

Stockholm den 12 januari 2024

R-2023/2130

Till Justitiedepartementet

Ju2023/02434

Sveriges advokatsamfund har genom remiss den 31 oktober 2023 beretts tillfälle att yttra sig över betänkandet Ökat informationsflöde till brottsbekämpningen – en ny huvudregel (SOU 2023:69).

Sammanfattning

Utredningens uppdrag har varit att lämna förslag på förbättrade möjligheter till informationsutbyte mellan brottsbekämpande myndigheter och vissa andra statliga och kommunala myndigheter samt ett stort antal enskilda aktörer inom ett flertal olika områden.

Advokatsamfundet anser inte att utredningen visar att samhällets intressen står i rimlig proportion till de omfattande inskränkningar i den enskildes rätt som förslagen innebär. Advokatsamfundet får därför, med hänvisning till de synpunkter som framförs i detta remissyttrande, avstyrka lagförslaget i dess helhet.

Synpunkter

Generella synpunkter

Advokatsamfundet har förståelse för de intressen som ligger bakom utredningens förslag och anser att det är av stor vikt att motverka och beivra kriminalitet. Samtidigt är det viktigt att reglerna ges en utformning och ett innehåll som inte skapar oförutsebarhet eller går för långt vad gäller intrång i den personliga integriteten.



Advokatsamfundet finner att införande av regler av aktuellt slag innebär en risk för ändamålsglidning när uppgifter ska börja behandlas för andra ändamål än vad som har varit avsett initialt. Reglerna kommer även att medföra att ytterligare myndigheter, och därmed fler personer, får tillgång till dem, vilket i sig innebär ökade risker.

För att nå ett rimligt hänsynstagande till de olika intressena är det nödvändigt att uppställa principer för när ett informationsutbyte kan ske och att det finns skyddsåtgärder jämte kontrollmekanismer som ger enskilda praktiska möjligheter att tillvarata sina rättigheter på ett sådant sätt att grundlagens och Europakonventionens skydd inte minskar. Advokatsamfundet får därför särskilt uppmärksamma om risken för att ett utökat utbyte av information kan komma i konflikt med grundlagsskyddet i 2 kap. 6 § regeringsformen.¹

Bestämmelserna får enligt regeringsformen inte utformas på ett sätt eller ges ett sådant innehåll som är oförenligt med legalitetsprincipen. Bestämmelserna får inte heller ges ett sådant innehåll som åsidosätter proportionalitetsprincipen så att det går alltför långt i förhållande till de ändamål som ska uppfyllas och som samtidigt är godtagbara i ett demokratiskt samhälle.² Advokatsamfundet finner att utredningens förslag i angivet hänseende har gått för långt. I dess förlängning innebär förslaget stora risker för att enskilda inte längre kommer att våga kontakta de aktörer, till exempel inom socialtjänsten och vården, som de har behov av att anlita, när det inte kan förutses till vem uppgifterna kommer att röjas. Noteras kan också särskilt att en ökad informationsskyldighet från aktörer som t.ex. skola och socialtjänst inte tillräckligt har analyserats ur ett barnperspektiv.

Synpunkter på utredningens förslag, sekretess och tystnadsplikten m.m.

Advokatsamfundet vill särskilt uppmärksamma frågan om sekretess för olika uppgifter som ingår i informationen och tystnadsplikt såvitt avser de privata aktörerna som åläggs att lämna information till de brottsbekämpande myndigheterna. Vissa slags uppgifter har högre skyddsvärde än andra och omfattas därför av olika bestämmelser i offentlighets- och sekretesslagen (OSL) med särskilda högre sekretesskrav och motsvarande gäller för de privata aktörerna med deras regelverk om tystnadsplikt. Advokatsamfundet får därför framhålla behovet av särskild försiktighet när det blir

¹ Se även artiklarna 7 och 8 Europeiska Unionens stadga om de grundläggande rättigheterna

² Angående legalitetsprincipen, se 1 kap. 1 § st.3, 2 kap. 10 § RF, samt prop. 2016/17:180 s. 57 ff., se även 5 § st.1 förvaltningslagen (2017:900). Angående proportionalitetsprincipen, se 2 kap. 21 § RF.



fråga om informationsutbyte där uppgifter ingår som omfattas av ett särskilt starkt sekretesskydd och där kravet på tydlighet och förutsebarhet måste anses extra angeläget.

Enligt förslagen ska uppgiften som omfattas av sekretess och tystnadsplikt lämnas ut om det inte är *olämpligt*. Det går inte att utläsa i vilka situationer som ett utlämnande är att anse som olämpligt. Detta utvidgar utrymmet för utlämnande på ett oförutsebart sätt som går för långt. Något beaktande av vad som ska uppnås med utlämnandet synes inte vägas in i bedömningen. För att sekretess och tystnadsplikt ska få brytas bör rimligen krävas att skälet och syftet har betydelse för prövningen. Detta bör förtydligas i den fortsatta beredningen.

Behandling av personuppgifter

Uppgifterna kommer därtill bestå i personuppgifter enligt den Europeiska unionens (EU) förordning 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) (GDPR). Personuppgifterna kan även omfattas av kompletterande dataskyddsregler, exempelvis i brottsdatalagen, de särskilda brottsdatalagar som gäller specifikt för berörd brottsbekämpande myndighet eller annan särskild registerlagstiftning som gäller för berörd myndighet eller för den privata aktören som tvingas lämna ut uppgifter till de brottsbekämpande myndigheterna.

Förslagen om införandet av bestämmelser om informationsutbyte mellan de olika aktörerna kommer oundvikligen att innebära en behandling av personuppgifter som ska ske för andra ändamål än vad som gällt från början. Detta föranleder enligt Advokatsamfundet noggranna överväganden om ett informationsutbyte kan strida mot de olika regelverken om behandling av personuppgifter.

Advokatsamfundet får särskilt framhålla att även informationsutbytet mellan myndigheterna och vissa privata aktörer kommer att utgöra behandling av personuppgifter. Detta innebär att utbytet måste uppfylla de grundläggande principerna i GDPR och att det även måste finnas en rättslig grund för behandlingen.³

³ Artikel 5, 6, 9 och 10 GDPR.



Det bör därför bli aktuellt för myndigheterna och de privata aktörerna som omfattas av förslagen att anskaffa olika informationssystem och tjänster för att möjliggöra att informationsutbytet sker i enlighet med GDPR.

Dessa system och tjänster måste uppfylla kraven i GDPR på en ”lämplig” säkerhetsnivå.⁴ Uppgifter om enskilda personer som förekommer inom de många områden där utlämnade föreslås utgör typiskt sett känsliga personuppgifter enligt GDPR och omfattas även av sekretess och tystnadsplikt med omvänt skaderekvisit. Detta föranleder att säkerhetsfrågorna måste bli föremål för särskilda och noggranna överväganden, en aspekt som borde ha fått ökad fokus i utredningens arbete.

Behandlingen och informationsutbytet kommer att involvera olika aktörer. Detta aktualiserar frågor om vem av de olika aktörerna som ska anses vara personuppgiftsansvarig och vem som är personuppgiftsbiträde.⁵ Detta kan i sin tur medföra att det måste åstadkommas personuppgiftsbiträdesavtal mellan den som är personuppgiftsansvarig för behandlingen och den som eventuellt anlitas för genomförandet av åtgärderna och behandlingen.⁶ Vid ett mer utvecklat utbyte av personuppgifter mellan myndigheter, och även vissa privata aktörer, kan det bli oklart vem som egentligen står för bestämmandet över ändamål och medel för behandlingen. Detta kan få till följd att ett samordnat ansvar anses föreligga enligt artikel 26 GDPR, vilket kan leda till oförutsedda och oönskade effekter vad gäller ansvarsfördelningen mellan myndigheterna. Advokatsamfundet anser att dessa frågeställningar förtjänar ytterligare uppmärksamhet.

Olika regelverk lämnar utrymme för behandling av personuppgifter för sekundära ändamål, som kan bestå i andra ändamål för behandlingen än de ursprungliga. Även sådan behandling kan anses tillåten om det nya ändamålet har stöd i annan lag och inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

Advokatsamfundet ställer sig principiellt tveksamt till sådana sekundära ändamål och känner oro för att deras generella utformning kan legitimera godtycke hos myndigheterna och de privata aktörerna som omfattas av förslagen. Eftersom det blir svårt att förutse vilka nya ändamål personuppgifterna skulle kunna komma att

⁴ Artikel 32 GDPR.

⁵ Artikel 4.7 och 4.8 GDPR.

⁶ Artikel 28 GDPR.



användas för uppstår även problem med legalitetsprincipen. Det förordas därför en uttrycklig och tydligare hänvisning till de ytterligare ändamål som skulle kunna komma i fråga, så att de registrerade ges en rimlig chans att kunna förutse för vilka ändamål uppgifterna kan behandlas.

Därtill finner Advokatsamfundet att utredningen inte ger finalitetsprincipen tillräcklig vikt och att risken för ändamålsglidning underskattats. Det saknas en egentlig analys avseende i vilken omfattning uppgifter kommer att bli tillgängliga för ytterligare myndigheter genom de föreslagna bestämmelserna och de risker som detta typiskt sett innebär. Det torde dock stå klart att de föreslagna bestämmelserna kommer att kunna leda till att allt fler myndigheter kommer att ha tillgång till ökat antal uppgifter om de enskilda. Det finns i sammanhanget en risk för att samhällets intresse i att kunna behandla allt fler uppgifter för allt fler ändamål leder till att den personliga integriteten urholkas i en omfattning som ytterligare kan öka allmänhetens känsla att vara övervakade, samtidigt som informationsutbytet inte självklart behöver ge de resultat som avses.

Utredningen saknar också en erforderlig analys av barnperspektivet beträffande förslagen om ökad personuppgiftsbehandling. Som exempel kan nämnas att utredningen bedömer att den föreslagna uppgiftsskyldigheten för skolan kommer att leda till en ökad personuppgiftsbehandling som medför en inskränkning av skyddet för enskildas personliga integritet (s. 439 f.). På vilket sätt den personliga integriteten kommer att inskränkas och särskilt påverka barn berörs emellertid inte närmare, trots att det kan bli fråga om behandling av känsliga personuppgifter. Att konstatera att intresset av att förebygga och bekämpa brott väger tyngre än intresset av skydd för den enskildes personliga integritet inom skolan (s. 441), utan en konsekvensanalys av barnperspektivet, är inte tillfredsställande.

Anlitande av extern leverantör för genomförandet av informationsutbytet

Om någon extern aktör ska anlitas för genomförandet av informationsutbytet blir det svårt att se att en sådan lösning skulle kunna genomföras utan att de aktuella personuppgifterna kommer att anses utlämnade till leverantörerna.⁷ Under sådana förhållanden torde det bli särskilt svårt att låta en utomstående leverantör få tillgång

⁷ SOU 2018:25 s. 348 ff.



till de sekretessbelagda uppgifterna och uppgifter där det för de privata aktörerna råder tystnadsplikt.⁸ Det kan dessutom tänkas att uppgifterna kan finnas tillgängliga för en extern leverantör som finns utomlands. Advokatsamfundet finner därför att problematiken med att uppgifter som utgör känsliga eller annars särskilt integritetskänsliga personuppgifter eller som omfattas av sekretess och tystnadsplikt med ett omvänt skaderekvisit kan komma att lämnas ut för behandling av en extern leverantör inte i tillräcklig grad har beaktats i betänkandet. Införandet av en ny sekretessbrytande grund i OSL vid utkontraktering av lagring eller teknisk bearbetning ändrar inte på detta. Även om bedömningen av säkerhetsfrågor kan anses ligga utanför utredningens uppdrag, får sådana frågor betydelse för hur lagtexten ska utformas och bör övervägas i den fortsatta beredningen.

Säkerhetsfrågorna

Det finns enligt Advokatsamfundet anledning att särskilt uppmärksamma säkerhetsfrågorna, inte minst med tanke på det slags uppgifter eller personuppgifter som det kan bli fråga om. Eftersom det är uppgifter som angår enskilds hälsa och sjukvård, men även brott eller lagföring för brott, utgör detta slags uppgifter sådana personuppgifter som GDPR räknar som särskilda kategorier och känsliga personuppgifter.⁹ Detta slags uppgifter jämte uppgifter inom socialtjänsten omfattas ofta av särskilda sekretessbestämmelser med omvänt skaderekvisit eller motsvarande tystnadsplikter för de privata aktörerna. Detta borde föranleda särskilda hänsynstaganden vad gäller säkerhetsfrågorna. Det saknas en närmare analys avseende vilka säkerhetsrisker som följer av att informationen kan bli utlämnad till och finnas tillgänglig hos ytterligare myndigheter, där den utlämnande myndigheten eller privata aktören inte har någon möjlighet att kontrollera hur informationen hanteras.

Mot bakgrund av de aktuella uppgifternas känslighet borde utredningen lagt större vikt kring frågor om behörighetsbegränsning och behörighetskontroll avseende den personal hos myndigheterna som ska ha tillgång till personuppgifterna. Detsamma gäller beträffande loggning avseende de åtgärder som personalen vidtar med personuppgifterna. Därtill borde frågan om eventuellt anlitanande av extern part för

⁸ Jfr. SOU 2018:25 s. 364.

⁹ Jfr. art. 9 GDPR.



informationsutbytets genomförande ha fått större uppmärksamhet, särskilt om leverantören finns utomlands.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander