Sveriges advokatsamfund

Stockholm den 18 november 2022

R-2022/1613

Till Finansdepartementet
Fi2021/02991

Sveriges advokatsamfund har genom remiss den 24 augusti 2022 beretts tillfälle att avge yttrande över departementspromemorian Utökat informationsutbyte (Ds 2022:13).

## Sammanfattning

Utredningens uppdrag är att bedöma förutsättningarna för och behovet av ytterligare informationsutbyte för att säkerställa att myndigheter, kommuner och arbetslöshetskassor har tillgång till information om enskilda personer och företag som behövs för att fatta korrekta beslut i frågor om ersättning från välfärdssystemen och för att motverka arbetslivskriminalitet.

Advokatsamfundets uppgift är främst att ta ställning till om lagförslaget påverkar den enskildes rätt till integritet och privatliv samt om inskränkningen av denna rätt som förslaget innebär står i rimlig proportion till samhällets intresse av att kunna behandla personuppgifter för de aktuella ändamålen.

Advokatsamfundet, som hänvisar till tidigare synpunkter i angränsande lagstiftningsärenden,[1] finner att departementspromemorian huvudsakligen kan anses

[1] Se t.ex. Advokatsamfundets remissyttrande den 29 oktober 2020 över betänkandet Kontroll för ökad tilltro – en ny myndighet för att förebygga, förhindra och upptäcka felaktiga utbetalningar från välfärdssystemen (SOU 2020:35), remissyttrande den 28 april 2020 över utkast till proposition Ett effektivare informationsutbyte inom Skatteverket, remissyttrande den 24 april 2020 över betänkandet Samlade åtgärder för korrekta utbetalningar från välfärdssystemen (SOU 2019:59), samt remissyttrande den 11 juni 2018 över betänkandet Bidragsbrott och underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen – en utvärdering (SOU 2018:14).

Laboratoriegatan 4, Box 27321, 102 54 Stockholm
Tfn 08-459 03 00, advokatsamfundet.se, info@advokatsamfundet.se

väl genomtänkt och godtagbart vad gäller de olika förslagen, men att det samtidigt finns vissa förhållanden som bör föranleda ytterligare överväganden och bedömningar i enlighet med vad som påtalas i detta remissvar. Advokatsamfundet kan mot denna bakgrund inte ställa sig bakom förslagen i deras nuvarande utformning.

## Synpunkter

*Allmänna synpunkter på förslaget*

Advokatsamfundet har förståelse för de intressen som ligger bakom utredningens förslag och anser att det är av stor betydelse att motverka felaktiga beslut och att kunna bekämpa kriminalitet som riktar sig mot välfärdssystemen och arbetslivet. Samtidigt är det av stor vikt att reglerna ges en utformning och ett innehåll som inte skapar oförutsebarhet eller går för långt vad gäller intrång i den personliga integriteten. Advokatsamfundet anser överlag att införande av regler av nu aktuellt slag i sig innebär en risk för ändamålsglidning, när uppgifter ska börja behandlas för andra ändamål än vad som gällt 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 bör och kan ske. Det är vidare viktigt att tillförsäkra 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 vill i detta sammanhang särskilt uppmärksamma risken för att ett utökat utbyte av information kommer i konflikt med grundlagsskyddet i 2 kap. 6 § regeringsformen (1974:152) (RF) mot kartläggning av medborgarna.[2]

Utredningen nämner att det förekommer andra pågående utredningar avseende förslag till författningar för att kunna utöka informationsutbytet mellan olika myndigheter för olika ändamål.[3] När det på detta sätt förekommer utredningar i likartade frågeställningar finns det en risk för att utredningarna i vissa avseenden kan krocka med varandra eller komma fram till motstridiga slutsatser. Advokatsamfundet får därför framhålla vikten av att utredningarna är samordnade och att det finns en skarp och tydlig gräns mellan de olika utredningarna, jämte vilka uppdrag de egentligen har.

[2] Se även artiklarna 7 och 8 Europeiska unionens stadga om de grundläggande rättigheterna (2012/C 326/02).
[3] Se Ds 2022:13 s. 62 ff.

Det vore särskilt olyckligt om de olika utredningarna lämnar motstridiga förslag till lagändringar i samma frågor.

*Lagtekniska frågor*

Ett informationsutbyte aktualiserar frågeställningar av lagteknisk natur och som består i själva utformningen och innehållet i de rättsregler som blir aktuella att införa. Till detta kommer frågan om var rättsreglerna ska införas; om de kan införas i någon befintlig författning eller om det behövs nya författningar. Advokatsamfundet har principiellt sett inget att erinra mot utredningens förslag vad gäller i vilka författningar reglerna ska införas.

I norsk rätt finns möjligheter för vissa myndigheter att dela information mellan varandra för brottsbekämpande ändamål. För detta har en särskild föreskrift[4] införts med stöd i den norska förvaltningsloven.[5] Föreskriften innebär att information kan delas mellan vissa myndigheter under vissa förutsättningar. Vilka myndigheter som kan få tillgång till varandras information är uppräknade i föreskriften, samtidigt som föreskriften även innehåller en uppräkning av de olika slags uppgifter som kan komma i fråga jämte vilka förutsättningar som måste föreligga för att informationen ska få delas.

Bestämmelserna får enligt RF 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.[6]

*Åtgärder för att skydda personlig integritet*

Advokatsamfundet anser det vara särskilt angeläget att analysera och bedöma vilka särskilda åtgärder som de föreslagna bestämmelserna kan föranleda för att åstadkomma ett rimligt skydd för den personliga integriteten. Det kan gälla sättet för hur utbytet av information ska ske, vilka slags tekniska lösningar som kan vara

[4] Se Forskrift om deling av taushetspliktsbelagte opplysninger og behandling av personopplysninger m.m. i det tverretatlige samarbeidet mot arbeidslivskriminalitet (a-kriminformasjonsforskriften).
[5] Se 13 g § lov 1967-02-10 om behandlingsmåten i forvaltningssaker (forvaltningsloven).
[6] Angående legalitetsprincipen; se 1 kap. 1 § tredje stycket, 2 kap. 10 § RF, samt prop. 2016/17:180 s. 57 ff., se även 5 § första stycket förvaltningslagen (2017:900). Angående proportionalitetsprincipen, se 2 kap. 21 § RF.

lämpliga, vilka olika slags säkerhetsåtgärder som kan behövas, vem som ska besluta om utbytet och hur utbytet ska kunna ske.

Advokatsamfundets uppfattning är att bestämmelserna i RF innebär att bestämmelserna om informationsutbytet så långt som möjligt ska meddelas genom lag.[7] Det torde dock kunna vara möjligt att på motsvarande sätt som skett i den norska lagstiftningen överföra viss normgivningsrätt till regeringen. Därmed skulle regeringen i förordning kunna meddela närmare föreskrifter, exempelvis om vilka myndigheter som ska kunna få utbyta information, vilken slags information som kan få utbytas och under vilka förutsättningar informationen får utbytas. För att undvika att komma i konflikt med RF 2 kap. 6 § kan det vara nödvändigt att föreskriva att inhämtad information enbart får behandlas för ett bestämt syfte för att därefter göras oåtkomlig. På detta sätt kan det undvikas att stora och kartläggande databaser eller liknande sammanställningar av uppgifter ansamlas utan att de registrerade har kontroll över behandlingen. Dessa förutsättningar bör enligt Advokatsamfundets uppfattning vara klara och tydliga, samtidigt som de även bör vara uttömmande för att åstadkomma förutsebarhet och rättssäkerhet så att det inte lämnas alltför öppet när informationen får utbytas.

*Sekretessbestämmelserna i OSL*

Advokatsamfundet vill särskilt uppmärksamma frågan om sekretess för olika uppgifter som ingår i informationen. Eftersom det är fråga om uppgifter i allmänna handlingar kan dessa omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL). Vissa slags uppgifter har högre skyddsvärde än andra och omfattas därför av olika bestämmelser i OSL med särskilda högre sekretesskrav.

Sekretessprövningen och menbedömningen ska göras utifrån olika skaderekvisit. I de allra flesta fall omfattas uppgifterna av ett rakt skaderekvisit. I ett mindre antal fall omfattas uppgifterna av ett omvänt skaderekvisit och i något enstaka fall gäller absolut sekretess. När uppgifter omfattas av starkare sekretess torde större krav ställas för att uppgiften ska få lämnas ut. Detta följer av proportionalitetsprincipen och måste beaktas vid bedömningen av om uppgiften ska kunna bli föremål för informationsutbyte mellan myndigheterna. Advokatsamfundet får därför framhålla behovet av särskild försiktighet när det blir fråga om informationsutbyte där uppgifter

[7] Jfr 1 kap. 1 § och 2 kap. 20 § RF.

ingår som omfattas av ett särskilt starkt sekretesskydd och där kravet på tydlighet och förutsebarhet därför måste anses särskilt angeläget.

*Behandling av personuppgifter*

Uppgifter som skulle omfattas av informationsutbytet kan även 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 (2018:1177) (BDL), de särskilda brottsdatalagar som gäller specifikt för berörd brottsbekämpande myndighet eller annan särskild registerlagstiftning som gäller för berörd myndighet. Det aktuella införandet av bestämmelser om informationsutbyte mellan myndigheterna kommer därmed oundvikligen att innebära en behandling av personuppgifter som dessutom 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. I detta avseende har Advokatsamfundet betänkligheter avseende att sådana överväganden kan hamna i skymundan i förhållande till de intressen som myndigheterna har för att utbyta informationen.

Advokatsamfundet vill därför i detta sammanhang särskilt framhålla att även informationsutbytet mellan myndigheterna kommer att utgöra behandling av personuppgifter. Detta innebär att utbytet måste uppfylla de grundläggande principerna i GDPR[8] och det måste även finnas en rättslig grund för behandlingen.[9] Till detta kommer att de registrerade på något sätt måste informeras om behandlingen,[10] vilket i detta fall behöver kunna ske utan särskild information till varje registrerad i varje särskilt fall. Advokatsamfundet anser därför att det kommer att bli aktuellt för myndigheterna att anskaffa olika informationssystem och tjänster för att möjliggöra att informationsutbytet sker i enlighet med GDPR.

Dessa system och tjänster måste därutöver uppfylla kraven i GDPR på en ”lämplig” säkerhetsnivå.[11] Uppgifter om enskilda personer som förekommer inom socialtjänsten,

[8] Se artikel 5 GDPR.
[9] Se artikel 6, 9 och 10 GDPR.
[10] Se artikel 12–15 GDPR.
[11] Se artikel 32 GDPR.

hälso- och sjukvården, jämte uppgifter om enskildas fackliga tillhörighet, utgör typiskt sett känsliga personuppgifter enligt GDPR och omfattas även av sekretess med omvänt skaderekvisit. Advokatsamfundet vill därför särskilt framhålla att detta föranleder att säkerhetsfrågorna måste bli föremål för särskilda och noggranna överväganden. Detta har inte i tillräcklig mån uppmärksammats av utredningen och bör föranleda ytterligare överväganden inom ramen för den fortsatta lagstiftningsprocessen.

Behandlingen och informationsutbytet kommer vidare att involvera olika aktörer, myndigheterna och den som bistår myndigheterna genom tillhandahållandet av systemen och tjänsterna. Detta aktualiserar frågor om vem av de olika aktörerna som ska anses vara personuppgiftsansvarig och vem som är personuppgiftsbiträde.[12] 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.[13] Vid ett mer utvecklat utbyte av personuppgifter mellan myndigheter 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 överväganden i den fortsatta beredningen.

*Behandling av personuppgifter för sekundära ändamål och ändamålsglidning*

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.[14]

Advokatsamfundet ställer sig principiellt emellertid tveksamt till sådana sekundära ändamål och känner oro för att deras generella utformning kan legitimera godtycke hos myndigheterna. Eftersom det blir svårt att förutse vilka nya ändamål som personuppgifterna skulle kunna komma att användas för, uppstår även problem med legalitetsprincipen. Advokatsamfundet förordar därför en uttrycklig och tydligare hänvisning till de ytterligare ändamål som skulle kunna komma i fråga, så att de

[12] Se artikel 4.7 och 4.8 GDPR.
[13] Se artikel 28 GDPR.
[14] Se t.ex. Ds 2022:13 s. 164, 172, 184 och 193.

registrerade ges en rimlig chans att kunna förutse för vilka ändamål uppgifterna kan behandlas.

Därtill anser Advokatsamfundet att utredningen tar alltför lättvindigt på finalitetsprincipen och risken för ändamålsglidning.[15] 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 allt fler 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. Det är inte alltid så att ”ändamålen helgar medlen”.

*Direktåtkomst eller annan åtkomst än direktåtkomst*

Advokatsamfundet instämmer i utredningens slutsats att åtkomsten till uppgifter genom informationsutbytet i huvudsak ska ske på annat sätt än genom direktåtkomst. Tillgång till uppgifter genom direktåtkomst är särskilt integritetskänsligt och ska därför medges endast med stor restriktivitet. Såsom utredningen konstaterar blir det därmed fråga om att uppgifterna kommer att utlämnas genom den utlämnande myndighetens försorg i det specifika fallet.[16] När direktåtkomst är möjlig kommer det inte att ske någon prövning hos den utlämnande myndigheten av förutsättningarna för utlämnande, utan det är den mottagande myndigheten som själv prövar detta i samband med åtkomsten till informationen. Advokatsamfundet anser dock att det föreligger en risk för att den utlämnande myndigheten tillmötesgår en begäran om utlämnande utan att göra någon närmare bedömning av om kraven för att utlämnandet verkligen är uppfyllda.[17] Enligt Advokatsamfundets uppfattning måste det uttryckligen framgå att den utlämnande myndigheten i varje enskilt fall ska göra en självständig prövning av huruvida förutsättningarna för utlämnande är uppfyllda. Utredningen går inte tillräckligt långt och är inte tillräckligt tydlig i detta avseende.[18]

[15] Se Ds 2022:13 s. 128.
[16] Se Ds 2022:13 s. 192 ff.
[17] Jfr HFD 2021 ref. 10.
[18] Jfr Ds 2022:13 s. 200.

*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.[19] Under sådana förhållanden torde det bli särskilt svårt att låta en utomstående leverantör få tillgång till de sekretessbelagda uppgifterna.[20] Det kan dessutom tänkas att uppgifterna kan finnas tillgängliga för en extern leverantör som dessutom finns utomlands. Advokatsamfundet anser mot denna bakgrund att problematiken med att uppgifter som utgör känsliga eller annars särskilt integritetskänsliga personuppgifter eller som omfattas av sekretess med ett omvänt skaderekvisit, kan komma att lämnas ut för behandling av en extern leverantör, inte i tillräcklig grad har beaktats i departementspromemorian. Detta är inte tillfredsställande och erforderliga överväganden i detta hänseende bör göras inom ramen för den fortsatta lagstiftningsprocessen.

*Säkerhetsfrågorna*

Det finns enligt Advokatsamfundet anledning att särskilt uppmärksamma frågor om säkerheten kring det föreslagna informationsutbytet, inte minst med tanke på det slags uppgifter eller personuppgifter som kan komma ifråga för informationsutbytet. Eftersom det är uppgifter som angår enskilds hälsa och sjukvård, fackliga tillhörighet, men även brott eller lagföring för brott, utgör detta slags uppgifter sådana personuppgifter som GDPR räknar som särskilda kategorier och känsliga personuppgifter.[21] Detta slags uppgifter jämte uppgifter inom socialtjänsten omfattas ofta av särskilda sekretessbestämmelser med omvänt skaderekvisit. Detta borde föranleda särskilda hänsynstaganden vad gäller säkerhetsfrågorna. Advokatsamfundet anser dock inte att utredningen i tillräcklig grad har uppmärksammat dessa frågeställningar. Det finns exempelvis ingen närmare analys avseende vilka säkerhetsrisker som följer av att informationen kan bli utlämnad till och finnas hos ytterligare myndigheter, där den utlämnande myndigheten inte har någon möjlighet att kontrollera hur informationen hanteras.[22]

[19] Se SOU 2018:25 s. 348 ff.
[20] Jfr SOU 2018:25 s. 364.
[21] Jfr art. 9 GDPR.
[22] Jfr Ds 2022:13 s. 189 ff. och 200 ff.

Mot bakgrund av de aktuella uppgifternas känslighet borde departementspromemorian ha ägnat större uppmärksamhet 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 anlitande av extern part för informationsutbytets genomförande ha fått större uppmärksamhet, särskilt om leverantören finns utomlands. Advokatsamfundet förutsätter att dessa frågor nogsamt övervägs under den fortsatta beredningen av promemorians förslag.

*Cybersäkerhetsfrågor*

Säkerhetsfrågor blir även aktuella med anledning av EU:s cybersäkerhetsakt och kompletterande svensk lagstiftning.[23] Denna lagstiftning kan få betydelse genom att den anvisar olika åtgärder och krav för att åstadkomma hög cybersäkerhet. Detta ger anledning att i utredningen ytterligare beakta och uppmärksamma de möjligheter som reglerna om cybersäkerhet ger för att ställa ytterligare krav på leverantörer av de informationssystem, produkter eller tjänster som kan bli aktuella för att möjliggöra informationsutbyte mellan de berörda myndigheterna.

Eftersom värdet av information ökar i förhållande till antalet användare och mängden information, så ökar skyddsvärdet för informationen på motsvarande sätt.[24] För myndigheter som behandlar uppgifter för hela landets befolkning, innebär ett införande av bestämmelser om informationsutbyte att de höga krav på säkerhet som redan gäller hos dessa myndigheter kommer att behöva höjas ytterligare om de får tillgång till information från andra myndigheter. Detta gör det särskilt angeläget att informationen är korrekt och rättvisande, vilket medför att myndigheterna även måste reglera vem som ansvarar för *masterdata*.[25]

[23] Se Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten), samt lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
[24] Jfr *Metcalfes lag*, https://it-ord.idg.se/ord/metcalfes-lag/.
[25] Se https://it-ord.idg.se/ord/masterdata/.

*Upphandling av informationstekniska produkter och tjänster*

När det blir aktuellt att anskaffa olika informationstekniska system, produkter eller tjänster kommer olika upphandlingsrättsliga regelverk att bli tillämpliga.[26] Därmed måste det i upphandlingsdokumentationen uppställas klara och tydliga krav för att den upphandlande myndigheten ska kunna uppfylla sina krav enligt berörda författningar, inte minst vad gäller säkerheten och informationssäkerheten hos de system, produkter eller tjänster som ska anskaffas. Det finns därför anledning att ytterligare uppmärksamma och analysera även denna problematik.

*Upphovsrätt och licenser*

Anskaffningen av system, produkter och tjänster för den informationshantering som blir aktuell i samband med informationsutbytet aktualiserar även upphovsrättsliga frågeställningar. Detta slags frågor blir inte minst aktuella vid anskaffning av licenser för användning av datorprogram för att hantera informationen.[27]

För att säkerställa tillgången till systemen, produkterna och tjänsterna måste myndigheterna uppmärksamma de krav och licensvillkor som programvaruleverantörerna uppställer för nyttjandet. Detta aktualiserar frågan om myndigheterna ska äga rättigheterna, särskilt om det blir fråga om att specialutveckla programvara för myndigheternas informationsutbyte. Det kan vara särskilt intressant för myndigheterna att ha samtliga rättigheter till en specialutvecklad programvara där myndigheterna har stått för alla kostnader för utvecklingen. Samtidigt måste myndigheterna vara medvetna om att leverantörerna sannolikt är bättre lämpade än myndigheterna att svara för uppdatering, uppgradering, service, underhåll, vidareutveckling och andra åtgärder med programvaran.

Med ett ökande beroende av att använda olika former av molntjänster och tekniker som DevOPs,[28] kommer det sannolikt inte längre att vara möjligt för myndigheterna att ha full kontroll över säkerheten. Detta leder antingen till ökad egenutveckling som kommer att ha svårt att hänga med i den tekniska utvecklingen, eller till ett större behov av avancerade krypteringslösningar för att kunna hålla en rimlig säkerhetsnivå.

[26] Se lagen om offentlig upphandling (2016:1145) (LOU), lagen (2016:1146) om upphandling inom försörjningssektorerna (LUF), lagen (2016:1147) om upphandling av koncessioner (LUK), samt lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS).
[27] Se lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (URL).
[28] Se https://azure.microsoft.com/sv-se/resources/cloud-computing-dictionary/what-is-devops/.

Tidigare erfarenhet tyder på att myndigheter generellt sett har svårt att själva bedriva en konkurrenskraftig drift och utvecklingsverksamhet, samtidigt som myndigheterna även har ett stort konsultberoende. Detta talar mot att egenutveckling hos myndigheterna är ett realistiskt alternativ.

Om leverantörerna inte behåller rättigheterna och endast upplåter en licens till myndigheterna, finns det en stor risk för att deras intresse för att svara för sådana åtgärder minskar. Det finns därför ett stort behov av att se över och anpassa lagstiftningen som styr myndigheternas handläggning och databehandling till de processer som är dominerande inom kommersiell programvara.

En annan fråga gäller programvaruleverantörens rätt att få tillgång till den information som behandlas genom programvaran, exempelvis för att kontrollera att licensvillkoren inte åsidosätts. Det kan också gälla leverantörens rätt att ensidigt uppdatera eller uppgradera programvaran, ändra licensvillkoren, stänga av systemen, produkterna eller tjänsterna för underhåll, drift eller säkerhetsåtgärder. Det kan även gälla möjligheten att säkerställa fortsatt tillgång till källkoder m.m. för det fall leverantören upphör med eller ändrar sin verksamhet.

Advokatsamfundet anser mot bakgrund av vad som nu sagts att även de upphovsrättsliga överväganden som kommer att bli aktuella vid anskaffandet och upphandlingen av de system, produkter och tjänster som ska användas för informationsutbytet måste adresseras i det fortsatta lagstiftningsarbetet.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander