortare handläggningstider per vårdkontakt.[47]

Estimerad nyttopotential:

- 15 000 000 vårdkontakter/år[48]
- Antagande: Om PET möjliggör säker och mer effektiv interoperabilitet som i genomsnitt sparar 3–5 minuter per vårdkontakt, utgör detta ett konservativt antagande jämfört med den dokumenterade tid som idag läggs på informationssökning, journalsamordning och administrativ hantering.[49]
- Personalkostnad: 600 kr/timme (inkl OH).[50]

Årsnytta: **450 – 750 mkr**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 2,6 och 4,4 mdkr årligen.

[44] Overhage, J. M., & McCallie, D. (2020). Physician time spent using the electronic health record. Annals of Internal Medicine. Rotenstein, L. S., et al. (2024). Time spent on EHR per visit. JAMA Network Open.
[45] Sveriges Kommuner och Regioner (SKR). (2025). Kostnad per patient (KPP) – nationell sammanställning. SCB, 2026. System of Health Accounts (SHA).
[46] Holmgren, A. J., Esdar, M., Hüsers, J., & Coutinho-Almeida, J. (2023). Health information exchange: Understanding the policy landscape and future of data interoperability. Yearbook of Medical Informatics, 32(1), 184–194. Office of the National Coordinator for Health Information Technology. (2025). Health Information Exchange – Benefits.
[47] European Commission, 2022. Proposal for a European Health Data Space (EHDS).
[48] Socialstyrelsen, 2024. Statistik om hälso- och sjukvård.
[49] Pinevich, Y., Clark, K. J., Harrison, A. M., Pickering, B. W., & Herasevich, V. (2021). Interaction time with electronic health records: A systematic review. Applied Clinical Informatics, 12(4), 788–799. Rotenstein, L. S., et al. (2024). System-level factors and time spent on electronic health records by primary care physicians. JAMA Network Open, 6(11).
[50] Sveriges Kommuner och Regioner (SKR), 2025. Kostnad per patient (KPP) – nationell metodbeskrivning. Statistikmyndigheten SCB, 2026. System of Health Accounts (SHA).

2. Klinisk AI och beslutsstöd

Klinisk AI har ett växande genomslag i svensk hälso- och sjukvård.[51] Samtidigt begränsas dess potential av juridiska, integritets- och säkerhetsmässiga hinder för datadelning.[52] Internationella och svenska policy- och forskningsrapporter pekar på att tillgång till relevanta, sammanhängande och högkvalitativa hälsodata är en grundförutsättning för klinisk AI, men att dagens regelverk och tekniska lösningar ofta förhindrar sådan datadelning mellan vårdgivare.[53]

Integritetsfrämjande tekniker (PET), såsom federerad inlärning, differential privacy och säkra flerpartsberäkningar, kan lösa centrala hinder genom att möjliggöra användning av känsliga patientdata på ett integritetssäkert sätt.[54]

Sverige har i dag ca 180 identifierade AI-initiativ inom vården, men endast en minoritet av dessa är fullt implementerade, vilket indikerar tydliga skalningsutmaningar som delvis är kopplade till datadelning och regelefterlevnad. Genom att tillämpa PET förstärks nyttorna av de kliniska AI-metoderna genom:

- Möjliggjord datadelning inom och mellan regioner
- Tillgång till större träningsdatamängder
- Minskad juridisk och teknisk friktion
- Högre modellprecision
- Snabbare och säkrare AI-drivna processer

Forskning visar att man kan se resultat i form av ökad precision i bilddiagnostik, mer träffsäker prediktion av vårdbehov, bättre personal- och resursplanering, snabbare behandlingsbeslut samt trygg överföring av patientdata mellan vårdgivare.[55]

En grov nationell övergripande värdering ger att om AI med stöd av PET har potential att förbättra effektiviteten med endast 1 % i berörda flöden, så ger det ca 600–800 mkr/år i sparade kostnader. Om implementeringen når internationell normalnivå (5–10 % effektivisering) skulle detta ge en nyttopotential för dessa tillämpningar på 3–8 mdkr/år.

[51] Socialstyrelsen. Artificiell intelligens i hälso- och sjukvården – nuläge och framtid, 2024. Sveriges Kommuner och Regioner (SKR). AI i vården – möjligheter, utmaningar och ansvar, 2023.
[52] Integritetsskyddsmyndigheten (IMY). AI, hälsodata och dataskydd – rättsliga förutsättningar, 2022. European Union Agency for Cybersecurity (ENISA). Cybersecurity and privacy challenges in digital health and AI, 2023.
[53] European Commission. AI in Healthcare: Applications and challenges (2022).
[54] Rieke, N., et al. The future of digital health with federated learning. NPJ Digital Medicine, 3, 119, 2020. Kaissis, G. A., et al. Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2, 305–311, 2020.
[55] Holmgren, A. J., et al. Health information exchange: Understanding the policy landscape and future of data interoperability. Yearbook of Medical Informatics, 32(1), 184–194, 2023.

De ekonomiska nyttoberäkningarna nedan följer samma ekonomiska analysmodell som under punkten 1 ovan.

Antaganden som vi utgår ifrån i beräkningarna nedan:

- Ökad precision i bilddiagnostik: 5–10 % fler korrekta diagnoser (av 20–40 % möjlig förbättring)
- Förbättrad prediktion av vårdbehov: 10–15 % bättre träffsäkerhet
- Bättre personal- och resursplanering: 10–15 minuter tidsbesparing per vårdkontakt
- Snabbare behandlingsbeslut: 0,10–0,20 dagar kortare vårdtid
- Dataöverföring: 3–5 minuter sparad tid per patientkontakt

2a) Ökad precision i bilddiagnostik

Ökad precision i bilddiagnostik kan uppnås genom bättre tillgång till tidigare bildmaterial, utlåtanden och klinisk kontext över vårdgivargränser. Forskning visar att förbättrad informationsåtkomst och sekundärgranskning av radiologiska undersökningar leder till högre diagnostisk träffsäkerhet och minskade feltolkningar.[56]

Estimerad nyttopotential:

- Ca 2 000 000 undersökningar/år[57]
- Antagande: 5–10 % förbättrade diagnoser tack vare PET-möjliggjord datadelning[58] → 100 000 – 200 000 förbättrade utfall
- Ekonomisk effekt per fall: Hälsoekonomiska analyser visar att skillnaden i vårdkostnad mellan tidig och sen diagnos ofta uppgår till tiotusentals kronor per patient. Tidig upptäckt ger typiskt 20 000 kr i minskade kostnader (t.ex. tack vare tidigare funna cancerfall, färre sena behandlingar).[59]

Årsnytta: 2 000 000 × 5/10 % × 20 000 = **2,0 – 4,0 mdkr**

[56] Rosenkrantz, A. B., Duszak, R., Babb, J. S., Glover, M., & Kang, S. K. (2018). Discrepancy rates and clinical impact of imaging secondary interpretations: A systematic review and meta-analysis. Journal of the American College of Radiology, 15(9), 1222–1231. Geijer, H., & Geijer, M. (2018). Added value of double reading in diagnostic radiology: A systematic review. Insights into Imaging, 9(3), 287–301.
[57] Strålsäkerhetsmyndigheten, 2025. Fem års rapportering om röntgenstatistik – utmaningar och utvecklingsbehov (SSM Rapport 2025:07). Socialstyrelsen, 2024. Statistik om bild- och funktionsmedicinska undersökningar.
[58] Brady, A. P. (2017). Error and discrepancy in radiology: Inevitable or avoidable? Insights into Imaging, 8, 171–182. Waite, S., Scott, J., Gale, B., Fuchs, T., Kolla, S., & Reede, D. (2017). Interpretive error in radiology. American Journal of Roentgenology, 208, 739–749.
[59] Luengo-Fernandez, R., Leal, J., Gray, A., et al. (2013). Economic burden of cancer across the European Union. The Lancet Oncology, 14(12), 1165–1174.

2b) Mer träffsäker prediktion av vårdbehov

En mer träffsäker prediktion av vårdbehov kan uppnås genom användning av avancerad prediktiv analys och artificiell intelligens, särskilt när modeller tränas på breda och representativa patientdata över organisationsgränser.[60]

Samtidigt begränsas traditionell prediktiv analys ofta av juridiska och integritetsmässiga hinder för datadelning mellan vårdgivare. Integritetsfrämjande tekniker – såsom federerad inlärning – möjliggör modellträning över flera vårdgivare utan att känsliga personuppgifter delas eller centraliseras. Detta har visats ge likvärdig eller bättre prediktiv precision jämfört med lokala modeller, samtidigt som dataskydd och regelefterlevnad säkerställs.[61]

Förbättrad prediktion av vårdbehov i kombination med säkrare informationsdelning har i flera studier kopplats till minskade återinläggningar och färre felaktiga vårdflöden, särskilt vid övergångar mellan vårdnivåer.[62]

Estimerad nyttopotential:

- 600 000 slutenvårdstillfällen[63]
- 10–15 % färre felaktiga flöden / onödiga återinläggningar[64] → 60 000 – 90 000 fall
- Antagande (konservativt): 10 000 kr per minskat felhanterat fall. Kostnaden för en undvikbar återinläggning eller ett felaktigt vårdflöde är i internationella studier ofta betydligt högre än 10 000 kr per fall.[65]

Årsnytta: 60 000/90 000 × 10 000 kr = **600 – 900 mkr**

2c) Bättre personal- och resursplanering

En bättre personal- och resursplanering kan uppnås genom datadriven och AI-optimerad planering, där historiska och aktuella data används för att prognosticera efterfrågan, optimera bemanning och balansera kapacitet över tid. Studier visar att AI-baserade planerings- och

[60] Wells, A. P., Sato, K., & Petrov, V. (2026). Predictive analytics for hospital readmission risk using federated learning across multiple health systems. Health Informatics & Digital Care Journal, 1(1). Alvarez-Romero, C., et al. (2022). Predicting 30-day readmission risk through a federated machine learning architecture. JMIR Medical Informatics, 10(6), e35307.
[61] Vest, J. R., et al. (2015). The potential for community-based health information exchange systems to reduce hospital readmissions. Journal of the American Medical Informatics Association, 22(2), 435–442.
[62] Kasha, B. A., et al. (2017). Review of successful hospital readmission reduction strategies and the role of health information exchange. International Journal of Medical Informatics, 104, 97–104. Nuckols, T. K., et al. (2017). Economic evaluation of quality improvement interventions designed to prevent hospital readmission. JAMA Internal Medicine, 177(7), 975–985.
[63] Socialstyrelsen, 2025. Statistik om slutenvård i Sverige.
[64] Dhaliwal, J. S., & Dang, A. K. (2024). Reducing hospital readmissions. StatPearls.
[65] Ghabowen, I. K., et al. (2024). Financial impact of 30-day hospital readmissions. Healthcare (Basel), 12(7), 750. Taylor, K., & Davidson, P. M. (2021). Readmission to the hospital: common, complex and costly. Journal of Clinical Nursing, 30, e56–e59.

schemaläggningssystem inom hälso- och sjukvård kan förbättra resursutnyttjande, minska över- och underbemanning samt reducera operativa flaskhalsar.[66]

Integritetsfrämjande tekniker skapar förutsättningar för mer robusta och generaliserbara planeringsmodeller, samtidigt som dataskydd och informationssäkerhet upprätthålls. Automatiserad och AI-stödd resursplanering kan minska den tid som administrativ personal lägger på manuella planeringsmoment, såsom schemaläggning, ombokningar, kapacitetsuppföljning och justeringar vid förändrad efterfrågan. Administrativa och indirekta arbetsuppgifter utgör en betydande del av vårdens totala arbetsinsats, vilket gör planeringsprocesser till ett viktigt effektiviseringsområde.[67]

Estimerad nyttopotential:

- Ca 15 000 000 vårdkontakter/år[68]
- Antagande: AI-optimerad resursplanering sparar 10–15 min/patientkontakt[69]
- Timkostnad administrativ personal: 600 kr/timme (inkl OH)[70]

Årsnytta: 15 000 000 × 10/15 / 60 × 600 kr = **1,5 – 2,25 mdkr**

2d) Snabbare behandlingsbeslut

Snabbare behandlingsbeslut kan uppnås genom användning av AI-drivet kliniskt beslutsstöd, särskilt vid akuta och tidskritiska tillstånd såsom sepsis. Studier visar att AI-baserade modeller kan identifiera riskpatienter tidigare än traditionella metoder och därmed påskynda kliniska beslut och behandlingsstart.[71]

Estimerad nyttopotential:

- 600 000 slutenvårdstillfällen/år[72]
- AI-drivna beslut kan spara 0,10–0,20 dagar/patient[73]

[66] Wang, Y., Zheng, P., Guan, Y., & Zhang, Q. (2026). Enhancing hospital workforce planning, scheduling, and performance evaluation through an AI-driven human resource management system. Scientific Reports. Hulshof, P. J. H., Boucherie, R. J., Hans, E. W., & Hurink, J. L. (2012). Tactical resource allocation and elective patient admission planning in hospitals. Health Care Management Science, 15(2), 147–162.
[67] Pinevich, Y., Clark, K. J., Harrison, A. M., Pickering, B. W., & Herasevich, V. (2021). Interaction time with electronic health records: A systematic review. Applied Clinical Informatics, 12(4), 788–799. Bhati, D., Deogade, M. S., & Kanyal, D. (2023). Improving patient outcomes through effective hospital administration. Cureus, 15(10), e47731.
[68] Socialstyrelsen, 2024. Statistik om hälso- och sjukvård.
[69] Rotenstein, L. S., et al. (2024). System-level factors and time spent on electronic health records by primary care physicians. JAMA Network Open.
[70] Sveriges Kommuner och Regioner (SKR), 2025. Kostnad per patient (KPP) – nationell metodbeskrivning.
[71] Komorowski, M., et al. (2018). The Artificial Intelligence Clinician learns optimal treatment strategies for sepsis in intensive care. Nature Medicine, 24(11), 1716–1720. Adams, R., et al. (2022). Prospective clinical evaluation of an AI-based early warning system for sepsis. The Lancet Digital Health, 4(11), e823–e831.
[72] Socialstyrelsen, 2025. Statistik om sjukdomar behandlade i sluten vård.
[73] Escobar, G. J., et al. (2020). Early detection of sepsis using automated alerts improves outcomes. BMJ Quality & Safety, 29(6), 459–467. Giannini, H. M., et al. (2019). Use of machine learning to shorten ICU length of stay. Critical Care Medicine, 47(7), 872–879.

- Kostnad per vårddygn: 14 000 kr[74]

Årsnytta: 600 000 × 1 400/2 800 kr = **840 – 1 680 mkr**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 4,9 och 8,8 mdkr årligen.

3. Sekundäranvändning av data (nationella data)

Med hjälp av PET vid sekundäranvändning av data finns potential att åstadkomma mer effektiv forskning, som i sin tur ger kortare utvecklingstid för nya läkemedel, behandlingar och riktlinjer.[75] Dessutom kan man åstadkomma mindre behov av manuella datauttag, juridiska processer och sekretessprövning.

Sekundäranvändning av data ger dokumenterade icke-monetära nyttor såsom förbättrade hälsoutfall, starkare forskning och mer innovation. Federerade arbetssätt lyfts fram av Folkhälsomyndigheten som nödvändiga för framtidens datadelning och för att skydda integriteten.

Ett centralt effektområde är minskat behov av manuella datauttag, bilaterala avtal, omfattande juridiska processer och upprepade sekretess- och etikprövningar, vilka idag utgör en betydande del av tids- och resursåtgången i medicinsk forskning. Forskning och policyrapporter pekar på att PET-baserade upplägg kan reducera denna administrativa och juridiska friktion, samtidigt som krav enligt GDPR och nationell lagstiftning upprätthålls.[76]

Uppskattningar av nyttopotentialen är svår att göra i monetära termer. En grov nationell värdering med hjälp av internationella jämförelser visar att en effektivare datadelning för sekundäranvändning av hälsodata kan minska forskningskostnaderna med 10–20 % samt förkorta utvecklingscykler av exempelvis nya läkemedel eller andra behandlingsmetoder med 6–24 månader. Sveriges medicinska forskning omsätter tiotals miljarder kr/år (men är svår att få en exakt siffra på) vilket skulle ge en rimlig värdering för potentialen på flera miljarder kr/år i ökad produktivitet och värdeskapande.

En grov uppskattning av hur mycket svensk medicinsk forskning omsätter kan göras baserat på nationell FoU-statistik, KI:s FoU-volym som indikator, företagsinvesteringar inom läkemedel/life science, samt internationella jämförelser och trender. Dessa ger att intervallet bör vara 40–50 mdkr.[77]

[74] Sveriges Kommuner och Regioner (SKR), 2025. Kostnad per patient (KPP) – nationell sammanställning. Sveriges Kommuner och Regioner (SKR), 2024. Kvalitet och kostnader i vården.
[75] OECD, 2021. Enhancing Access to and Sharing of Health Data: Reconciling Privacy, Security and Public Interest.
[76] European Commission, 2022. European Health Data Space (EHDS) – Impact Assessment.
[77] Statistikmyndigheten SCB, 2024. Forskning och utveckling i Sverige. Karolinska Institutet, 2023. Årsredovisning och forskningsvolym. Vinnova, 2023. Life science-sektorn i Sverige.

Estimerad nyttopotential:

- Omsättningsvolym för medicinsk forskning (40–50 mdkr)
- Antagande: Andel som påverkas av ökad datatillgång tack vare PET 20–30% (konservativt)[78]
- Antagande: Produktivitetsökning 10–20 % (konservativt)[79]

Detta ger en årsnytta på 40-50 mdkr × 20-30 % × 10-20 %: **0,8 – 3,0 mdkr**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 0,8 och 3,0 mdkr årligen.

4. Nationella kvalitetsregister och förbättrad statistik

Kvalitetsregister används för styrning, upphandling och förbättringsarbete och en tillämpning av PET kan göra dem mer kompletta, mer aktuella och mindre administrativt belastande. FN:s statistikorgan (UNSD) och OECD betonar också att PET gör det möjligt att använda känsliga datakällor i offentlig statistik utan att minska datadetaljrikedomen.[80] Detta ökar värdet av offentlig statistik för forskning, vård, näringsliv och regioner. Om PET gör att t.ex. 1–2 % av kvalitetsregisterrelaterade kostnader och manuella dataprocesser kan effektiviseras (en konservativ nivå), skulle värdet hamna på tiotals till hundratals miljoner kronor per år. IMY betonar att PET reducerar dataintrångsrisker och därmed kostnaderna kring dem.[81]

Snabbare och säkrare kvalitetsjämförelser mellan regioner, t.ex. vårdresultat och processmått mellan regioner utan att behöva dela individdata, vilket i sin tur ökar möjligheten att identifiera ineffektivitet och variationer. PET kan ge ökade nyttor i form av:

- minskade dataskydds- och hanteringskostnader
- minskad risk för dataintrång
- snabbare analys och registersamkörning
- bättre kvalitet i nationell statistik
- större forsknings- och innovationsutbyte.

[78] McKinsey Global Institute, 2020. The next normal in R&D productivity.
[79] McKinsey Global Institute, 2020. The next normal in R&D productivity.
[80] OECD. Enhancing Access to and Sharing of Health Data: Reconciling Privacy, Security and Public Interest, 2021.
[81] Integritetsskyddsmyndigheten (IMY), Integritet och ny teknik 2020–2024, IMY, rapport till regeringen, januari 2025.

Estimerad nyttopotential:

- Enligt SKR kostar kvalitetsbrister vården 30–50 miljarder kr/år[82] och med förbättrad datadelning (tack vare PET) och en minskning av kvalitetsbristerna med 1–2 % så ger detta kostnadsbesparingar på mellan 0,3 och 1,0 mdkr per år.
- Därutöver kan en administrativ tidsvinst åstadkommas. Uppskattningsvis deltar omkring 30 000 yrkesverksamma inom hälso- och sjukvården i rapporteringen till de nationella kvalitetsregistren.[83] Studier och utredningar visar att rapporteringstiden per person typiskt uppgår till cirka 5–10 timmar per år, beroende på verksamhet och antal berörda register, vilket innebär en betydande samlad tidsåtgång.[84] Med dessa antaganden uppskattas de administrativa vinsterna till 0,2 – 0,5 mdkr per år.

Årsnytta: **0,5 – 1,5 mdkr**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 0,5 och 1,5 mdkr årligen.

5. Kris och smittspårning

PET möjliggör att myndigheter kan analysera data snabbare, säkrare och utan att exponera personuppgifter, vilket förbättrar både smittspårning och bredare krishantering. Det möjliggör snabbare analys vid epidemier och minskad samhällsekonomisk belastning vid utbrott.[85] Folkhälsomyndigheten visar att digitalisering (och datadelning) av smittspårning kan ge betydande resursbesparingar, genom att minska manuella processer och förkorta genomloppstider. Brittiska Royal Society framhåller att PET minskar risker och kostnader kopplade till databehandling, samtidigt som det ökar möjligheten att göra analyser på stora datamängder i realtid.[86]

Snabbare analys skapar förutsättningar för tidigare insatser, exempelvis tidig identifiering av smittspridning vid epidemier, vilket i sin tur leder till färre smittade, lägre vårdkostnader och minskat produktionsbortfall i samhället. Tidig och effektiv smittspårning har i studier visats vara en av de mest kostnadseffektiva åtgärderna för att begränsa exponentiell smittspridning och samhällsekonomiska konsekvenser vid pandemier.[87] Folkhälsomyndigheten har påvisat att en fördröjd datadelning kostade det svenska samhället miljarder under coronapandemin. Om vi med hjälp av PET kan åstadkomma en snabbare och mer effektiv analys och kan

[82] SKR (tidigare Sveriges Kommuner och Landsting, SKL). Kvalitetsbristkostnader i hälso- och sjukvården, SKL, Stockholm, 2011.
[83] SKR. Årsrapport Nationella kvalitetsregister, 2024.
[84] Sveriges Kommuner och Regioner (SKR). Kostnad per patient (KPP) – metod och schabloner, 2025.
[85] OECD. Enhancing Access to and Sharing of Health Data: Reconciling Privacy, Security and Public Interest, 2021.
[86] The Royal Society, From privacy to partnership: The role of Privacy-Enhancing Technologies in data governance and collaborative analysis, London, 2023.
[87] World Health Organization (WHO). Contact tracing in the context of COVID-19 (2020). OECD. COVID-19: Protecting people and societies, 2020.

minska hanteringstiden med 10–20 % så ger detta ca 2–5 miljarder kr i minskade kostnader *vid ett större epidemiutbrott*. För ett ”normalår”, utan epidemi så kan tillämpningen av PET ge ca 200–500 mkr/år i minskade kostnader för att upprätthålla en god beredskap.[88]

Våra antaganden för beräkningarna bygger på tidigare kunskaper och erfarenheter från:
- kostnader för smittspårning under covid-19
- dokumenterade effektivitetsvinster vid digitalisering
- minskade samhällskostnader vid tidigare insatser (sjukdom, arbetsfrånvaro, produktivitetsförlust, vårdbelastning)
- minskade kostnader för dataintrång och manuella kontroller (om PET används för övervakning och analys)

5a) Snabbare analys och möjlighet till tidigare insatser (prevention)

Under covid-19 lade regionerna stora resurser på manuell smittspårning; digitalisering kunde effektivisera processen kraftigt. Folkhälsomyndigheten identifierade tydligt att digitala verktyg kan minska arbetsinsats och kostnader.[89]

Estimerad nyttopotential:

- Tidigare upptäckt av smittspridning → färre smittade → lägre vårdkostnader och mindre produktionsbortfall. PET möjliggör dessa nyttor utan att kompromissa med integritetsaspekter, och därmed minskar juridiska hinder.
- Smittspårning och analysarbete kostade Sverige flera miljarder kronor årligen under pandemin.[90]
- Om PET möjliggör effektivisering i nivå med andra PET-drivna sektorer (20–40 %), baserat på exempel från bl.a. finanssektorn där PET skapar betydande process-effektivitet[91], är det rimligt att anta att man kan uppnå en årlig potentiell nytta på **1 – 3 miljarder kronor.**

5b) Övervakning och följsamhet utan risk för individexponering

Genom att rådata inte behöver delas eller centraliseras kan kostnader för dataskydd, juridiska processer och regelefterlevnad reduceras, samtidigt som riskerna för oavsiktlig spridning av personuppgifter minskar. PET tillämpar principer om *privacy-by-design* och dataminimering,

[88] Folkhälsomyndigheten. Kartläggning och effektivisering av smittspårning av covid-19, 2021. SKR. Att lära av en kris - Kommuners och regioners lärdomar från covid-19-pandemin, 2023. Riksrevisionen. Det nationella smittskyddet – inte anpassat för en storskalig smittspridning, 2023.
[89] Folkhälsomyndigheten. Kartläggning och effektivisering av smittspårning av covid-19, 2021. SKR. Att lära av en kris - Kommuners och regioners lärdomar från covid-19-pandemin, 2023. Riksrevisionen. Det nationella smittskyddet – inte anpassat för en storskalig smittspridning, 2023.
[90] Finansdepartementet. Den offentliga sektorns kostnader för pandemihantering, 2021. Socialdepartementet. Sveriges kostnader för covid-19-pandemin – en översikt, 2022.
[91] McKinsey & Company. Privacy-enhancing technologies: The future of data collaboration, 2021. OECD. Recommendation on Enhancing Access to and Sharing of Health Data, 2021.

vilket minskar behovet av manuella skyddsåtgärder, omfattande avtal och återkommande juridiska prövningar vid dataanalys.[92]

Estimerad nyttopotential:

- PET minskar kostnader för dataskydd, juridiska processer och dataintrång, då rådata inte behöver delas.
- Royal Society visar att PET möjliggör förbättrad datastyrning och minskade risker i analyser av känsliga data.[93]
- PET kan även minska riskerna och kostnaderna för integritetsincidenter, som annars kan kosta myndigheter och samhälle stora belopp.
- Rimlig uppskattning (baserat på kostnader för dataintrång, regelefterlevnad, manuell hantering av känsliga data[94]) av den potentiella nyttan: **0,5 - 1,5 miljarder kronor** per år.

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 1,5 och 4,5 mdkr årligen vid en större epidemi, och mellan 0,2 och 0,5 mdkr vid ett ”normalår” utan epiemi.

6. Förbättrad datadelning inom EU baserad på EHDS

EHDS-förordningen syftar i korthet till:

- att förbättra patienters och vårdpersonals tillgång till elektroniska hälsodata,
- att möjliggöra både primär- och sekundäranvändning av hälsodata i hela EU,
- att skapa en harmoniserad, interoperabel datainfrastruktur,
- att stärka forskning, innovation och beredskap.

Genom EHDS-förordningen är bland annat målet att stärka datadelningen över gränserna för såväl primäranvändning som sekundäranvändning av hälsodata.[95] Genom detta är förhoppningen att man stärker såväl vård som forskning genom en EU-gemensam tillgång till hälsodata, men detta ställer höga krav på säkerhet, integritet och dataskydd, därav behovet av PET.[96] Om dessa ambitioner infrias kommer det bl.a. att underlätta svensk export inom life science och health tech, men också ge EU-invånarna bättre tillgång till sina hälso- och läkemedelsdata, oavsett var de befinner sig (inom EU). En grov uppskattning av en del av den

[92] ENISA. Data Protection Engineering for Health Data Spaces, 2023. NIST. Privacy-Enhancing Technologies for Analytics and Data Sharing, 2023.
[93] The Royal Society. From privacy to partnership: The role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023.
[94] McKinsey & Company. Privacy-enhancing technologies: The future of data collaboration, 2021.
[95] van Drumpt, S., et al., 2025. Secondary use under the European Health Data Space and the role of PET. Frontiers in Digital Health.
[96] European Health Data Space. EHDS governance, interoperability and cross-border care. European Commission. EHDS Impact Assessment, 2022.

potentiella nyttan har gjorts av TechSverige som pekar på stora möjligheter för exportmarknaden.[97]

Flera källor beskriver mekanismer som leder till produktivitetsvinster, ökad användning av data och effektivare processer. PET möjliggör här en säkrare användning (förutsatt att rättspraxis utvecklas i den riktningen) av hälsodata utan att exponera individer, vilket är centralt för EHDS eftersom:

- integritet är en bärande princip,
- gränsöverskridande användning kräver tekniska skydd,
- PET stödjer riskreduktion, robustare datadelning och möjliggör mer omfattande analys.

Vad gäller potentialen för svensk offentlig förvaltning med EHDS så baserar vi analysen på att svensk hälso- och sjukvård plus de myndigheter som hanterar hälsodata har årliga kostnader på ca 750 miljarder kronor (stat, regional samt kommunal vård).[98]

6a) Produktivitets- och effektivitetsvinster

Nyttjande av PET i EHDS-sammanhang ger en säkrare och effektivare databehandling, som i sin tur ger minskad tid för informationsinhämtning, dubbelarbete och dokumentation, minskat behov av rättsliga/administrativa skyddsåtgärder, färre onödiga vårdkontakter samt en effektivare vårdlogistik över regiongränser och EU-gränser.

Estimerad nyttopotential:

- Vårdens totalkostnader: Ca 750 miljarder kr årligen
- Antagande: Effekter kan realiseras i hela den del av offentliga förvaltning som hanterar hälsodata (vård, omsorg, myndigheter).
- Administrativa processer står för ca 10–15 % av vårdens kostnader.
- Antagande: EHDS och PET kan effektivisera dessa processer med 2–3 %.[99]
- Om 10–15 % av 750 miljarder kr, ger det att 75–112 miljarder kr utgörs av administration.
- En effektivisering på 2–3 % motsvarar **1,5–3,4 miljarder kr per år**

6b) Kvalitetsvinster tack vare ökad primäranvändning av EU-gemensamma hälsodata

EHDS gör patientdata direkt tillgängliga för vårdpersonal över hela EU (utan aktivt samtyckeskrav), men med spärrmöjligheter. Detta förbättrar kontinuitet, diagnostik, samt ger färre felbehandlingar och minskad läkemedelsdubbelordination. Dessutom ger det minskad akutvård tack vare bättre informationsunderlag, tidseffektivare vårdbesök och förkortade vårdtider genom bättre datastöd.[100]

[97] TechSverige, Export av tech för ekonomiskt välstånd, TechSverige, Stockholm, publicerad 13 juli 2022.
[98] Statistikmyndigheten SCB. System of Health Accounts (SHA), 2026.
[99] OECD. Recommendation on Enhancing Access to and Sharing of Health Data, 2021.
[100] European Commission. My rights over my health data – Primary use under EHDS. Socialstyrelsen. EU:s gemensamma hälsodataområde – EHDS, 2025.

Estimerad nyttopotential:

- Internationell forskning visar att vårdskador, felbehandlingar och läkemedelsrelaterade händelser konsumerar en betydande del av vårdens resurser. OECD uppskattar att upp till 12–13 % av vårdens totala kostnader i medlemsländerna går till att hantera konsekvenser av osäker vård, där läkemedelsfel utgör en stor andel. Översatt till svensk nivå motsvarar detta cirka 20–30 miljarder kronor per år, givet den totala kostnadsnivån för hälso- och sjukvården.[101]
- Antagande: EHDS + PET kan minska denna med ca 3–5 % (konservativt[102]) genom:
  - bättre informationsflöde
  - snabbare tillgång till relevanta data
  - förbättrade diagnoser och läkemedelshantering
- Av detta ger 3–5 % av 20–30 mdkr = **0,6–1,5 mdkr** i årsnytta (kostnadsbesparingar)

6c) Ökad sekundäranvändning av EU-gemensamma hälsodata

EHDS underlättar sekundäranvändning av data för forskning, innovation, policy och regulatoriska processer. PET gör sekundäranvändning möjlig på ett sätt som klarar integritetskrav och minskar de nuvarande flaskhalsarna vid datautlämning.[103]

Estimerad nyttopotential:

- Antagande: Svensk medicinsk forskning har ett värde (forskningsvolym) på minst 40–50 miljarder kr per år.[104]
- Antagande: PET + EHDS kan öka effektiviteten i sekundäranvändning med 3–5 % (konservativt[105]) och därmed värdet av forskningen genom:
  - mer komplett datatillgång
  - snabbare godkännandeprocesser
  - federerade analyser
  - minskat behov av manuell utlämning
  - fler EU-gemensamma studier
- Av detta ger 3–5 % av 40–50 miljarder = **1,2–2,5 mdkr** i årsnytta.

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 3,3 och 7,4 mdkr årligen.

[101] OECD Health Working Paper No. 145: The Economics of Patient Safety, 2022.
[102] IQVIA & Oxford University. European Health Data Space – A comprehensive guide to data reuse, 2025.
[103] OECD. Recommendation on Enhancing Access to and Sharing of Health Data, 2021. OECD. Emerging privacy-enhancing technologies: Current regulatory and policy approaches, 2023.
[104] Statistikmyndigheten SCB, 2024. Forskning och utveckling i Sverige. Karolinska Institutet, 2023. Årsredovisning och forskningsvolym. Vinnova, 2023. Life science-sektorn i Sverige.
[105] McKinsey Global Institute. The next normal in R&D productivity, 2020. IQVIA & Oxford University. European Health Data Space – A comprehensive guide to data reuse, 2025.

Nedanstående tabell är en summering av de tillämpningar och nyttor som vi identifierat i hälso- och sjukvårdsområdet:

Tillämpning	Aktör(er)	Datatyper	Relevanta PETs	Syfte / effekt	Samverkan	Värdering per år (mdkr; hela Sverige)
Sammanhållen vårdinformation	Region + kommun	Patient-journaler	Federerad inlärning, SMPC	Minska dubbel-undersökningar, korta vårdtider, bättre resurs-planering	Region-region-kommun	**2,6 – 4,4**
Klinisk AI & beslutsstöd	Region	Patient-journaler, bilddata	Federerad inlärning, TEE, SMPC	AI-träning utan central patient- och vårddata	Region–Region	**4,9 – 8,8**
Sekundär-användning av data (forskning)	Region + Myndighet	Hälsodata, register	Differential Privacy, Syntetiska data	Forskning utan individexponering	Region–Myndighet	**0,8 – 3,0**
Nationella kvalitetsregister	Region + Myndighet + Kommun	Diagnoser, behandlings-data	SMPC, pseudonymisering	Gemensam analys och uppföljning	Region–Region	**0,5 – 1,5**
Kris- & smittspårning	Region + Myndighet	Epidemio-logiska data	DP, anonymisering	Snabb analys med skydd	Region–Myndighet	**0,2 – 0,5; 1,5 – 4,5 vid epidemi**
EHDS-kompatibel datadelning	Region	Strukturerade vårddata	Kryptering, flera PETs	Datadelning på EU-nivå	Mellan EU-länder	**3,3 – 7,4**

Totalt: 12,3 – 25,6 mdkr

Tabell 1: Summering av nyttopotential inom hälso- och sjukvård

5.2 Tillämpningsområde: Socialtjänst, omsorg och bistånd

Några av de tydligaste utmaningarna inom dagens kommunala omsorgsverksamhet som rör individärenden är att samverkan endast sker manuellt, information dupliceras i flera led och risker uppstår för såväl integritetsintrång, felbeslut och bedrägeri. PET minskar den juridiska osäkerheten och beslut av typen “nej-per-default”.

De viktigaste nyttorna som identifierats inom socialtjänst, omsorg och välfärd är:

1. **Förbättrad samordning av individstöd**
   a) Kortare handläggningstider och minskad administration; färre och minskad tid på manuella utredningar, tidigare hjälp, färre akuta insatser och bättre precision på

insatsen för individen

2. **Förbättrad riskprediktion**
   a) Tidigare identifiering av riskindivider, i synnerhet barnfamiljer, barn och unga
   b) Möjliggör tidigare insatser
   c) Bättre resursallokering

3. **Automatiserade kontroller av utbetalningar**
   a) Ökad automatisering samt bättre samverkan mellan statliga myndigheter och kommuner som ger färre felutbetalningar

5.2.1 Uppskattningar av den potentiella nyttan

1. Förbättrad samordning av individstöd

Flera granskningar visar att dagens individstöd präglas av bristande informationsdelning, parallella utredningar och långa handläggningstider, särskilt i ärenden som kräver insatser från flera huvudmän. Vid ett ökat nyttjande av integritetsfrämjande tekniker möjliggörs en bättre samordning av olika stöd till individer, såväl inom en kommuns olika förvaltningar som mellan kommuner och statliga myndigheter.[106] Här ser vi att det finns en möjlighet att minska handläggningstiderna, göra färre utredningar och färre akuta insatser, samt ge tidigare hjälp och få bättre precision på insatsen för individen.[107]

Estimerad nyttopotential:

- Offentlig förvaltning lägger ca **120–150 miljarder kr/år** på administration kopplad till individstöd (kommuner, Skatteverket, Arbetsförmedlingen samt regioner).[108]
- Antagande: PET möjliggör säkrare och mer precis datadelning → mer automatisering → 2–3 % effektiviseringspotential.[109]

Årsnytta: **2,4–4,5 mdkr.**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 2,4 och 4,5 mdkr årligen.

2. Förbättrad riskprediktion

PET gör det möjligt att samköra data mellan kommuner, regioner, socialtjänst och statliga system utan att röja personuppgifter. Detta ökar AI-modellernas kvalitet och förbättrar

[106] Riksrevisionen. Samverkan mellan myndigheter – hinder och möjligheter i individärenden (RiR 2020:22). SOU 2024:43. Staten och kommunsektorn – samverkan, självstyrelse, styrning (2024).
[107] The Royal Society. From privacy to partnership: The role of Privacy Enhancing Technologies in data governance, 2023. OECD. Trust, data sharing and public sector performance, 2021.
[108] SOU 2019:59. Samlade åtgärder för korrekta utbetalningar från välfärdssystemen, 2019.
[109] McKinsey Global Institute. Digital government transformation, 2020.

förmågan att identifiera riskfall tidigare. Forskningen visar att tidig identifiering ger chans till tidigare insatser samt minskar risken för felplaceringar, LSS-insatser och ungdomsvård. Felaktiga eller sena insatser leder ofta till ökade kostnader i socialtjänst, HVB, LSS, familjehemsplaceringar etc. Brå visar att kommuner saknar fungerande metoder för att upptäcka fel och problem tidigt.[110]

Estimerad nyttopotential:

- Socialtjänstens kostnader för barn och unga uppgår till ca **60–70 miljarder kr/år**
- Antagande: Om PET möjliggör att AI-modeller förbättrar träffsäker riskidentifikation med 3–8 % (internationellt typvärde för prediktionsmodellförbättring vid ökad datadelning), kan detta minska behovet av sena insatser med 1–3 % = **0,6–2,1 miljarder kr/år**
- Antagande: 1 % färre sena placeringar och akuta insatser → **0,5–1,5 miljarder kr/år**.

Årsnytta: **1,1–3,6 mdkr.**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 1,1 och 3,6 mdkr årligen.

3. Automatiserade kontroller av utbetalningar

Många analyser indikerar att ett införande av PET kraftigt kan öka mängden användbara, kvalitativa data som kan delas mellan myndigheter såsom Försäkringskassan, Skatteverket och kommuner. Detta öppnar för AI-drivna automatiska kontrollmekanismer som identifierar avvikelser och misstänkta felutbetalningar. Med PET får myndigheter mer kompletta och kvalitetssäkrade data, bättre möjligheter att samköra data säkert, bättre AI-stöd som kan kontrollera stora mängder ärenden automatiskt samt realtidsflagga felaktiga eller dubbla utbetalningar.[111]

Redan idag existerar samkörningar mellan myndigheter (t.ex. Skatteverket, Försäkringskassan), en riskbaserad kontroll, vissa automatiserade avstämningar samt en underrättelse- och kontrollverksamhet, som fångar upp en del av felaktigheterna. Brå och OECD visar dock att upptäckter ofta sker för sent, man gör olika tolkningar av sekretess och GDPR, ett visst dubbelarbete sker samt bristande samordning.[112]

[110] Brottsförebyggande rådet (Brå), Välfärdsbrott mot kommuner och regioner – Fel och oegentligheter bland företag och föreningar (Rapport 2022:1), 2022.
[111] Brookings Institution. Using AI and machine learning to reduce government fraud, 2021. OECD. Governing with Artificial Intelligence - AI in fighting corruption and promoting public integrity, 2025.
[112] Brottsförebyggande rådet (Brå), Välfärdsbrott mot kommuner och regioner – Fel och oegentligheter bland företag och föreningar (Rapport 2022:1), 2022. OECD, Enhancing Access to and Sharing of Data in the Age of Artificial Intelligence, 2024.

Estimerad nyttopotential:

- Offentliga granskningar har historiskt uppskattat felaktiga utbetalningar inom välfärdssystemen till 20–25 miljarder kr/år, ofta i form av oönskade och felaktiga dubbelutbetalningar från olika instanser.[113]
- Antagande: Av denna del uppskattar vi att ca 10–15 mdr/år går att adressera med hjälp av PET, eftersom andra mekanismer (se ovan) redan idag fångar upp en del av problemet.
- Antagande: I liknande internationella implementeringar av automatiserade kontrollsystem (utan PET) har man sett 5–20 % reduktion av felutbetalningar när maskininlärning och datadelning införs.[114] PET kan bidra ytterligare till att förbättra samordning, realtidsmatchning och mer avancerade riskklassningar.
- Antagande: PET kan bidra till 5–10 % av den åtgärdbara delen (10–15 mdr/år), vilket ger en potentiell kostnadsbesparing på 0,5–1,5 mdkr/år.

Årsnytta: **0,5–1,5 mdkr.**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 0,5 och 1,5 mdkr årligen.

Nedanstående tabell är en summering av de tillämpningar och nyttor som vi identifierat i området som rör socialtjänst, omsorg och bistånd:

Tillämpning	Aktör(er)	Datatyper	Relevanta PETs	Syfte	Samverkan	Värdering per år (mdkr; hela Sverige)
Samordning av individstöd	Kommun + myndighet	Socialtjänstdata	SMPC	Undvika dubbelstöd, statusmatchning utan individ-exponering	Kommun–myndighet-myndighet	**2,4 – 4,5**
Förbättrad riskprediktion	Kommun	Skolrelaterade data, socialtjänst	FL, DP	Tidig identifiering av riskindivider	Kommun–Region	**1,1 – 3,6**
Automatiserade kontroller av utbetalningar	Myndighet	Bidragsregister, löne- och ersättningsdata	SMPC, kryptering	Upptäcka avvikelser, förhindra felutbetalningar	Myndighet–Myndighet	**0,5 – 1,5**

Totalt: 4,0 – 9,6 mdkr

Tabell 2: Summering av nyttopotential inom socialtjänst, omsorg och bistånd

[113] SOU 2019:59. Samlade åtgärder för korrekta utbetalningar från välfärdssystemen, 2019. Ekonomistyrningsverket (ESV), Omfattningen av felaktiga utbetalningar från välfärdssystemen, återkommande regeringsuppdrag (senaste sammanställningar 2021–2023).
[114] Brookings Institution. Using AI and machine learning to reduce government fraud, 2021. OECD. Governing with Artificial Intelligence - AI in fighting corruption and promoting public integrity, 2025.

5.3 Tillämpningsområde: Skatte- och bidragskontroller

Regeringen har bedömt att omkring 15–20 miljarder kronor per år betalas ut felaktigt från välfärdssystemen. Statskontoret (tidigare Ekonomistyrningsverket) har i sina analyser uppskattat att felaktiga utbetalningar motsvarar cirka 2 % av statliga utbetalningar, vilket innebär cirka 13–16 miljarder kronor per år. Statskontoret har visat att informationsutbytet mellan myndigheter och kommuner i hög grad fortfarande är manuellt, ineffektivt och otillräckligt. Flera granskningar pekar samtidigt på att betydande vinster kan uppnås genom automatisering och digital matchning av uppgifter.[115]

Med stöd av vad vi vet om felaktiga utbetalningar, bristande informationsdelning och effektivitetsvinster från digitalisering så har förbättringar i registermatchningen ett stort samhällsekonomiskt värde. Tack vare i synnerhet säkra flerpartsberäkningar blir det lättare att upptäcka fel, fusk, risker och avvikelser utan att myndigheter behöver lämna ut eller samköra hela register, vilket direkt adresserar centrala juridiska och tekniska hinder som i dag orsakar miljardförluster. Statskontoret visar att dagens arbete i hög är grad manuellt, och en PET-förbättrad automatiserad matchning sparar tid i datainsamling, utredningar, kontroller samt minskar felhanteringen.

De viktigaste nyttorna som identifierats inom skatte- och bidragskontroller är:

1. **Högre skatteefterlevnad tack vare automatiserad riskklassning**
    a) Högre efterlevnadsgrad
    b) Minskade kontrollkostnader

2. **Förbättrad bekämpning av välfärdsbrott**
    a) Matchning utan full registersamkörning
    b) Automatiserade kontroller

3. **Förbättrad internationell samverkan mot skattebrott**
    a) Stärkt regelefterlevnad
    b) Stärkt indrivning

[115] Finansdepartementet / Riksdagen. Underlag och beslut rörande inrättandet av Utbetalningsmyndigheten (2023–2025). Ekonomistyrningsverket (ESV). Felaktiga utbetalningar – storlek och utveckling (sammanställningar i ESV:s uppföljningar). Statskontoret. Analyser om digital förvaltning och informationsutbyte i individärenden (2021–2023). Riksrevisionen. Ändrade förhållanden – ineffektiv hantering i socialförsäkringen (RiR 2026:4).

5.3.1 Uppskattningar av den potentiella nyttan

1. Högre skatteefterlevnad tack vare automatiserad riskklassning

Automatiserad riskklassning utgör ett centralt verktyg för att förbättra träffsäkerhet och effektivitet i skatteförvaltningens kontrollverksamhet. Skatteverket använder redan AI för urval, analys och beslut och regeringen förstärker kapaciteten via AI-tjänster. PET gör det möjligt att skala urvalen till fler datakällor med lägre integritetsrisker. Förbättrad träffsäkerhet ger två effekter: (1) högre regelefterlevnad (frivillig och efter kontroll), (2) lägre kontrollkostnad per upptäckt fel.[116]

Estimerad nyttopotential:

- Antagande: Del av skattegapet adresserbar genom bättre kontrollurval utgör 10–20 mdkr per år[117]
- Antagande: AI-adresserbar andel (30–50%) × förbättring i kontrollträffsäkerhet (20–30%) [118]
- Direkta återförda belopp (fel som kunnat undvikas): 0,8–1,6 mdkr per år + Produktivitetsvinster (handläggningstid, ärendeprioritering, mindre manuell granskning): 0,2–0,4 mdkr per år.

Årsnytta: **1,0–2,0 mdkr**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 1,0 och 2,0 mdkr årligen.

2. Förbättrad bekämpning av välfärdsbrott

Riksrevisionen menar att brister i identitetskontroll och registerkvalitet leder till felaktiga utbetalningar och brott, just på grund av att myndigheterna inte kunnat dela data effektivt och rättssäkert. En försiktig bedömning från SKR/KPMG uppskattar att minst 30 miljarder kronor per år felaktigt betalas ut på grund av välfärdsbrott. Riksdagen visar att AI redan används i regioner för att upptäcka välfärdsbrott med goda resultat, och att datadelning är en kritisk förutsättning för skala och precision.[119]

PET möjliggör att:

- Myndigheter kan jämföra data attribut-mot-attribut

[116] OECD. Emerging privacy-enhancing technologies: Current regulatory and policy approaches, 2023.
[117] Skatteverket. Tax Gap-rapporter (senaste tillgängliga).
[118] OECD/IMF. Advancing accountability in AI, 2023.
[119] Riksrevisionen. Subventionerade anställningar – att motverka fel i ett system med allvarliga risker (RiR 2023:17). SOU 2019:59. Samlade åtgärder för korrekta utbetalningar från välfärdssystemen (2019). SKR & KPMG. Analyser av välfärdsbrott och automatiserade kontroller (refererat i SKR:s ekonomirapporter och remissyttranden).

- …utan att dela rådata eller göra otillåten registersamkörning
- …vilket minskar både juridiska och praktiska hinder.

Det gör att fler indikatorer på välfärdsbrott kan upptäckas, t.ex.:
- parallella stöd i olika kommuner
- orimliga kombinationer av inkomst, bidrag och närvaro
- identitetsmönster som tyder på organiserad brottslighet

När matchning blir möjlig över fler myndigheter ökar träffsäkerheten, och bortfallet ackumuleras exponentiellt. Enligt SKR/KPMG är automatiserade kontroller avgörande för att ersätta manuella stickprov, de är mer träffsäkra, snabbare och kontinuerliga och en direkt metod för att stoppa felaktiga utbetalningar. PET är möjliggöraren som gör att dessa automatiseringar kan ske lagligt och på mer fullständiga data, vilket ger ett lyft bortom vad exempelvis dagens RPA klarar. PET-lösningar möjliggör säkrare matchning mellan kommun–stat utan integritetsrisker.[120]

Estimerad nyttopotential:

- Antagande: Internationella studier av datadrivna kontrollsystem samt svenska pilotfall visar att vi kan förvänta oss en minskning med 5–10 % av välfärdsbrotten när datadelning, AI och automatisering kombineras.[121]
- Antagande: 5–10 % (konservativt) av 30 mdkr = 1,5–3,0 mdkr per år.
- Minskat manuellt arbete och snabbare ärendehantering → ytterligare 0,2–0,4 mdkr per år.

Årsnytta: **1,7–3,4 mdkr.**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 1,7 och 3,4 mdkr årligen.

3. Förbättrad internationell samverkan mot skattebrott

Enligt OECD:s och Skatteverkets bedömningar kan PET möjliggöra en förbättrad skattebrottsbekämpning över gränserna. Att öka tillämpningen av PET (bl.a. för säkrare delning, lägre risk och snabbare processer) stärker både indrivning och regelefterlevnad.[122]

[120] SKR & KPMG. Analyser av välfärdsbrott och automatiserade kontroller (refererat i SKR:s ekonomirapporter och remissyttranden).
[121] Brookings Institution. Using AI and machine learning to reduce government fraud (2021). OECD. Governing with Artificial Intelligence - AI in fighting corruption and promoting public integrity (2025).
[122] OECD, Emerging privacy-enhancing technologies: Current regulatory and policy approaches, OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023. OECD, Tax Administration 3.0: The Digital Transformation of Tax Administration, OECD Publishing, Paris, 2020. Skatteverket, Skatteverket leder nytt regeringsuppdrag – samordnad digital informationsdelning för att bekämpa brott, pressmeddelande, 27 juni 2025. Skatteverket, Informationsutbyte med andra länder inom beskattningsverksamheten, Rättslig vägledning, uppdaterad 2026.

Estimerad nyttopotential:

- Antagande: Bas för gränsöverskridande skattebrott: 10–20 mdkr/år
- Antagande: Ekonomisk bas × andel beroende av internationell datadelning (20–40%) × förbättring från säkrare datautbyte (10–20%)

Årsnytta: **0,2–1,0 mdkr**

Summering: Nyttopotentialen inom dessa tillämpningar uppskattas till mellan 0,2 och 1,0 mdkr årligen.

Nedanstående tabell sammanfattar nyttopotentialen för skatte- och bidragskontroller:

Tillämpning	Aktör(er)	Datatyper	Relevanta PETs	Syfte	Samverkan	Värdering per år (mdkr; hela Sverige)
Högre skatteefterlevnad - automatiserad riskklassning	Skatteverket	Skattehistorik	FL, TEE	AI-stöd utan data-centralisering för att minska skattebrott	Myndighet - myndighet	**1,0 – 2,0**
Förbättrad bekämpning av väfärdsbrott	Myndighet + Kommun	Bidrag, inkomster	SMPC, Zero Knowledge Proof	Matchning utan full register-samkörning	Myndighet-myndighet-kommun	**1,7 – 3,4**
Förbättrad internationell samverkan mot skattebrott	Myndigheter	Gränsöver-skridande data	SMPC, kryptering, ZKP	Säker EU-samverkan för att minska exv. skattebrott	Myndighet-EU	**0,2 – 1,0**

Totalt: 2,9 – 6,4 mdkr

Tabell 3: Summering av nyttopotential inom skatte- och bidragskontroller

5.4 Tillämpningsområde: Tvärgående tillämpningar

Detta område belyser några av de mer generiska, tvärgående tillämpningar där PET kan användas för att skapa nyttor för ett flertal sektorer. De tillämpningar vi tittat närmare på är:

- AI-träning av modeller som kan användas av flera aktörer
- Förbättrad gemensam kvalitetsuppföljning med flera aktörer
- Förbättring av statistik

Dessa tillämpningar har vissa överlappningar med de tidigare verksamhetsindelade tillämpningsområdena som beskrivits ovan, vilket gör att vi inte kan addera ihop summorna

av de potentiella nyttorna, men det kan ändå vara intressant att försöka beskriva potentialen ur ett annat perspektiv. Nedan följer *beskrivningar* av nyttopotentialen i form av några exempel inom de fyra tillämpningarna ovan.

Exempel 1: Gemensam AI-träning för kommuner

En utmaning idag när kommuner vill använda AI för olika ändamål är att man är mer eller mindre förhindrad att träna sina modeller som omfattar persondata, bl.a. finns det juridiska, etiska och säkerhetsrelaterade hinder. Det finns en rädsla för att dela verksamhetsdata, samtidigt som små kommuner saknar analys- och IT-kapacitet.

Dessa utmaningar kan man adressera med hjälp av PET och träna AI-modellerna utan att använda faktiska rådata, t.ex. med hjälp av federerad inlärning eller betrodda exekveringsmiljöer (Trusted Execution Environment, TEE). Resultatet blir att AI-modellerna kan tränas lokalt i varje kommun och endast modelluppdateringarna delas utan att lagra rådata centralt.

- Här kan man även använda sig av syntetiska data för att t.ex. utveckla och testa system, utbilda personal eller samverka med leverantörer – utan att behöva hantera riktiga persondata.
- Andra nyttor som kan genereras är att olika kommuner enklare kan göra olika typer av analyser, t.ex. för att kunna jämföra kostnader, utfall, metoder eller arbetssätt.

Exempel 2: AI-träning av gemensamma modeller för statliga myndigheter

Statliga myndigheter såsom Skatteverket, Polisen, Migrationsverket m.fl. kan ha en stor nytta av att gemensamt skapa förmågan till AI-stöd utan central datalagring eller modellträning på känsliga register. Detta åstadkoms t.ex. med hjälp av federerad inlärning och betrodda exekveringsmiljöer (TEE).

Exempel 3: Förbättrad regiongemensam kvalitetsuppföljning

Med hjälp av PET kan regionerna skapa ökade möjligheter till uppföljning av olika mål med hjälp av gemensamma, förbättrade analyser av kvalitetsregistren. Så här kan man då resonera för att bedöma nyttopotentialen:

- Antaganden: Ett urval av indikatorer från kvalitetsregister (t.ex. återinläggning, väntetider) analyseras kvartalsvis med hjälp av säker flerpartsberäkning för alla 21 regioner.
- Mål: minst 8 gemensamma beräkningar/kvartal, förbättringscykler dokumenterade.
- Antagande: Resultatet minskar onödiga återbesök och dubbelprovtagningar med 1–2 %.
- Nyttopotential: Årlig besparing som i medelstora regioner ligger i spannet tiotals miljoner kr (mindre akuta kostnader, kortare vårdtider).

Exempel 4: Förbättrad statistik

Genom att tillämpa PET kan statistikunderlaget förstärkas och förbättras, vilket ökar värdet för många myndigheter, kanske i synnerhet statistikansvariga myndigheter såsom SCB, Konjunkturinstitutet och Socialstyrelsen. Med hjälp av differentiell integritet så kan man uppnå mer omfattande publicerbar statistik med hög integritetsnivå och fortsatt högt analysvärde.

5.5 Summering av nyttopotentialen – Mikroperspektivet

Nedanstående tabell summerar på aggregerad nivå de potentiella nyttoestimaten för de tillämpningsområden och tillämpningar som är beskrivna ovan. Dessa estimat används som utgångspunkt för beräkningarna i scenarioanalysen (kapitel 7).

Tillämpningsområde	Potentiell nytta (per år)	Kommentar
Hälso- och sjukvård	12,3 – 25,6 Mdkr	
Socialtjänst, omsorg och bistånd	4,0 – 9,6 Mdkr	
Skatte- och bidragskontroller	2,9 – 6,4 Mdkr	
TOTALT	**19 – 42 Mdkr**	Något högre än makro-estimatet (10 – 40 mdkr)

Tabell 4: Summering av nyttopotentialen i de olika tillämpningsområdena

6 Investerings- och kostnadsanalys

Detta kapitel behandlar de initiala investeringar och löpande kostnader som de medverkande statliga myndigheterna har estimerat utifrån utredningens förslag. Kapitlet innehåller också en uppskattning av de investeringar och kostnader som också kommer att krävas hos de användande (”lokala”) aktörerna inom offentlig förvaltning (statliga myndigheter, regioner och kommuner) som kommer att kunna dra nytta av ett införande av integritetsfrämjande tekniker.

Estimaten har uttryckts i spann, och till sist kopplar vi dessa till de scenarion som behandlas i nästa kapitel.

6.1 Skatteverket

Utredningen bedömer att de gemensamma tjänsterna initialt bör fokusera på tekniker som:

- är mogna för praktisk användning,
- har stor potential i offentlig förvaltning,
- idag används i begränsad omfattning.

Utifrån dessa kriterier pekas *säker flerpartsberäkning* (SMPC) ut som den teknik där behovet av en gemensam nationell tjänst är störst. Skattverket bedöms i utredning vara lämplig att ta fram, drifta och utveckla denna tjänst, och har gjort nedanstående kostnadsuppskattningar.

Kostnaden för att utvärdera och genomföra en pilot av en gemensam tjänst för säker flerpartsberäkning bedöms uppgå till **cirka 46 miljoner kronor**. Estimatet omfattar projektledning, uppbyggnad av PET- och SMPC-kompetens, marknadsdialog och anskaffningsförberedelser, licenser och leverantörsstöd för SMPC-produkt, teknisk plattform, arkitektur, utveckling och konfiguration, dataförberedelser, juridiska analyser, informationssäkerhet, säkerhetstestning, onboarding av pilotaktörer samt slutlig utvärdering och rapportering.

Vid en efterföljande produktionssättning bedöms engångskostnaden uppgå till **cirka 72 miljoner kronor**. Den årliga kostnaden för drift och förvaltning av en gemensam tjänst bedöms därefter uppgå till **cirka 57 miljoner kronor per år**.

Estimatet är förenat med viss osäkerhet, främst avseende vald SMPC-produkt, licensmodell, antal deltagande aktörer, krav på tillgänglighet och säkerhet, mängden anpassningar samt ambitionsnivån för onboarding och stöd till offentlig förvaltning. Kostnadsuppskattningarna för produktionssättning samt drift och förvaltning är indikativa och kommer att tydliggöras i samband med att uppdraget konkretiseras.

Sammanfattande tabell för kostnadsestimaten från Skatteverket:

Del	Kostnadsestimat
Utvärdering och pilot av gemensam SMPC-tjänst	46 mnkr
Engångskostnad för produktionssättning efter pilot	72 mnkr
Drift och förvaltning, årlig planeringsnivå	57 mnkr/år

Tabell 5: Kostnadsestimat från Skatteverket

Alternativ: Långsiktig etablering av robust SMPC-tjänst, utan pilotskede

Förslagen i utredningen om integritetsfrämjande teknik, kapitel 9, syftar till att skapa organisatoriska och styrningsmässiga förutsättningar för användning av integritetsfrämjande teknik, inklusive säker flerpartsberäkning (SMPC). Tyngdpunkten ligger på ansvarsfördelning, samordning och långsiktig förvaltning. Lösningen är medvetet försiktig och inriktad på att möjliggöra användning, medan den initiala tekniska ambitionsnivån lämnas relativt låg.

Vår bedömning är att denna ansats innebär en risk. SMPC är en tekniskt avancerad lösning som inte kommer till faktisk användning om den inte från start erbjuds som en robust och driftsatt tjänst. Myndigheter använder inte tekniken om den upplevs som omogen eller resurskrävande att ta i bruk.

Vår bedömning är att en gemensam SMPC-tjänst redan från etableringsfasen bör utformas med:

- Färdig och sammanhållen teknisk arkitektur, anpassad för säker flerpartsberäkning och andra kryptografiskt avancerade tillämpningar.
- Fastställda säkerhetslösningar, inklusive kryptering, sekretshantering (secret management) och skydd av kryptografiska nycklar.
- Etablerad driftmiljö, med krav på stabilitet, tillgänglighet och incidenthantering, motsvarande annan förvaltningsgemensam infrastruktur.
- Tydliga ansvarsförhållanden i drift, där det är klart vem som ansvarar för teknik, säkerhet, support och vidareutveckling.
- Grundläggande support- och förvaltningsförmåga, så att användande myndigheter inte själva behöver lösa tekniska problem eller tolka lösningen.
- Standardiserade anslutnings- och användningsprocesser, som gör att nya användningsfall kan påbörjas utan omfattande lokala anpassningar.
- Förberedda och fastställda juridiska och organisatoriska arbetssätt, som stödjer användning inom befintliga regelverk och minskar osäkerhet hos användande aktörer.
- Tillräcklig teknisk mognad från start, så att tjänsten upplevs som tillförlitlig och användbar, inte som ett pilot- eller experimentverktyg.

Om genomförandet sker med för låg initial teknisk ambitionsnivå finns en påtaglig risk att tjänsten etableras formellt men inte används, vilket leder till nya pilotinsatser och parallella

lösningar. Vårt alternativa förslag minskar denna risk genom att prioritera faktisk användbarhet från början.

En sådan inriktning innebär ett något högre initialt kostnadsestimat. En tekniskt mogen och driftsatt SMPC-tjänst bedöms kräva **ytterligare 20 miljoner kronor i etableringsfasen** samt en **något högre årlig driftskostnad**. Denna merkostnad är enligt vår bedömning motiverad, eftersom den minskar behovet av upprepade piloter och ger bättre kostnadseffektivitet över tid.

Sammanfattningsvis är vår bedömning att detta mer ambitiösa alternativ för utredning och pilot bör genomföras för att säkerställa faktisk användning och långsiktig samhällsnytta.

- Initiala kostnader (exklusive pilot): 87–97 mkr
- Löpande kostnader: 57–62 mkr

6.2 Digg (Myndigheten för digital förvaltning)

Utredningen bedömer att Digg är den myndighet som är mest lämpad att ansvara för ett nationellt stödjande och vägledande uppdrag avseende integritetsfrämjande teknik. Diggs ansvar för den förvaltningsgemensamma digitaliseringen och infrastrukturen Ena, samt myndighetens sektorsövergripande roll inom digitalisering och datadelning, innebär att delar av den organisatoriska och samordnande kapacitet som krävs redan finns etablerad.

Detta innebär att de initiala investeringarna och kostnaderna kan begränsas, jämfört med om uppdraget skulle läggas på en myndighet utan motsvarande strukturer. Samtidigt kräver uppdragets tekniska och metodmässiga innehåll viss förstärkning med ny spetskompetens, särskilt inom avancerade integritetsfrämjande tekniker.

Uppskattade initiala investeringar/kostnader:

- Uppbyggnad och förstärkning av PET-kompetens inom åtminstone juridik, data, AI, analys och rådgivning, inkl. rekrytering och upphandling av resurser.
- Fördjupad behovsanalys med målgrupper för att förstå vilken typ av vägledning som behövs och hur den bör spridas för att nå största möjliga nytta.
- Ta fram vägledning, utbildning och metodstöd för införandet av prioriterade tekniker (DI, Syntetiska data; ej SMPC)
- Etablera metod och utvärdering av återidentifieringsrisker
- Starta upp samverkan med expertmyndigheter för dessa frågor (bl.a. IMY och FRA).
- Etablera former för att föra ut vägledning och metodstöd i digitala kanaler och vid behov i fysiska kanaler, t.ex. utbildningar.

Uppskattade löpande kostnader:

- Personal
- Löpande vägledning och uppdateringar (t.ex. best practice, rättspraxis, EU-krav, AI-utveckling)
- Samverkan och kunskapsspridning till målgrupper (forum, utbildningar, stöd etc)

- Löpande expertstöd/samverkan med andra myndigheter/expertaktörer
- Vidmakthålla och uppdatera digitala kanaler för spridning av vägledning och stöd.

Kostnadsestimat från Digg under de tre första åren av uppdraget:

Kostnadspost	2027 (kkr)	2028 (kkr)	2029 (kkr)
Personal	6 500	7 400	6 500
Konsulter/expertstöd	2 100	1 200	950
Webbutv, film och utbildningar	500	700	700
Resor	150	200	200
Summa	9 250	9 500	8 350

Tabell 6: Kostnadsestimat från Digg

Till detta tillkommer ett spann för att beskriva en viss osäkerhet i estimatet på ca 2 000 kkr. Detta ger:

- Initiala kostnader (år 1 och 2): 8,5–10,5 mkr
- Löpande kostnader: 7,5–9,5 mkr

6.3 IMY

IMY bedömer att deras del av kostnaderna utgörs av löpande kostnader för stöd och rådgivning i intervallet 1,0–1,3 årsarbetskrafter (där kostnaden för en ÅA ligger på 1,5 mkr).

Detta ger att de årliga kostnaderna uppskattas till ca 1,5–2,0 mkr.

6.4 SCB

SCB bedömer att deras del av kostnaderna utgörs av löpande kostnader för stöd och rådgivning i intervallet 0,25–0,50 årsarbetskrafter (där kostnaden för en ÅA ligger på 1,6 mkr).

Detta ger att de årliga kostnaderna uppskattas till ca 0,4–0,8 mkr.

6.5 NCSC/FRA

NCSC bedömer att deras del av kostnaderna utgörs av löpande kostnader för stöd och rådgivning i intervallet 0,25–0,5 årsarbetskrafter (där kostnaden för en ÅA ligger på 1,6 mkr).

Detta ger att de årliga kostnaderna uppskattas till ca 0,4–0,8 mkr.

6.6 E-hälsomyndigheten

E-hälsomyndigheten bedömer att de årliga kostnaderna uppskattas till ca 2,5–3,5 mkr.

6.7 Socialstyrelsen

Socialstyrelsen bedömer att det första av deras två uppdrag kommer att kräva en årlig kostnad på ca 2,5–3,5 mkr. Deras andra uppdrag bedöms inte kräva några ytterligare kostnader.

6.8 Lokala kostnader för de användande aktörerna

För att de användande aktörerna (d.v.s. statliga myndigheter, regioner och kommuner) ska kunna tillgodogöra sig de nya möjligheterna med PET (initialt med fokus på de fyra olika tekniker som utredningen föreslår att kraftsamla kring), nyttjandet av de nationella tjänsterna och delvis förändrade arbetsprocesser så kommer de att behöva investera ”lokalt”. Vi antar att anslutningsgraden och anpassningarna som krävs lokalt kommer att ske gradvis över tid, vilket återspeglar sig i nedanstående kostnadsberäkningar samt i de utvecklingsscenarion som beskrivs i kapitel 7. De första åren bedömer vi att endast en minoritet av de användande aktörerna gör investeringar och satsningar för att bygga sin förmåga att utnyttja möjligheterna med PET, och andelen kommer därefter växa successivt över tid.

För att kunna göra en uppskattning av hur stora de *lokala* investeringarna och kostnaderna är, som är kopplade till användande aktörer, så använder vi oss av följande resonemang: investeringar och kostnader avser *lokala anpassningar*, *anslutning till tjänsterna* och *egen kapacitets- och kompetensuppbyggnad.*

6.8.1 Grundläggande antaganden

För samtliga aktörer gäller att kostnaderna är betydligt lägre än vid egenutveckling av de föreslagna PET-tjänsterna, men inte noll. För kommuner, regioner och statliga myndigheter har följande antaganden gjorts:

1. Aktörerna utvecklar inte egna avancerade PET-lösningar**,** utan använder de nationella tjänsterna.
    - Den mest resurskrävande tekniken (SMPC) tillhandahålls centralt av Skatteverket.
    - Digg tillhandahåller nationell vägledning, mallar, stöd och utbildning.

2. ”Lokala” kostnader för varje mottagande aktör uppstår främst för:
    - juridisk och verksamhetsmässig anpassning (analys, DPIA etc)
    - teknisk anslutning/integration

- säkerställande av intern kompetens och resurser för införande, förvaltning, samverkan och användning.

Detta innebär att lokala kostnader i huvudsak är användar- och anpassningskostnader**,** snarare än utvecklingskostnader.

6.8.2 Övergripande beräkningslogik för lokala kostnader

För att kunna estimera de lokala (användarnas) kostnad så har vi använt oss av följande grundlogik:

Lokal kostnad = juridisk analys + anslutning + anpassning och förmåga + löpande användning

Det innebär att lokala kostnader:

- domineras av personella insatser och verksamhetsarbete, inte IT-utveckling
- är relativt begränsade och hanterbara**,** även för små aktörer
- skalar relativt linjärt med verksamhetens storlek och komplexitet.

6.8.2.1 Segmentering av användande aktörer

För att möjliggöra ett sammanvägt kostnadsestimat för hela landet har kommuner, regioner och statliga myndigheter delats in i tre storlekssegment (små, mellanstora och stora) baserat på:

- invånarantal (kommuner och regioner)
- antal anställda och verksamhetsbredd (statliga myndigheter).

Segmenteringen bygger på vedertagna indelningar som används av bland annat SKR och ESV. Kostnaderna har därefter schabloniserats per segment för att spegla skillnader i komplexitet, antal potentiella användningsfall och intern kapacitet. Vi använder följande segmentering för att kunna beräkna de lokala kostnaderna:

Statliga myndigheter:

- Små: < 500 anställda
- Mellanstora: 500–2 000 anställda
- Stora: > 2 000 anställda

Regioner:

- Små regioner: < 200 000 invånare
- Mellanstora regioner: 200 000–600 000 invånare
- Stora regioner: > 600 000 invånare

Kommuner:

- Små: < 20 000 invånare

- Mellanstora: 20 000–100 000 invånare
- Stora: > 100 000 invånare

Totala antal aktörer i de tre segmenten:

Aktörstyp	Antal
Statliga myndigheter	340[123]
Regioner	21
Kommuner	290

Dessa fördelas i storlekssegment enligt segmenteringen ovan:

Aktörstyp	Små	Mellanstora	Stora
Statliga myndigheter	220	90	30
Regioner	6	9	6
Kommuner	190	80	20

6.8.2.2 Antagande om Årsarbetskraftsbelopp (ÅA)

Vid beräkning av lokala kostnader som är kopplade till personella insatser har vi använt en schablon om 1,2–1,4 miljoner kronor per årsarbetskraft (ÅA), inklusive lön, sociala avgifter och overheadkostnader. Intervallet har tillämpats differentierat beroende på kompetensnivå och aktörstyp, med ett vägt genomsnitt om cirka 1,3 miljoner kronor per årsarbetskraft för de flesta lokala aktörer. Beloppen är medvetet valda i ett högre spann än snittet, eftersom PET-användning kräver kvalificerad kompetens och kostnaderna bör vara jämförbara mellan de olika sektorerna.[124]

Typ av resurs och genomsnittliga ÅA:

- Verksamhetsutvecklare, handläggare: 1,2 mkr/ÅA
- IT-förvaltare, systemansvarig: 1,3 mkr/ÅA
- Jurist, IT-arkitekt, specialist: 1,4 mkr

Dessa belopp har använts vid beräkning av de löpande lokala kostnaderna. Även de initiala investeringarna/kostnaderna bygger på dessa årsarbetskraftsbelopp, men är omräknade till en projektinsats under 6–12 månader.

6.8.3 Lokala kostnadskomponenter

De lokala kostnaderna har beräknats genom att dela upp anslutning och drift i fyra återkommande delar, som förekommer hos samtliga aktörstyper, beskrivna i styckena nedan.

[123] Regeringskansliet.
[124] Sveriges Kommuner och Regioner (SKR). Personalkostnader i kommuner och regioner – schabloner för kalkyler och investeringar. SKR, Stockholm. Ekonomistyrningsverket (ESV). Vägledning i samhällsekonomiska analyser (senaste version).

6.8.3.1 Juridisk analys och regelefterlevnad

De aktiviteter som vi här inkluderar är:
- Ändamålsbedömning
- DPIA-analys
- Analys av registerförfattningar och sekretesskrav
- Dialog med Digg och IMY vid behov

Typisk resursåtgång:
- jurist + verksamhetsrepresentant
- intensivt i uppstartsfasen, begränsat löpande

Schablonantagande: 0,2–0,6 årsarbetskrafter under första året (beroende på storlek), därefter 0,05–0,1 årsarbetskraft per år.

6.8.3.2 Teknisk anslutning och systemintegration

De aktiviteter som vi här inkluderar är:
- konfigurering mot nationell SMPC-tjänst
- anpassning av lokala datamodeller
- loggning, behörighet, åtkomstkontroller
- test och verifiering

Egen utveckling av SMPC-algoritmer samt drift av egna beräkningsnoder inkluderas ej.

Schablonantagande: 1–3 integrationsflöden per aktör, huvudsakligen arbete för systemförvaltare/IT-arkitekt.

6.8.3.3 Verksamhetsanpassning och kompetensuppbyggnad

De aktiviteter som vi här inkluderar är:
- anpassning av arbetssätt
- definition av användningsfall
- utbildning av nyckelpersoner
- deltagande i Diggs nationella stödstrukturer

Schablonantagande: Varje aktör behöver (minst) 1–2 interna nyckelpersoner som förstår både verksamhet och PET-tillämpning.

Resursåtgången antas vara relativt låg men kritisk för om tjänsterna faktiskt används.

6.8.3.4 Löpande användning och förvaltning

De aktiviteter som vi här inkluderar är:
- återkommande SMPC-körningar

- kvalitetsuppföljning och löpande förbättringar
- dialog med Skatteverket (tjänsteägare)
- uppdateringar vid förändrade behov eller regelverk

Schablonantagande: Dessa insatser motsvarar en liten del av befintlig förvaltning, och faller ofta inom redan existerande roller.

6.8.4 Beräkning för olika aktörstyper

Nedan redovisas konkret hur schablonerna räknats fram för respektive aktörstyp. För att säkerställa rimligheten har kostnaderna jämförts med kända kostnader vid anslutning till andra nationella tjänster (t.ex. Mina meddelanden, SDK, Skatteverkets tjänster).[125]

6.8.4.1 Beräkningsmodell för att aggregera kostnadsestimaten

De aggregerade lokala kostnaderna har beräknats genom att schabloniserade initial- och årskostnader per aktör och storlekssegment multiplicerats med antal aktörer och antagen anslutningsgrad. Kostnaderna härrör primärt från personella insatser för juridik, integration, verksamhetsanpassning och löpande användning, uttryckta i årsarbetskrafter med ett enhetligt kostnadsantagande om cirka 1,3 mkr per ÅA (Årsarbetskraft).

De nationella totalsiffrorna utgör summeringar över samtliga tre segment och reflekterar olika utvecklingsscenarier (se kapitel 7) snarare än osäkerhet i schablonerna.

Övergripande princip

Aggregeringen bygger på en uppsummering (bottom-up) enligt följande steg:

- Individuell schablonkostnad per aktör →
- summering per segment →
- viktning med anslutningsgrad (tre olika scenarion med olika anslutningsgrad) →
- nationellt totalestimat (spann min/max).

Ingen genomsnittskostnad appliceras direkt på riket; alla totalsiffror är explicit härledda från:

- segmentvisa schabloner, och
- antal aktörer per segment.

Grundekvation

För varje aktörstyp a (statlig myndighet, region, kommun) och varje storlekssegment s:

Initial kostnad:

[125] Digital myndighetspost, SOU 2024:47, särskilt avsnitten om kostnader för Digg och anslutande myndigheter. Digg, SKR m.fl., Samhällsekonomisk kostnadsnyttoanalys – Säker digital kommunikation (SDK). Ekonomistyrningsverket, Avgifter i staten, årliga redovisningar av statliga myndigheters avgiftsbelagda och gemensamma tjänster.

$$K_{a,s}^{init} = N_{a,s} \times p_{a,s} \times C_{a,s}^{init}$$

Årlig löpande kostnad:

$$K_{a,s}^{år} = N_{a,s} \times p_{a,s} \times C_{a,s}^{år}$$

Där:

- $N_{a,s}$ = antal aktörer i segmentet
- $p_{a,s}$ = anslutningsgrad (andel som faktiskt använder PET-tjänster)
- $C_{a,s}^{init}$ = schablon för *initial* kostnad per aktör
- $C_{a,s}^{år}$ = schablon för *årlig* kostnad per aktör

Anslutningsgrad

Anlsutningsgraden nedan antas vara den grad av anslutning som nås efter en relativt lång tidsrymd (> 10 år) då införandet har nått en hög mognad och mättnad, för att estimera de lokala kostnaderna. Dessa antaganden motsvarar utvecklingen i de tre scenarion vi skapat (se kapitel 7) för att beskriva införandet av PET över tid (scenario A= låg, scenario B = medelhög, scenario C=hög).

Aktörstyp / Scenario	**A**	**B**	**C**
Statliga myndigheter	30 %	60 %	90 %
Regioner	50 %	75 %	100 %
Kommuner	20 %	40 %	70 %

Notera: Det är variationen i anslutningsgrad, inte variationen i schabloner, som ger de breda intervallen.

Härledning av schablonkostnader per aktör

Alla kostnadskomponenter räknas i grunden som:

$$K = ÅA \times kostnad_{ÅA}$$

Där:

- ÅA = årsarbetskraft (andelar tillåtna, t.ex. 0,3 ÅA)
- Kostnad (ÅA) = 1,2–1,4 mkr (vägt snitt ≈ 1,3 mkr)

Initiala kostnader räknas som tidsbegränsade projektinsatser (6 – 12 månader):

$$ÅA_{init} = ÅA_{helår} \times 0{,}5–1{,}0$$

RI. SE
Research Institutes of Sweden

Kostnadskomponenter per aktör

För varje aktör summeras fyra delar:

$$C_{a,s}^{init} = C_{a,s}^{juridik} + C_{a,s}^{integration} + C_{a,s}^{verksamhet} + C_{a,s}^{koordination}$$

$$C_{a,s}^{år} = \mathring{A}A_{a,s}^{år} \times 1{,}3 \text{ mkr}$$

Skillnader mellan segment beror på:

- antal integrationer,
- antal användningsfall,
- komplexitet i juridik och dataskydd,
- antal interna verksamheter.

6.8.5 Segmentsvisa schabloner

6.8.5.1 Statliga myndigheter

Kostnaderna som uppstår för en statlig myndighet är framför allt dessa:

- anpassning till nationell SMPC-tjänst,
- lokal juridik, loggning och revisionskrav,
- egen systemintegration,
- löpande deltagande i Diggs stödstruktur.

Beräkningsexempel för en mellanstor myndighet:

Initial kostnad (2–4 mkr):

- Juridik och registeranalys: 0,8–1,2 mkr
- Integration mot interna system: 0,8–1,5 mkr
- Verksamhet och utbildning: 0,4–0,8 mkr

Årlig kostnad (0,9–1,5 mkr):

- ca 0,7–1,2 årsarbetskrafter

Statliga myndigheter har ofta fler användningsfall än kommuner, men ofta tillgång till resursstarkare IT-förmåga.

Nedanstående tabell sammanfattar estimaten för de *lokala kostnaderna*, för de olika myndighetssegmenten:

Segment	Initial investering/ kostnad	Löpande årlig kostnad	Kommentar
Liten myndighet	1–2 mkr	0,5–0,9 mkr	Begränsat antal SMPC-flöden
Mellanstor myndighet	2–4 mkr	0,9–1,5 mkr	Operativ återkommande användning
Stor myndighet	4–7 mkr	1,5–3,0 mkr	Flera parallella användarfall

Tabell 7: Sammanfattning av lokala kostnader för statliga myndigheter

6.8.5.2 Regioner

Kostnaderna som uppstår för en region är framför allt dessa:
- juridisk analys och DPIA (lokalt),
- teknisk anslutning till SMPC-tjänsten,
- verksamhetsanpassning (hälso- och ekonomidata),
- 1–3 interna resurser deltid,
- deltagande i Diggs stöd- och samverkansforum.

Regioner har generellt:
- fler datakällor,
- högre skyddsvärde,
- fler juridiska beroenden.

Beräkningsexempel för en *mellanstor* region:

Initial kostnad (4–7 mkr):

- Juridik/DPIA: 1,0–1,5 mkr
- IT-integrationer (flera system): 1,5–2,5 mkr
- Verksamhetsarbete & utbildning: 1,0–1,5 mkr
- Projektledning/koordination: 0,5 mkr

Årlig kostnad (1,5–2,5 mkr):

- 1–1,5 årsarbetskrafter totalt (fördelat)
- återkommande SMPC-användning i flera verksamheter

Nedanstående tabell sammanfattar estimaten för de *lokala kostnaderna*, för de olika regionsegmenten:

Segment	Initial investering/ kostnad	Löpande årlig kostnad	Kommentar
Liten region	2–4 mkr	1,0–1,5 mkr	Begränsade användarfall, få integrationer
Mellanstor region	4–7 mkr	1,5–2,5 mkr	Flera förvaltningar, återkommande SMPC-användning
Stor region	7–12 mkr	2,5–4,0 mkr	Många verksamheter, hög datavolym

Tabell 8: Sammanfattning av lokala kostnader för regioner

6.8.5.3 Kommuner

Kostnaderna som uppstår för en kommun är framför allt dessa:

- lokal juridisk bedömning,
- teknisk anslutning via standardgränssnitt,
- deltagande i Digg-ledd utbildning,
- begränsad intern specialkompetens (ofta deltid),
- användning av färdiga SMPC-use case.

Beräkningsexempel för en *liten* kommun:

Initial kostnad (0,8–1,5 mkr) består av:

- Juridik: ca 0,3–0,5 mkr
- IT-integration: ca 0,2–0,4 mkr
- Verksamhet/utbildning: ca 0,2–0,3 mkr

Årlig kostnad (0,3–0,6 mkr) består av:

- 0,2–0,4 årsarbetskraft (fördelad på flera personer)
- begränsad återkommande samverkan

Varför kostnaden är låg för små kommuner?

- Få användningsfall
- Färdiga nationella lösningar
- Starkt beroende av Diggs vägledning

- Ingen parallell utveckling av egna lösningar

Nedanstående tabell sammanfattar estimaten för de *lokala kostnaderna*, för de olika kommunsegmenten:

Segment	Initial investering/ kostnad	Löpande årlig kostnad	Kommentar
Liten kommun	0,8–1,5 mkr	0,3–0,6 mkr	Enstaka användningsfall
Mellanstor kommun	1,5–3 mkr	0,6–1,2 mkr	Flera nämnder, viss automatisering
Stor kommun	3–5 mkr	1,2–2,0 mkr	Regelbunden användning, större integration

Tabell 9: Sammanfattning av lokala kostnader för kommuner

6.8.6 Aggregerade lokala kostnader per segment

Vid en aggregering av ovanstående lokala kostnadsestimat får vi denna bild, beroende på de utvecklingsscenarion vi använt oss av (där ”anslutningsgraden” till PET-tjänsterna varierar):

Segment (användande aktör)	Total initial investering/kostnad (mkr)	Total löpande årlig kostnad (mkr)	Kommentar
Statliga myndigheter	105 – 315	44 – 133	
Regioner	32 – 96	12 – 35	
Kommuner	120 – 359	48 – 142	
Summering	**257 – 770**	**104 – 310**	

Tabell 10: Summering av de lokala kostnaderna för de olika segmenten

6.9 Sammanställning av investerings- och kostnadsestimat

Nedanstående tabell sammanfattar *samtliga* investerings- och kostnadsestimat ovan:

Aktörer	Total initial investering/kostnad (mkr)	Total löpande årlig kostnad (mkr)	Kommentar
Skatteverket	87 – 97	57 – 62	Beräknat på alternativet med långsiktig implementation av SMPC-tjänsten utan att gå via pilot
Digg	9 – 11	8 – 9	Initiala kostnader antas vara giltiga för både år 1 och år 2
Övriga myndigheter och aktörer	7 – 11	7 – 11	Initiala kostnader är desamma som löpande kostnader
Användande aktörers lokala kostnader	257 – 770	104 – 310	Se tabell 10 ovan
Totalt	**360 – 889**	**176 – 392**	

Tabell 11: Summering av samtliga kostnadsestimat

7 Scenarioanalys: Nyttopotential och kostnader

Baserat på ett flertal uppskattningar att 30–80 miljarder kronor per år kan frigöras i samhällsekonomiskt värde genom förbättrad datadelning (*se kapitel 3 Nyttopotential: Makroperspektivet*). Av dessa bedöms **19–42 miljarder kronor per år** (*se kapitel 5 Nyttopotenial: Mikroperspektivet*) i potentiell nytta vara direkt beroende av ett nyttjande av integritetsfrämjande tekniker (PET) som då möjliggör en mer avancerad och rättssäker datadelning med god överblick. För att analysera hur stor del av den totala potentialen av förbättrad datadelning i offentlig förvaltning som kan realiseras *över tid* används i studien en *scenariobaserad ansats.*

Scenarierna beskriver tre olika utvecklingsvägar (beräkningsmässigt baserade på s k logistiska tillväxtkurvor eller S-kurvor) beroende på ambitionsnivå och graden av institutionella reformer, förbättrad interoperabilitet samt i vilken utsträckning integritetsfrämjande tekniker (PET) införs som operativ kapacitet för säker datadelning.[126]

Vi har valt att skapa tre olika scenarier som representerar olika ambitionsnivåer, teknisk och organisatorisk mognad i offentlig förvaltning. De tre scenarierna kan också betraktas som olika strategiska vägval för statens hantering av PET och ger en mer realistisk syn på att nyttorealisering ofta tar tid.

- **Scenario A** innebär ett alternativ med lägre ambitions- och risknivå, som möjliggör visst lärande, men utan goda förutsättningar för att realisera mer omfattande samhällsekonomiska nyttor.

- **Scenario B** framstår som ett mer robust alternativ, där ambitionsnivå, kostnader, risker och nyttor är mer i balans och där PET börjar etableras som en praktiskt användbar nationell förmåga.

- **Scenario C** innebär i sin tur ett mer ambitiöst, långsiktigt och transformativt angreppssätt, med potential att i grunden förändra förutsättningarna för datadelning i offentlig förvaltning, men till priset av högre krav på insatser, styrning, investeringar och samordning.

Nedan följer en kortfattad beskrivning av av vad varje scenario innebär vad gäller investerings- och kostnadsnivåer samt den förväntade nyttopotentialen.

7.1 Investeringar och kostnader

Scenarierna skiljer sig tydligt åt vad gäller både initiala investeringar och löpande kostnader.

[126] Samtliga monetära värden redovisas i fasta belopp, d.v.s. med dagens valutanivå. Scenarieresultaten inkluderar därmed inte en schabloniserad inflation under den tioåriga analysperioden. Förändringar över tid speglar därför antagen realisering av nyttor och kostnader, inte förändringar i den allmänna prisnivån.

Scenario A kännetecknas av relativt låga initiala investeringar och begränsade årliga löpande kostnader. Kostnadsnivån är hanterbar inom ramen för mindre anslagsförstärkningar, men begränsar samtidigt möjligheten till bred nyttorealisering.

Scenario B innebär relativt måttliga men tydliga resursförstärkningar, både initialt och löpande. Kostnaderna är högre än i scenario A men bedöms stå i god proportion till de nyttor som kan realiseras genom en mer operativ användning av PET.

Scenario C medför de högsta investeringarna och de största årliga kostnaderna. Detta scenario innebär ett långsiktigt åtagande för staten, där satsningen på PET kan betraktas som ambitiös, strukturell och relativt omfattande.

7.2 Förväntad nyttorealisering

Skillnaderna i samhällsekonomisk nyttorealisering mellan scenarierna är betydande, beroende på ambitions- och investeringsnivå, hur pass mycket PET anammas och används bland de användande aktörerna, men är också beroende av hur rättspraxis utvecklas. En betydande del av nyttorealiseringen är beroende av att tillsynspraxis och rättspraxis utvecklas i en positiv riktning:

I **scenario A** uppstår nyttor främst i form av ökad kunskap, viss rättslig klarhet och lärdomar från pilotprojekt. Nyttorna är i huvudsak begränsade till enskilda användningsfall.

I **scenario B** möjliggörs realisering av en väsentlig del av den identifierade nyttopotentialen inom bland annat välfärdsadministration, bidragskontroller och andra känsliga datadelningstillämpningar. Nyttorna är bredare och mer strukturella, men fortfarande koncentrerade till prioriterade områden.

I **scenario C** kan en stor andel av nyttopotentialen realiseras över tid. Genom systematisk användning av PET i merparten av den offentliga förvaltningen skapas förutsättningar för mer genomgripande produktivitets- och kvalitetsvinster, minskade felutbetalningar, färre välfärdsbrott och förbättrad styrning.

7.3 Scenarioanalysens beräkningsmodell

När vi räknar på utvecklingen av potentialen för de tre scenariona, utgår vi från en klassisk logistisk tillväxtkurva (S-kurva):

M = makroekonomisk potential (referensvärde, t.ex. ”0,1–1,5 procent av BNP”)
R(t) = realiserad andel av denna potential vid tidpunkt *t* (0–100 %)
GDP(t) = BNP-nivå

Den årliga nyttan kan då uttryckas som:

Årlig nytta(t) = M × GDP(t) × R(t)

Realiseringen av potentialen delas upp i två komponenter:

α = den andel av den makroekonomiska potentialen som är beroende av PET (dvs. användning av data i känsliga verksamhetsområden)

(1–α) = den andel som inte är beroende av PET (d.v.s. förbättrad interoperabilitet och användning av data med låg känslighet)

Den realiserade andelen kan då uttryckas som:
R(t) = (1–α) × r_base(t) + α × r_pet(t−t₀)

där:

r_base(t) ökar i takt med förbättrad interoperabilitet och institutionell mognad i styrning och regelverk

r_pet(t) ökar i takt med införandet och uppskalningen av PET i verksamhetsområden som hanterar känsliga data

S-kurvans spridningslogik kan uttryckas med följande formel:

$$r(t) = \frac{K}{1 + e^{-b(t-t_0)}}$$

där:

K = taknivå (maximal realiseringsgrad i det aktuella scenariot)
b = införandehastighet
t₀ = inflektionsår (den tidpunkt då tillväxttakten är som högst)

De olika scenarierna skiljer sig åt genom olika taknivåer och införandehastigheter.

Varför S-kurvor är lämpliga att använda:

Införandet av institutionella teknologier följer ofta ett mönster som kan beskrivas med en S-kurva:

- utforskningsfas (pilotprojekt)
- tidig uppskalning (hög osäkerhet)
- standardisering och ökat förtroende
- bred institutionalisering
- mognad och avtagande tillväxt

Införandet av integritetsfrämjande tekniker (PET) passar särskilt väl in i detta mönster eftersom:

- initial rättslig och styrningsmässig osäkerhet begränsar den tidiga användningen

- återanvändbara lösningsmönster minskar den marginella kostnaden för införande
- politisk och organisatorisk riskaversion minskar när framgångsrika användningsfall etableras.

Spridningen sker därför **inte linjärt**, utan följer typiskt en S-formad utvecklingsbana över tid.

Baserat på uppskattningen att ca 30–80 miljarder kronor per år kan frigöras i samhällsekonomiskt värde genom förbättrad datadelning, varav cirka 19 - 42 miljarder kronor per år beräknas vara direkt beroende av PET: Om medianvärdet för den totala makroekonomiska potentialen antas vara 50 miljarder kronor per år, och den del som är beroende av PET antas vara cirka (19+42) / 2 ≈ 31 miljarder kronor per år, motsvarar detta en andel på ungefär 61 %, d v s:

Antagande α = 61 %

Detta antagande innebär att merparten av värdet från förbättrad datadelning antas kunna realiseras genom generella förbättringar i interoperabilitet, styrning och datatillgänglighet, medan integritetsskyddande tekniker (PET) främst möjliggör realisering av en mindre, men fortfarande betydande, del av den totala makroekonomiska potentialen.

7.4 Scenario A

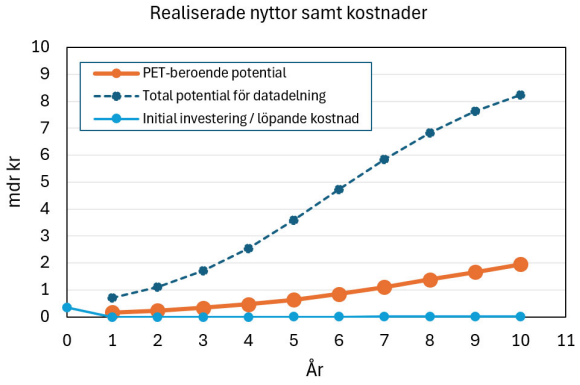
Begränsad strukturell användning av PET: Datadelning förbättras i viss utsträckning genom generella reformer vad gäller interoperabilitet, styrning och rättsliga förutsättningar, men PET etableras inte som operativ, strukturell lösning för känsliga användningsfall. Scenariot innebär ett försiktigt angreppssätt, där staten främst fokuserar på övergripande vägledning och enstaka tekniska piloter. PET introduceras som koncept och prövas i begränsad skala. Genomförandet är selektivt och huvudsakligen koncentrerat till ett fåtal statliga aktörer med hög digital mognad. Den operativa användningen förblir begränsad.

Scenario A innebär därför att en viss grundläggande realisering av nyttor ändå kan ske genom:

- viss förbättring av interoperabilitet
- viss klargöring av rättsliga och styrningsrelaterade förutsättningar
- fortsatt användning av traditionella kontroll- och säkerhetsmekanismer

Samtidigt saknas en strukturell kapacitet för införande och användning av PET, vilket innebär att användning av data i känsliga verksamhetsområden i stor utsträckning förblir begränsad.

Nedanstående graf och tabell illustrerar utvecklingen av realiserad nytta samt kostnader över tid i scenario A:



Figur 3: Realisering av nyttopotentialen och kostnader enligt scenario A

År	PET-beroende potential, mdkr	Total potential för datadelning, mdkr	Initial investering (år 0) / löpande kostnad, mdkr
0			0.36
1	0.17	0.70	0.0010
2	0.24	1.11	0.0014
3	0.34	1.71	0.0019
4	0.47	2.55	0.0027
5	0.64	3.58	0.0037
6	0.85	4.73	0.0049
7	1.10	5.85	0.0064
8	1.38	6.83	0.0080
9	1.67	7.63	0.0096
10	1.95	8.24	0.0112

Tabell 12: Realisering av nyttopotentialen, inkl datadelningspotentialen, samt kostnader enligt scenario A

Reflektion: I detta scenario når vi en realiserad nytta på knappt 2 mdkr efter 10 år sedan införandet av PET, vilket är en positiv men relativt blygsam avkastning på satsningen och investeringen.

Utan användning av PET kan omkring en tredjedel av den ekonomiska potentialen av datadelning realiseras genom mer traditionella reformer, såsom förbättrad interoperabilitet,

organisatorisk samordning och rättsliga förtydliganden. Övergången till denna nivå av realisering (d.v.s. från 10 % ➔ 90 %) sker dock relativt långsamt, med en uppskattad tidsperiod på cirka 7–10 år. I ett sådant scenario där *PET inte etableras som en operativ kapacitet* kan däremot endast en mycket liten del (< 10 %) av värdet av datadelning i känsliga verksamhetsområden realiseras. Även denna begränsade realisering sker gradvis, med en uppskattad tid (d.v.s. från 10 % ➔ 90 %) på cirka 10–15 år.

7.5 Scenario B

Prioriterad operativ användning av PET: PET etableras som en fungerande nationell förmåga inom prioriterade områden. Staten tar ett tydligare ansvar för både styrning och teknisk kapacitet. Digg tillhandahåller inte enbart vägledning utan även strukturerat införandestöd, och Skatteverket påbörjar uppbyggnaden av en SMPC-baserad infrastruktur som kan börja användas av flera aktörer. PET används här i ett antal operativa verksamheter och bidrar till påtagliga effektivitetsvinster. PET införs i vissa prioriterade sektorer och användningsfall, vilket möjliggör ökad användning av känsliga data, men utan en bred och systematisk tillämpning i hela offentlig förvaltning.

Detta innebär att en större del av den makroekonomiska potentialen av datadelning kan realiseras än i Scenario A, eftersom vissa hinder kopplade till hantering av känsliga data kan hanteras genom tekniska lösningar.

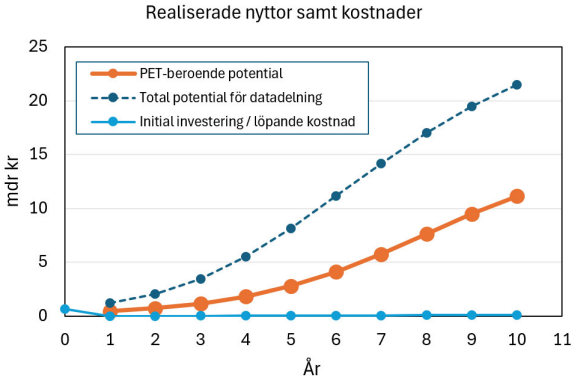
Scenario B innebär därför att en betydande del av nyttorna kan realiseras genom:

- förbättrad interoperabilitet och datastandardisering
- tydligare rättsliga ramar och styrning för datadelning
- införande av PET i utvalda sektorer och användningsfall
- utveckling av pilotprojekt och begränsade produktionsmiljöer för PET

Eftersom användningen av PET fortfarande är selektiv och inte fullt integrerad i offentlig förvaltning, kvarstår dock vissa begränsningar i möjligheten att skala upp datadelning mellan organisationer. Känsliga data kan därför endast i begränsad utsträckning utnyttjas i bredare analys- och beslutsstödssystem.

Detta alternativ kan vi betrakta som ett *realistiskt och trovärdigt scenario*, givet att det överensstämmer väl med utredningens förutsättningar, förslag och ambitioner.

Nedanstående graf och tabell illustrerar utvecklingen av realiserad nytta samt kostnader över tid i scenario B:



Figur 4: Realisering av nyttopotentialen enligt scenario B

År	PET-beroende potential, mdkr	Total potential för datadelning, mdkr	Initial investering (år 0) / löpande kostnad, mdkr
0			0.6245
1	0.45	1.19	0.0042
2	0.72	2.06	0.0067
3	1.16	3.45	0.0108
4	1.82	5.50	0.0169
5	2.78	8.14	0.0259
6	4.10	11.15	0.0382
7	5.76	14.19	0.0536
8	7.63	17.01	0.0710
9	9.49	19.48	0.0884
10	11.15	21.47	0.1038

Tabell 13: Realisering av nyttopotentialen, inkl datadelningspotentialen, samt kostnader enligt scenario B

Reflektion: I detta mer proaktiva scenario når vi en realiserad nytta på ca 11 mdkr efter 10 år sedan införandet av PET, vilket är en realistisk och god avkastning på satsningen och investeringen.

Uppskattning är att omkring hälften till två tredjedelar av den totala potentialen gradvis kan realiseras över tid. Den övergripande utvecklingen i Scenario B sker stegvis genom förbättrad

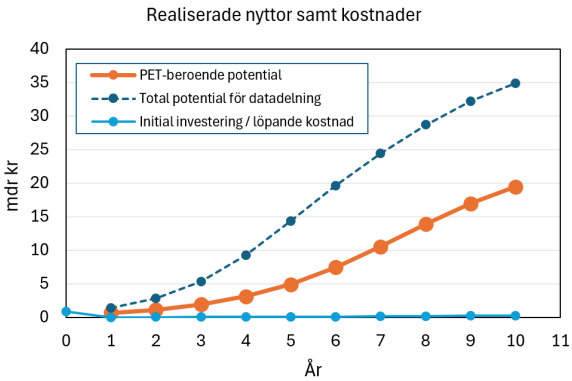
interoperabilitet, tydligare rättsliga ramar och viss organisatorisk anpassning. Övergången till denna nivå av realisering (d.v.s. från 10 % ➔ 90 %) kan därför uppskattas ta cirka 5–8 år. För den del av nyttorna som är direkt beroende av PET bedöms utvecklingen ske långsammare, eftersom införandet fortfarande är selektivt och kräver ytterligare teknisk, organisatorisk och rättslig mognad. Övergången för denna del kan därför uppskattas ta cirka 7–10 år (d.v.s. från 10 % ➔ 90 %).

7.6 Scenario C

Strukturell och systematisk användning av PET: PET etableras som en bred och operativ kapacitet för säker datadelning mellan organisationer, vilket möjliggör en betydande realisering av den makroekonomiska potentialen av datadelning. Scenariot innebär ett strategiskt vägval där PET utgör en integrerad del av offentlig förvaltnings digitala infrastruktur. Användningen är bred, långsiktig och normerande. Såväl vägledning som tekniska tjänster byggs ut för att stödja hela offentlig förvaltning, inklusive kommuner och regioner, och PET används konsekvent i stora reformer och nya system.

Detta innebär att en stor del av den makroekonomiska potentialen av datadelning kan realiseras över tid, eftersom både generella hinder för datadelning och mer specifika hinder kopplade till känsliga data gradvis reduceras. Utvecklingen förutsätter dock fortsatt teknisk uppbyggnad, organisatorisk anpassning, gemensamma standarder och etablerade styrformer, vilket innebär att även detta scenario präglas av en successiv uppskalning över tid.

Nedanstående graf och tabell illustrerar utvecklingen av realiserad nytta samt kostnader över tid i scenario C:



Figur 5: Realisering av nyttopotentialen enligt scenario C

År	PET-beroende potential, mdkr	Total potential för datadelning, mdkr	Initial investering (år 0) / löpande kostnad, mdkr
0			0.889
1	0.66		0.0085
2	1.13	1.42	0.0145
3	1.89	2.79	0.0243
4	3.11	5.30	0.0399
5	4.92	9.27	0.0633
6	7.43	14.36	0.0956
7	10.53	19.63	0.1354
8	13.87	24.47	0.1782
9	16.97	28.71	0.2180
10	19.48	32.23	0.2503

Tabell 14: Realisering av nyttopotentialen, inkl datadelningspotentialen, samt kostnader enligt scenario C

Reflektion: I detta mer framåtlutade scenario når vi en realiserad nytta på knappt 20 mdkr efter 10 år sedan införandet av PET, vilket är en betydande avkastning på satsningen och investeringen.

I detta scenario bedöms en stor del av den ekonomiska potentialen av datadelning kunna realiseras. Sammantaget uppskattas att omkring 80 procent av den totala potentialen kan uppnås på längre sikt, i takt med att både generella förbättringar i interoperabilitet och en bred användning av integritetsskyddande tekniker etableras i offentlig förvaltning.

Den del av potentialen som kan realiseras genom generella förbättringar i interoperabilitet, styrning och rättslig tydlighet bedöms kunna nå en hög nivå inom cirka 4–6 år. För den del av nyttorna som är direkt beroende av PET bedöms utvecklingen ske med viss eftersläpning, och en bred realisering av dessa nyttor kan därför uppskattas ta cirka 6–9 år. Vid slutet av analysperioden bedöms en stor del, men inte hela, den PET-beroende potentialen ha realiserats.

8 Slutsatser och reflektioner

En tydlig bild framträder i vår samlade analys: Potentialen med en ökad användning av integritetsfrämjande tekniker, för förbättrad datadelning, inom offentlig förvaltning överstiger vida de investeringar och kostnader som en sådan satsning innebär, om den görs i tillräcklig omfattning och på ett strukturerat sätt. Det är dock viktigt att poängtera att satsningens omfattning inte får bli alltför begränsad, då finns en stor risk att "nyttotröskeln" aldrig passeras och att de positiva effekterna på det stora hela uteblir. Dock bör man ha en realistisk förväntan *på med vilken hastighet* införandet kan genomföras och därmed hur snabbt de potentiella nyttorna kan realiseras. Vikten av att säkerställa *tillräcklig förmåga och kapacitet*, inte minst för de användande aktörerna, kan inte nog betonas – och här är det primärt organisatoriska, kompetens- och resursrelaterade utmaningar man behöver adressera, snarare än tekniska (även om sådana också existerar).

Det bör också påtalas att det finns stora potentiella nyttor för det *övriga samhället* av en ökad PET-användning (inte enbart för aktörerna inom offentlig förvaltning), t.ex. för medborgare och företag. Här finns en god möjlighet att rättssäkerheten för individen ökar samt att det bidrar till ett mer rättvist samhälle, med exempelvis minskad ekonomisk brottslighet och skattefusk. Ur ett hälsoperspektiv kan PET bidra till förbättrade vårdinsatser, prevention och i slutändan en ökad hälsa för den enskilda individen.

Rapportens analyser bygger på ett stort antal källor och antaganden, och viss osäkerhet kan ej uteslutas, därav uppskattningar uttryckta i spann och med hjälp av tre olika utvecklingsscenarier. Däremot pekar den absoluta merparten av sekundärkällor och studier på att en satsning på PET har en betydande och robust uppsida för såväl de användande aktörerna inom offentlig förvaltning som för medborgarna.

Förutom de potentiella (positiva) nyttorna som vi identifierat så vill vi här slutligen poängtera att användningen av PET inte är riskfri – men det är ofta det minst riskfyllda sättet att uppnå nyttorna med datadelning. Riskerna är hanterbara, men kräver aktiv styrning, juridisk analys, etisk prövning och relevant kompetens kring de olika teknikerna – PET är riskreducerande, inte riskeliminerande.

Slutligen behöver förvaltningen även löpande arbeta med riskhantering, verifiering, kvalitetssäkring och justeringar/anpassningar för att PET ska kunna stödja en rättssäker och ändamålsenlig datadelning där man kan lita på teknikerna och vidtagna åtgärder.

9 Källförteckning

Internationella organisationer

G20/OECD (2024). *Compendium on Data Access and Data Sharing*. Paris: OECD Publishing.

G20 (2021). *Data for Development and Economic Growth.* G20 Information Centre.

International Monetary Fund (IMF). (2021). *Measuring the Economic Value of Data.* IMF Staff Discussion Notes.

International Monetary Fund (IMF) (2025). *Advancing accountability and trust in AI and data-driven public administration*. Washington, DC.

NIST (2023). *Privacy-Enhancing Technologies for Analytics and Data Sharing.*

OECD (2019). *Enhancing Access to and Sharing of Data*. Paris: OECD Publishing.

OECD (2021). *Enhancing Access to and Sharing of Health Data: Reconciling Privacy, Security and Public Interest*. Paris: OECD Publishing.

OECD (2022). *The Economics of Patient Safety*. OECD Health Working Paper No. 145. Paris: OECD Publishing.

OECD (2023). *Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches*. Paris: OECD Publishing.

OECD (2024). *Digital Government Review of Sweden*. Paris: OECD Publishing.

OECD (2025). *Governing with Artificial Intelligence – AI in fighting corruption and promoting public integrity*. Paris: OECD Publishing.

OECD (2019). *Digital Government Review of Sweden.* Paris: OECD Publishing.

OECD (2020). *Health at a Glance: Europe.* Paris: OECD Publishing.

OECD (2022). *The Economics of Public Sector Data.* OECD Digital Economy Papers No. 351.

OECD (2023). *Enhancing Data Sharing in the Public Sector.* OECD Digital Government Studies.

OECD & WHO (2020). *Patient Safety and Systems Performance.* Paris/Geneva.

Office of the National Coordinator for Health IT (2025). *Health Information Exchange – Benefits.*

United Nations Statistics Division (UNSD). (2022). *Privacy-Preserving Techniques for Official Statistics.* UN DESA.

World Economic Forum (WEF). (2021). *Unlocking the Value of Public Sector Data.* Geneva: WEF.

World Economic Forum (WEF) (2023). *The Impact of Privacy-Enhancing Technologies*. Geneva: World Economic Forum.

World Health Organization (WHO) (2020). *Contact Tracing in the Context of COVID-19*. Geneva: WHO.

Europeiska unionen och europeiska organ

ENISA. (2023). *Privacy-Enhancing Technologies in Data Analytics.* European Union Agency for Cybersecurity.

European Commission (2020). *Economic Impact of Open Data*. Luxembourg: Publications Office of the European Union.

European Commission (2022). *Proposal for a European Health Data Space* (COM/2022/197 final).

European Commission (2022). *European Health Data Space – Impact Assessment*. Luxembourg.

European Commission (2025). *My Rights over My Health Data – Primary Use under EHDS*. Brussels.

European Union Agency for Cybersecurity (ENISA) (2023). *Data Protection Engineering for Health Data Spaces*. Athens: ENISA.

European Commission (2022). *Proposal for a Regulation on the European Health Data Space* (EHDS), COM (2022).

European Commission (2024). *European Health Data Space – Implementation Guidance.* Brussels.

European Commission (2020). *European Strategy for Data.* COM (2020).

European Observatory on Health Systems and Policies. (2024). *Health Data Governance in Europe.*

European Union (2016). *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679.

van Drumpt, S., m.fl. (2025). *Secondary use under the European Health Data Space and the role of PET*. *Frontiers in Digital Health*.

Svenska statliga utredningar och regeringsunderlag

Finansdepartementet & Socialdepartementet (2022). *Nationell strategi mot välfärdsbrott.*

SOU 2019:59. *Samlade åtgärder för korrekta utbetalningar från välfärdssystemen*.

SOU 2024:43. *Staten och kommunsektorn – samverkan, självstyrelse och styrning.*

SOU 2025:12. *AI-kommissionens färdplan för Sverige*.

Regeringskansliet (2023–2025). *Underlag rörande inrättandet av Utbetalningsmyndigheten.*

Regeringskansliet (2023). *Nationell strategi för datadelning inom offentlig förvaltning.*

SOU 2024:47. *Digital myndighetspost i offentlig förvaltning.*

SOU 2025:96. *Fler möjligheter till ökat välstånd – Produktivitetskommissionens slutbetänkande.*

Svenska statliga myndigheter

Brottsförebyggande rådet (Brå) (2022). *Välfärdsbrott mot kommuner och regioner – Fel och oegentligheter bland företag och föreningar* (Rapport 2022:1).

Datainspektionen / Integritetsskyddsmyndigheten (IMY) (2023). *Integritetsfrämjande teknik enligt GDPR.*

Digg – Myndigheten för digital förvaltning (2023–2025). *Vägledning för öppna och delade data*.

Digg – Myndigheten för digital förvaltning (2023, 2024), *Uppföljning av statliga myndigheters digitalisering*.

Digg – Myndigheten för digital förvaltning (2024). *Vägledning om Privacy Enhancing Technologies (PET).*

Digg, SKR m.fl. *Samhällsekonomisk analys – Säker digital kommunikation (SDK).*

Ekonomistyrningsverket (ESV) (2022). *Felaktiga utbetalningar i välfärdssystemen.*

Ekonomistyrningsverket (ESV) (2021–2025). *Målet att minska de felaktiga utbetalningarna från välfärdssystemen – måluppfyllelse*.

Folkhälsomyndigheten (2021–2023). *Digital smittspårning och lärdomar från covid-19.*

Folkhälsomyndigheten (2021). *Smittspårning under covid-19 – erfarenheter och lärdomar.*

Integritetsskyddsmyndigheten (IMY) (2022). *AI, hälsodata och dataskydd – rättsliga förutsättningar*.

Riksrevisionen (2020). *Samverkan mellan myndigheter – hinder och möjligheter i individärenden* (RiR 2020:22).

Riksrevisionen (2023). *Subventionerade anställningar – att motverka fel i ett system med allvarliga risker* (RiR 2023:17).

Riksrevisionen (2026). *Ändrade förhållanden – ineffektiv hantering i socialförsäkringen* (RiR 2026:4).

Riksrevisionen (2023). *Statens arbete mot välfärdsbrott.*

Riksrevisionen (2025) *Statliga strategiska digitaliseringsprojekt – stora gemensamma utmaningar* (RiR 2025:8), 29 april 2025.

Socialstyrelsen (2024–2026). *Statistik om hälso- och sjukvård, slutenvård och öppenvård*.

Socialstyrelsen (2024–2026). *Kostnader och resursanvändning i hälso- och sjukvården.*

Statskontoret (2019). *Staten och kommunerna – samverkan för individen*.

Statskontoret (2021). *Felaktiga utbetalningar – omfattning, orsaker och åtgärder.*

Statistiska centralbyrån (SCB). (2024). *Nationalräkenskaper och offentlig konsumtion.*

Strålsäkerhetsmyndigheten (2025). *Fem års rapportering om röntgenstatistik* (SSM 2025:07).

Vetenskapsrådet (2025), *Digitalisering i offentlig sektor: Nyttor, kostnader och mätbarhet.*

Kommuner, regioner och sektorsorganisationer

Region Stockholm (2025). *Kostnad per patient och vårdkontakt (KPP)*.

SKR – Sveriges Kommuner och Regioner (2023–2025). *Kostnad per patient (KPP)* – nationell sammanställning

SKR – Sveriges Kommuner och Regioner (2023). *Kvalitetsbrister i hälso- och sjukvården.*

SKR – Sveriges Kommuner och Regioner (2024). *Nationella kvalitetsregister – kostnader och nyttor.*

SKR & KPMG (2022). *Välfärdsbrottens samhällskostnader*.

SKR & KPMG (2023–2025). *Analyser av välfärdsbrott och automatiserade kontroller* (refererade i ekonomirapporter och remissyttranden).

TechSverige (2022). *Datadelning och tillväxt i offentlig sektor*.

Vårdgivarguiden, Region Stockholm (2025). *Vårdadministration och tidsåtgång*.

Statistik

Statistikmyndigheten SCB (2024). *Forskning och utveckling i Sverige*.

Statistikmyndigheten SCB (2026). *System of Health Accounts (SHA)*.

Karolinska Institutet (2023). *Årsredovisning och forskningsvolymer*.

Vinnova (2023). *Life science-sektorn i Sverige*.

Karolinska Institutet (2024). *FoU-statistik för medicinsk forskning i Sverige.*

SCB (2024). *BNP, offentlig sektor och arbetskraft.*

SKR (2023). *Kommun- och regionkostnader – verksamhetsstatistik.*

Socialstyrelsen (2024). *Slutenvård, vårdtider och vårdrelaterade skador.*

Vetenskapliga studier och forskningslitteratur

Adams, R., et al. (2022). *Prospective clinical evaluation of an AI-based early warning system for sepsis.* The Lancet Digital Health, 4(11), e823–e831.

Al-Na'seh, M. H., et al. (2024). *Optimizing emergency department length of stay and quality of care.* Cureus, 16(10), e71989.

Alotaibi, Y. K., & Federico, F. (2017). *The impact of health information technology on patient safety.* Saudi Medical Journal, 38(12), 1173–1180.

Alvarez-Romero, C., et al. (2022). *Predicting 30-day readmission risk through a federated machine learning architecture.* JMIR Medical Informatics, 10(6), e35307.

Ayer, T., Ayvaci, M. U. S., Karaca, Z., & Vlachy, J. (2019). *The impact of health information exchanges on emergency department length of stay.* Production and Operations Management, 28(3), 740–758.

Ayabakan, S., Bardhan, I., Zheng, Z. E., & Kirksey, K. (2017). *The impact of health information sharing on duplicate testing.* MIS Quarterly, 41(4), 1083–1103.

Bhati, D., Deogade, M. S., & Kanyal, D. (2023). *Improving patient outcomes through effective hospital administration.* Cureus, 15(10), e47731.

Brady, A. P. (2017). *Error and discrepancy in radiology: Inevitable or avoidable?* Insights into Imaging, 8, 171–182.

Chimbo, B., & Motsi, L. (2024). *The effects of electronic health records on medical error reduction.* JMIR Medical Informatics, 12, e54572.

Dhaliwal, J. S., & Dang, A. K. (2024). *Reducing hospital readmissions*. StatPearls.

Durand, M., et al. (2024). *Evaluating the costs of adverse drug events in hospitalized patients.* Health Economics Review, 14, 11.

Escobar, G. J., et al. (2020). *Early detection of sepsis using automated alerts improves outcomes.* BMJ Quality & Safety, 29(6), 459–467.

Geijer, H., & Geijer, M. (2018). *Added value of double reading in diagnostic radiology: A systematic review.* Insights into Imaging, 9(3), 287–301.

Ghabowen, I. K., et al. (2024). *Financial impact of 30-day hospital readmissions.* Healthcare (Basel), 12(7), 750.

Giannini, H. M., et al. (2019). *Use of machine learning to shorten ICU length of stay.* Critical Care Medicine, 47(7), 872–879.

Hirani, R., et al. (2025). *Strategies to reduce hospital length of stay.* Medicina, 61(5), 922.

Holmgren, A. J., et al. (2023). *Health information exchange: Understanding the policy landscape and future of data interoperability.* Yearbook of Medical Informatics, 32(1), 184–194.

Kaissis, G. A., et al. (2020). *Secure, privacy-preserving and federated machine learning in medical imaging.* Nature Machine Intelligence, 2, 305–311.

Kasha, B. A., et al. (2017). *Review of successful hospital readmission reduction strategies and the role of health information exchange.* International Journal of Medical Informatics, 104, 97–104.

Komorowski, M., et al. (2018). *The artificial intelligence clinician learns optimal treatment strategies for sepsis in intensive care.* Nature Medicine, 24(11), 1716–1720.

Komorowski, M., et al. (2018). *Artificial Intelligence in intensive care medicine*. Nature Medicine.

Lacasse, M. L., et al. (2024). *Electronic medical information systems and timeliness of care in the emergency department.* Discover Health Systems, 3, 23.

Luengo-Fernandez, R., Leal, J., Gray, A., et al. (2013). *Economic burden of cancer across the European Union.* The Lancet Oncology, 14(12), 1165–1174.

McKinsey Global Institute (2020). *The next normal in R&D productivity*. McKinsey & Company.

Nuckols, T. K., et al. (2017). *Economic evaluation of quality improvement interventions designed to prevent hospital readmission.* JAMA Internal Medicine, 177(7), 975–985.

Nuckols, T. K., et al. (2014). *Information continuity and patient safety.* Annals of Internal Medicine.

Overhage, J. M., & McCallie, D. (2020). *Physician time spent using the electronic health record.* Annals of Internal Medicine.

Pinevich, Y., et al. (2021). *Interaction time with electronic health records: A systematic review.* Applied Clinical Informatics, 12(4), 788–799.

Ranasinghe, S., et al. (2024). *Calculating the cost of medication errors.* BMJ Open Quality, 13(2), e002570.

Rieke, N., et al. (2020). *The future of digital health with federated learning.* NPJ Digital Medicine, 3, 119.

Rome, B. N., et al. (2020). *Effect of shared electronic health records on duplicate imaging after hospital transfer.* Journal of General Internal Medicine, 35(5), 1617–1619.

Rotenstein, L. S., et al. (2024). *System-level factors and time spent on electronic health records by primary care physicians*. JAMA Network Open, 6(11).

Rotenstein, L. S., et al. (2022). *Administrative burden and clinician productivity*. Health Affairs.

Rosenkrantz, A. B., et al. (2018). *Discrepancy rates and clinical impact of imaging secondary interpretations.* Journal of the American College of Radiology, 15(9), 1222–1231.

Royal Society. (2023). *Privacy-Enhancing Technologies: Principles and Practice*. London.

Sergi, C. M. (2024). *Medical errors can cost lives.* Archives of Medical Science, 20(4), 1378–1383.

Steinkamp, J., Kantrowitz, J. J., & Airan-Javia, S. (2022). *Prevalence and sources of duplicate information in the electronic medical record.* JAMA Network Open, 5(9), e2233348.

Taylor, K., & Davidson, P. M. (2021). *Readmission to the hospital: Common, complex and costly.* Journal of Clinical Nursing, 30, e56–e59.

Vest, J. R., et al. (2015). *The potential for community-based health information exchange systems to reduce hospital readmissions.* Journal of the American Medical Informatics Association, 22(2), 435–442.

Vest, J. R., et al. (2021). *Health Information Exchange and Clinical Outcomes*. Journal of the American Medical Informatics Association.

Waite, S., et al. (2017). *Interpretive error in radiology*. American Journal of Roentgenology, 208, 739–749.

Wang, Y., et al. (2026). Enh*ancing hospital workforce planning, scheduling and performance evaluation*. Scientific Reports.

Policyanalys och andra analyser

McKinsey Global Institute (2020). *The next normal in R&D productivity.*

DAMVAD Analytics & Lantmäteriet (2019). *The Economic Value of Open and Shared Data in Sweden.*

EIT Health & Swedish Medtech (2023). *Implementing the European Health Data Space in Sweden.*

IQVIA & Oxford University (2025). *European Health Data Space – data reuse guide.*

Statens offentliga utredningar 2026

Kronologisk förteckning

1. Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. Fi.
2. 710 miljoner skäl till reformer. Ju.
3. Genomförande av plattformsdirektivet. A.
4. Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. U.
5. Utvidgad avdragsrätt för sponsring m.m. Fi.
6. En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. S.
7. Förstärkt uppföljning och utvärdering av folkhälsopolitiken.
   Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser.
   Del II: Utvärdering av alkoholpolitikens styrmedel. S.
8. Rättssäker samhällsvård för barn och unga. S.
9. Registrering av EES-medborgare. Ju.
10. Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. Ju.
11. Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. Fi.
12. Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. Fi.
13. Straffansvar för deltagande i och samröre med kriminella sammanslutningar. Ju.
14. Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. KN.
15. Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. Ku.
16. Försvarsexportinitiativ. För gemensam säkerhet. Fö.
17. Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. LI.
18. Odlingstorv och klimatet. Fi.
19. Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. S.
20. Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. Fi.
21. Återkallelse av svenskt medborgarskap. Ju.
22. Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. S.
23. Tolkavgift och förbud mot barntolkning. A.
24. Mervärdesskatt vid uthyrning och överlåtelse av fastighet. Fi.
25. Ett smittskydd för framtiden. S.
26. Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. Ju.
27. Lättnader i kraven på hållbarhetsrapportering. Ju.
28. Tillgång till passageraruppgifter i brottsbekämpningen. Ju.
29. Förbud mot uppfödning av djur för pälsproduktion. LI.
30. Mer flexibla regler om verkställighet av häktning och fängelsestraff. Ju.
31. Ett investeringsprogram för kultur. Ku.
32. Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. KN.
33. Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. KN.

34. Nya nätbrott och andra åtgärder för genomförandet av direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Volym 1 & 2. Ju.
35. En åldersgräns för barns tillgång till sociala medier. S.
36. Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. S.
37. Förutsättningar för en likvärdig och språkutvecklande förskola. U.
38. Behovsstyrd vård. S.
39. Ett nytt system för återkrav inom socialförsäkringen. S.
40. Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. KN.
41. Jämställdhet i en föränderlig tid – nuläge och vägar framåt. Volym 1 & 2. A.
42. Ett nytt regelverk för granskning av utländsk finansiering av trossamfund och andra verksamheter. Volym 1 och 2. Ju.
43. Åtgärder mot överskuldsättning. Fi.
44. En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning. Fi.

Statens offentliga utredningar 2026

Systematisk förteckning

Arbetsmarknadsdepartementet

Genomförande av plattformsdirektivet. [3]

Tolkavgift och förbud mot barntolkning. [23]

Jämställdhet i en föränderlig tid – nuläge och vägar framåt. Volym 1 & 2. [41]

Finansdepartementet

Skatteincitament för forskning och utveckling – ett nytt incitament baserat på utgifter för FoU-personal. [1]

Utvidgad avdragsrätt för sponsring m.m. [5]

Om överföring av Första AP-fondens verksamhet och tillgångar till Tredje och Fjärde AP-fonderna. [11]

Om överföring av Sjätte AP-fondens verksamhet och tillgångar till Andra AP-fonden. [12]

Odlingstorv och klimatet. [18]

Belägg för broms? Åtgärder för starkare incitament till lägre kommunalskattesatser. [20]

Mervärdesskatt vid uthyrning och överlåtelse av fastighet. [24]

Åtgärder mot överskuldsättning. [43]

En stärkt förmåga till modern datadelning – integritetsfrämjande teknik i offentlig förvaltning. [44]

Försvarsdepartementet

Försvarsexportinitiativ. För gemensam säkerhet. [16]

Justitiedepartementet

710 miljoner skäl till reformer. [2]

Registrering av EES-medborgare. [9]

Ökade möjligheter till tillgångsinriktad brottsbekämpning. Del 1 och 2. [10]

Straffansvar för deltagande i och samröre med kriminella sammanslutningar. [13]

Återkallelse av svenskt medborgarskap. [21]

Digitala verktyg inom bolagsrätten. Genomförande av EU:s direktiv om ytterligare digitalisering inom bolagsrätten. [26]

Lättnader i kraven på hållbarhetsrapportering. [27]

Tillgång till passageraruppgifter i brottsbekämpningen. [28]

Mer flexibla regler om verkställighet av häktning och fängelsestraff. [30]

Nya nätbrott och andra åtgärder för genomförandet av direktivet om bekämpning av våld mot kvinnor och våld i nära relationer. Volym 1 & 2. [34]

Ett nytt regelverk för granskning av utländsk finansiering av trossamfund och andra verksamheter. Volym 1 och 2. [42]

Klimat- och näringslivsdepartementet

Ädelmetallutredningen – en moderniserad reglering av handel med ädelmetallarbeten. [14]

Att säga ja! Kommunernas förutsättningar att ta emot stora företagsetableringar och företagsexpansioner. [32]

Vägen mot utfasning. Styrmedel för ett fossilfritt samhälle. [33]

Ny kärnkraft i Sverige – moderna regler för beredskap och skadeståndsansvar. [40]

Kulturdepartementet

Marken, vattnet, tankarna. Konsekvenser för samer av svensk politik. Volym 1 och 2. [15]

Ett investeringsprogram för kultur. [31]

Landsbygds- och infrastrukturdepartementet

Öresundsförbindelser 2050 – behov av kapacitet, redundans och svenskt-danskt samarbete. [17]

Förbud mot uppfödning av djur för pälsproduktion. [29]

Socialdepartementet

En nationell digital infrastruktur i hälso- och sjukvården. Styrning med tydliga roller och ansvar för aktörerna. [6]

Förstärkt uppföljning och utvärdering av folkhälsopolitiken.
Del I: Effektivare folkhälsoinsatser genom hälsoekonomiska analyser.
Del II: Utvärdering av alkoholpolitikens styrmedel. [7]

Rättssäker samhällsvård för barn och unga. [8]

Stärkt tillsyn och uppföljning – förslag för att motverka oegentlig läkemedelsförskrivning. [19]

Stärkt läkemedelsförsörjning i samverkan. Nationella åtgärder för fördelning, omfördelning och inköp vid brist. [22]

Ett smittskydd för framtiden. [25]

En åldersgräns för barns tillgång till sociala medier. [35]

Bättre förutsättningar att inkludera personer med nedsatt beslutsförmåga i medicinsk forskning. [36]

Behovsstyrd vård. [38]

Ett nytt system för återkrav inom socialförsäkringen. [39]

Utbildningsdepartementet

Rektor i fokus – förutsättningar för ett pedagogiskt ledarskap. [4]

Förutsättningar för en likvärdig och språkutvecklande förskola. [37]