

Stockholm den 17 december 2020

ASF\_MATTER\_ID

Till Infrastrukturdepartementet

I2020/02346

Sveriges advokatsamfund har genom remiss den 24 september 2020 beretts tillfälle att avge yttrande över betänkandet Innovation genom information (SOU 2020:55).

### **Sammanfattning**

Advokatsamfundet avstyrker förslaget med den motivering som framgår av nedan angivna kommentarer.

### **Allmänt**

Implementering av Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (omarbetning) (nedan öppna data-direktivet) på det sätt som föreslås i betänkandet kan innebära betydande risker för enskildas fri- och rättigheter, framför allt rätten till integritet. Advokatsamfundet anser att betänkandet inte i tillräcklig utsträckning tillvaratar integritetsfrågorna utifrån de möjligheter som ges i direktivet. Vidare anser Advokatsamfundet att den valda lagstiftningstekniken har brister, att vissa begrepp är otydliga samt att det finns skäl att se över hur lagförslaget påverkar de nya handlingarna och uppgifterna som skapats och skapas med anledning av den innovation genom digitalisering som skett de senaste decennierna och alltjämt pågår.

### **Särskilda hanteringskrav enligt lagförslaget**

Lagförslaget, lag (2021:000) om öppna data och vidareutnyttjande av information från myndigheter och offentliga företag (nedan öppna datalagen), innebär kodifiering av särskilda hanteringskrav kopplat till personuppgifter. Dessa krav riskerar att tillämpas i strid med 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 (nedan GDPR). De särskilda hanteringskraven ger sken av att det kan finnas rättslig grund för tillgängliggörande av personuppgifter med stöd av öppna datalagen och att finalitetsprincipen inte ska tillämpas. I skäl 52 i öppna data-direktivet framgår dock att

direktivet inte ska påverka skyddet för enskildas personuppgifter. Där nämns särskilt att principen om ändamålsbegränsning enligt 5.1.b GDPR och rättslig grund enligt artikel 6 GDPR ska beaktas.

Det bör noteras att öppna data-direktivet inte ska ses som *lex specialis* i förhållande till GDPR, varför det inte sätter GDPR ur spel. GDPR gäller således fullt ut och parallellt med öppna data-direktivet. Det sätt som valts för att reglera dataskyddsfrågor i öppna datalagen innebär dock att det kan uppfattas som *lex specialis*.

På s. 151 i betänkandet anges att problemet med finalitetsprincipen enligt artikel 5.1.b GDPR inte ska överskattas. Denna slutsats kan ifrågasättas. Samtliga de grundläggande principerna för personuppgiftsbehandling i GDPR bör tas på allvar för att bevara intentionerna med såväl öppna data-direktivet som GDPR. Vidareutnyttjanden som omfattar personuppgiftsbehandling måste följa dessa grundläggande principer. I denna del kan framhållas att artikel 86 GDPR möjliggör utlämnanden enligt 2 kap. TF, med den begränsning som finns i 21 kap. 7 § offentlighets- och sekretesslagen (2009:400), enligt vilken sekretess gäller för personuppgift om det kan antas att uppgiften efter ett utlämnande kommer behandlas i strid med GDPR. Dock saknas motsvarande reglering för vidareutnyttjanden enligt öppna data-direktivet. GDPR och annan dataskyddslagstiftning måste således följas fullt ut vid sådant vidareutnyttjande. Därutöver vill Advokatsamfundet lyfta fram att avsikten med öppna data-direktivet är att den personliga integriteten inte ska äventyras eller påverkas.

Vidare bör uppmärksammas att den personuppgiftsbehandling som genomförs för att anonymisera personuppgifter enligt tillämplig lagstiftning även den betraktas som personuppgiftsbehandling och behöver följa de grundläggande principerna samt ha en rättslig grund enligt GDPR. Dvs. även den möjlighet till skydd genom anonymisering som lyfts fram i betänkandet, och som framgår av skäl 52 i öppna data-direktivet, kräver rättslig grund för personuppgiftsbehandlingen.

Såvitt avser de särskilda hanteringskraven i förslaget till öppna datalagen, bör det övervägas om de materiellt tillför adekvata regleringar och förtydliganden eller riskerar skapa tillämpningssvårigheter. Detta med hänsyn till att öppna data-direktivet, och därigenom öppna datalagen, inte får implementeras, eller tillämpas, på ett sådant sätt att den personliga integriteten påverkas (jfr skäl 52 samt 71 i öppna data-direktivet). Med de särskilda hanteringskraven avses reglering vad gäller personuppgiftshantering i 2 kap. 1 § och 4 kap. 6 § i förslaget till öppna datalagen. Med föreslagna bestämmelser och formuleringar finns en risk för tolkning innebärande att det enbart är de prövningar som framgår av paragraferna som är nödvändiga att genomföra. Verksamheter som prövar frågor om vidareutnyttjande kan därmed missa att pröva om det t.ex. finns en rättslig grund för personuppgiftsbehandlingen i GDPR eller om vidareutnyttjandet är förenligt med finalitetsprincipen. Advokatsamfundet anser att det bör övervägas om 4 kap. 6 § i förslaget ska tas bort. Dessutom riskerar formuleringen i 2 kap. 1 § öppna datalagen förleda tillämpare att tro att GDPR inte blir något problem utifrån öppna data-direktivet. Paragrafen bör därför i stället formuleras som en upplysningsbestämmelse.

Att tillgängliggörande i första hand ska ske digitalt (se 2 kap. 2 § och 3 kap. 2 § öppna datalagen) går längre än öppna data-direktivet, där det anges att handlingar ska tillgängliggöras digitalt om möjligt (jfr 5.1 öppna data-direktivet). Denna starkare presumtion för digitalt tillgängliggörande medför ytterligare risker för konflikt med GDPR.

### **Syftesparagrafen**

Utifrån vad som anges ovan anser Advokatsamfundet att personuppgiftsskyddet bör stärkas genom att det redan i den bestämmelse som avser lagstiftningens syfte anges att lagen inte får tillämpas i strid med gällande personuppgiftslagstiftning. Det bör där förtydligas att lagen inte påverkar rätten till integritet enligt GDPR och anknytande nationell rätt vid sidan om att Sveriges säkerhet m.m. ska beaktas. Utöver detta bör lagen kompletteras på så sätt att det i 1 kap. 4 § tillförs undantag motsvarande de i artikel 1.2. h öppna data-direktivet för att på ett ändamålsenligt sätt skydda integriteten för enskilda i linje med direktivets avsikt.

### **Särskilda överväganden i förhållande till sekretesslagstiftningen**

Advokatsamfundet vill även peka på att det kommer finnas fall där vidareutnyttjande av personuppgifter är lämpligt och kan ske lagligt med respekt för enskildas integritet. Den snabba digitala utvecklingen, och den föreslagna lagstiftningen, gör att fler handlingar och uppgifter från myndigheter kommer bli tillgängliga för intresserade parter.

Advokatsamfundet vill därför i detta sammanhang – där avsikten är att fler uppgifter som hanteras av myndigheter och offentliga bolag ska bli tillgängliga – framhålla att det finns skäl att göra en större översyn av vilka uppgifter som ska vara sekretessbelagda med hänsyn till skyddet för såväl enskildas som bolags intressen, och framför allt enskildas legitima intresse av att deras personuppgifter skyddas. Nuvarande sekretesslagstiftning innehåller luckor som ger möjlighet att göra stora datainsamlingar på ett integritetskränkande sätt med stöd av offentlighetsprincipen. Detta är en följd av en teknisk utveckling där myndigheter och offentliga bolag skapar nya typer av handlingar som inte omfattas av sekretess inom ramen för såväl verksamhetsutveckling som digitalisering av ärendeprocesser, men även av att tekniken ökat enkelheten i att begära ut och bearbeta handlingar. Det ska i sammanhanget även pekas på de möjligheter som finns för personuppgiftsbehandling på integritetskränkande sätt genom frivilliga utgivningsbevis. Advokatsamfundet anser det sannolikt att en större tillgång till uppgifter genom öppna datalagen ökar problematiken kopplad till offentlighet för information om enskilda från myndigheter och offentliga bolag. Risken är således att kommersiella intressen kommer kunna skapa fler integritetskränkande sammanställningar av personuppgifter om lagförslagen införs.

## Definitioner och begrepp

Det bör övervägas om det till uppräknigen i 1 kap. 5 § öppna datalagen ska läggas till definitioner avseende personuppgiftsbehandling, bl.a. definition av vad en personuppgift är genom hänvisning till de legaldefinitioner som finns i GDPR.

Informationssäkerhet definieras normalt som skyddet av information och bevarandet av:

- Konfidentialitet
- Riktighet
- Tillgänglighet

Advokatsamfundet anser från dessa utgångspunkter det svårt att förstå vad som avses med begreppet "Sveriges ... informationssäkerhet i övrigt" som återkommer på flera ställen i lagförslaget. Såvitt Advokatsamfundet känner till finns ingen legaldefinition av detta begrepp, och någon annan tydlig förklaring finns inte heller i betänkandet. Om begreppet innebär att konfidentialiteten i uppgifter inte får äventyras bör detta förtydligas. Vad som anges i avsnitt 17.5.4 om informationssäkerhet bidrar inte till tillräcklig klarhet.

Genom att använda begreppet information i stället för handling (jfr implementeringen av PSI-direktivet genom PSI-lagen) förhindras att lagstiftningen blir allt för vidsträckt, vilket är gynnsamt för integritetsskyddet. Det kan emellertid samtidigt leda till viss förvirring när någon begär vidareutnyttjande av information som samtidigt är en del av en allmän handling. Detta kan, om man inte är noggrann vid rättstillämpningen, leda till att regelverken i öppna datalagen och offentlighetsprincipen förväxlas.

## Tillsyn

Vad gäller tillsynsfrågan instämmer Advokatsamfundet att det inte har framkommit behov av en särskild tillsynsmyndighet för att säkerställa att den nya lagen följs.

Advokatsamfundet erinrar dock om att andra tillsynsmyndigheter kan komma att granska ärenden där lagstiftningen är tillämplig, t.ex. JO, Datainspektionen och ev. myndigheter för särskild sektortillsyn så som IVO, SÄPO, Läkemedelsverket etc., beroende på vilken typ av uppgifter som gjorts tillgängliga.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander