TIERPS KOMMUN

Dokumentnamn
Remissvar

Datum
2024-10-23

Diarienummer
KS/2024:988

Svar på remiss - Sekretess och dataskydd i det tekniska systemet enligt EU:s förordning om en gemensam digital ingång

Inledning

Vi ser positivt på ambitionen att genomföra EU förordning om en gemensam digital ingång (SDG-förordningen) och skapa ett automatiserat system för gränsöverskridande bevisutbyte mellan medlemsstaterna. Ett sådant system kommer sannolikt underlätta för både medborgare och organisationer i hanteringen av gränsöverskridande ärenden, vilket ligger i linje med principerna för EU:s inre marknad och den nationella strategin för digitalisering.
Samtidigt medför implementeringen av SDG-förordningen betydande utmaningar för kommunala verksamheter i Sverige, särskilt med avseende på informationssäkerhet, dataskydd och hanteringen av uppgifter som omfattas av sekretess. På området informationssäkerhet, cybersäkerhet, och dataskydd pågår samtidigt ett omfattande arbete med anledning av andra lagar som skärper kraven på säkerhet. SDG-förordningens och promemorians innehåll att påbörja en omfattande informationsdelning trots att detta säkerhetsarbete i många kommuner inte är färdigt är bakvänt, och riskerar att flytta resurser från säkerhetsarbetet till implementering av lösningar som inte är genomtänkta eller säkra.

Nedan beskrivs ett antal problemområden där vi skulle önska ytterligare klargöranden och åtgärder. Vi ser även ett behov av en längre övergångsperiod för att ge kommuner och andra berörda organisationer tid att anpassa sina rutiner och tekniska system.

Omfattningen av uppgifter

SDG-förordningen innebär att kommunerna kan behöva lämna ut en omfattande mängd uppgifter, såsom:

- Examensbevis och betyg
- Intyg om bosättning och adresshistorik
- Information om ekonomiskt bistånd och sociala förmåner
- Information om bygglov och fastighetsinformation
- Företagsregistreringar och tillstånd för näringsverksamhet

Mängden och variationen av dessa uppgifter ställer stora krav på kommunernas förmåga. Det är helt centralt att kommunerna får stöd i att möta denna nya börda utan att riskera brister i hanteringen. I Sverige finns 290 kommuner, och omfattningen av vilken information som både inhämtas och delas torde kunna samordnas på ett mer effektivt och tydligt sätt än vad som finns tillgängligt idag. Vi efterfrågar att mer detaljerade riktlinjer tas fram för hur mängden uppgifter ska hanteras och skyddas.

Otydligheter i ansvarsfördelning rörande informationssäkerhet och dataskydd

Promemorian berör inte i tillräcklig grad ansvarsfördelningen mellan de olika aktörerna och hanteringen av sekretessbelagd information. Enligt promemorian ska Myndigheten för digital förvaltning (DIGG) förvalta det tekniska systemet, medan kommuner och andra myndigheter ansvarar för att lämna ut bevis och följa nationella regler om sekretess.

Enligt dataskyddsförordningen är den som bestämmer ändamål och medel för personuppgiftsbehandlingen den personuppgiftsansvarige. Om kommunerna själva fattar beslut om hur uppgifterna ska delas och behandlas i systemet, kan de betraktas som personuppgiftsansvariga. Om DIGG däremot styr hur behandlingen sker och kontrollerar villkoren, kan kommunerna istället komma att anses agera i egenskap av personuppgiftsbiträde. Det här skapar en oklarhet om vem som egentligen är ansvarig, och riskerar därmed också en följdproblematik vid incidenter eller anspråk från medborgarna gällande deras fri- och rättigheter.

Vid en personuppgiftssincident kan exempelvis ansvaret för att rapportera incidenten till tillsynsmyndighet, informera de registrerade, och vidta åtgärder bli otydligt. Om ansvaret är oklart uppstår risken att ingen tar fullt ansvar, vilket kan försvaga skyddet för de registrerade och leda till oförutsedda konsekvenser, vilket kan inkludera rättsliga problemställningar för kommunerna.

Vi önskar därför att ansvarsfördelningen mellan DIGG och kommunerna klargörs vad gäller ansvarsfrågan. Kommuner bör även få tillgång till vägledning om hur man bör hantera incidenter och överträdelser som sker inom ramen för SDG-förordningen.

Tidsramen för implementering

Promemorian föreslår att de nya reglerna ska träda i kraft den 15 februari 2025 och därmed bli operativa i verksamheterna. Detta innebär att kommunerna har extremt lite tid på sig att förbereda och implementera nödvändiga förändringar. Förordningen ska implementeras samtidigt som ett antal andra lagar som innebär ett förändrat arbetssätt och krav på informationshantering och informationssäkerhet skärps.

Åtgärderna innefattar bland annat att upprätta styrdokument och ledningssystem, uppdatera tekniska plattformar och system, genomföra

informationskartläggning och klassning, införa verksamhetsspecifika rutiner, samt utbilda personal inom informationssäkerhet, sekretess och dataskydd, samt förstå och bedöma hanteringen av internationella förfrågningar och informationsutbytet.

Detta innebär en stor utmaning med tanke på att många kommuner har begränsade resurser. Vi anser att tidsramen är orealistiskt kort och riskerar att leda till brister i både informationssäkerhet och efterlevnad av sekretessregler. För att säkerställa en säker och effektiv implementering föreslår vi därför att tidsramen förlängs. Alternativt bör man överväga ett etappvis införande, där kommuner gradvis kan anpassa sina system och rutiner. Ett pilotprojekt där ett mindre antal kommuner och myndigheter får implementera systemet tidigt skulle kunna ge värdefulla insikter inför ett fullskaligt införande.

Säkerhetsrisker vid gränsöverskridande informationsutbyte
Automatiskt utbyte över nationsgränser innebär risker. Promemorian nämner inte i någon detaljerad utsträckning hur krav på säkerhetsåtgärder ska tillses. Det här är avgörande för att säkerställa att informationens riktighet och konfidentialitet upprätthålls vid överföring. Tidigare erfarenheter från system som IMI och Schengens informationssystem (SIS) visar att en gemensam säkerhetsstandard och process för incidenthantering är nödvändiga för att minimera säkerhetsbrister.

Vi föreslår härav inkluderade krav på en gemensam standard, och åtgärder som kryptering, autentisering och loggning. Som nämnt i stycke Det är också centralt att etablera en tydlig process för incidentrapportering och hantering av säkerhetsincidenter som berör systemet.

Otillräcklig analys av kostnader och resursbehov
Promemorian ger ingen tillfredställande analys av de ekonomiska och resursmässiga konsekvenserna för kommunerna och skillnaderna i förutsättningar. Som nämnt i stycke 2 behöver kommuner genomföra en omfattande mängd förändringar för att kunna möta förordningen, vilket även inkluderar ett omfattande förberedande analysarbete. Detta medför betydande kostnader, särskilt för mindre kommuner med begränsade resurser. Promemorians förslag saknar konsekvensanalys, och en specifikation över vilka kostnader som förväntas, samt vilken typ av statligt stöd som kan tillhandahållas.

Slutsats
Vi ser potential i SDG-förordningens ambition att underlätta gränsöverskridande informationsutbyte, men anser att de föreslagna åtgärderna inte är tillräckligt anpassade för kommunernas specifika förutsättningar i nuläget. Tidsramarna är korta, ansvarsfördelningen oklar, det finns brister i nationell samordning och de säkerhetsrelaterade riskerna är betydande, särskilt i fråga om hanteringen information som omgärdas av

konfidentialitet. Förslagen kolliderar dessutom med den förstärkning av informations- och cybersäkerhetsarbete som pågår inom kommunerna.

Vi önskar därför förlängning av den tidsram som promemorian föreslår.

För kommunstyrelsen,

Andreas Bäckström
Informationssäkerhetssamordnare
Ledningsstöd