Stockholm den 8 januari 2016

R-2015/1712

Till Justitiedepartementet

Ju2015/06913/L4

Sveriges advokatsamfund har genom remiss den 18 september 2015 beretts tillfälle att avge yttrande över departementspromemorian Passdatalag (Ds 2015:44).

Advokatsamfundet har även tidigare yttrat sig över flertalet lagstiftningsförslag rörande pass, till vilka yttranden hänvisas i nu aktuella hänseenden.[1]

Sammanfattande synpunkter

I promemorian föreslås en särskild passdatalag med vissa kompletterande författningar som ska gälla utöver personuppgiftslagen (1998:204). En målsättning med förslagen i promemorian är att åstadkomma att passverksamheten bedrivs effektivt samtidigt som de föreslagna reglerna ska skydda mot intrång i den personliga integriteten.

Advokatsamfundet finner att de föreslagna reglerna i många delar är lämpliga och motiverade utifrån samhällets behov att få behandla berörda personuppgifter. Förslaget eftersträvar även att motverka att personuppgifter behandlas på ett sätt som äventyrar den personliga integriteten, något som givetvis är positivt.

Advokatsamfundet finner dock att förslaget brister i tre väsentliga avseenden. Förslaget utgår nämligen ifrån de nuvarande reglerna om behandling av personuppgifter i personuppgiftslagen (PuL), som inom kort och i väsentliga avseenden kommer att ersättas av nya EU-regler. Om de föreslagna reglerna införs kommer de därför att mycket snart behöva genomgå omfattande förändringar för att anpassas till de nya EU-reglerna. Därtill tar förslaget inte tillräcklig hänsyn till att de personuppgifter som förekommer även kan

[1] Se särskilt Advokatsamfundets remissyttrande den 1 september 2015 över departementspromemorian Missbruk av svenska pass – Omfattning och åtgärdsförslag (Ds 2015:12), men även yttranden den 15 september 2014 över utkast till lagrådsremiss Ökade möjligheter att resa inom EU utan pass (Ju2014/4374/L4), den 18 november 2008 över promemorian Fingeravtryck i pass (Ju2008/7893/PO), den 10 januari 2005 över utkast till lagrådsremiss Ökad säkerhet i pass m.m. (Ju2004/1747/PO), den 29 april 2004 över departementspromemorian Ökad säkerhet i pass m.m. (Ds 2004:8) och den11 december 2000 över promemorian Sekretessen för passfoton m.m. (Ds 2000:57).

vara känsliga och att säkerhetsfrågorna därför borde ha blivit föremål för en betydligt mer omfattande analys. Dessutom möjliggör förslaget att personuppgifter behandlas för vissa sekundära ändamål, som lämnas mer eller mindre öppna utan att det närmare analyserats vilka dessa ändamål kan vara och vilka konsekvenser behandlingen kan medföra.

Utöver detta saknas en analys av hur tillgången till uppgifter och informationsflödet mellan myndigheterna kan komma att påverka den personliga integriteten och rättssäkerheten. Detsamma gäller beträffande hur de föreslagna reglerna kan komma att påverka de enskildas förtroende för myndigheternas verksamhet.

Advokatsamfundet kan därför i nuläget inte ställa sig bakom förslagen och anser att förhållandet till de nya EU-reglerna, säkerhetsfrågorna och konsekvenserna av de sekundära ändamålen görs till föremål för en grundlig utredning.

Därutöver vill Advokatsamfundet anföra följande.

De kommande förändringarna av EU-reglerna om behandling av personuppgifter

Inom Europeiska unionen (EU) pågår ett reformarbete avseende reglerna om dataskydd och personuppgiftsbehandling.[2] Dessa regler kommer sannolikt att införas genom en förordning och ett direktiv redan under 2016 och därefter börja tillämpas 2018. I motsats till vad som gäller enligt nuvarande ordning där PuL är subsidiär i förhållande till annan lag,[3] kommer de nya EU-reglerna att gälla överordnat. Enligt utredningens förslag ska de föreslagna reglerna träda i kraft redan under sommaren 2016.[4]

Utredningen har inte tagit någon större hänsyn till att EU-reglerna för behandling av personuppgifter inom kort kommer att genomgå omfattande förändringar och de ändrade förutsättningar som detta kan medföra (jfr s. 79).[5] Således utgår de föreslagna reglerna i flera avseenden ifrån möjligheten att behandla personuppgifter i löpande text och ostrukturerat enligt nuvarande undantagsbestämmelse i 5 a § PuL, trots att denna bestämmelse sannolikt kommer att upphöra att gälla inom kort och utan att bedöma konsekvenserna därav.[6]

Advokatsamfundet finner det mycket betänkligt att utredningen inte avvaktat beslutet om de kommande förändringarna innan förslaget lämnades. Det finns en överhängande risk för att reglerna inom en mycket snar framtid måste ändras på nytt. Därför kan utredningens arbete rentav ha varit i onödan. Detta förhållande utgör i sig tillräckliga skäl för Advokatsamfundet att avstyrka utredningens förslag. Advokatsamfundet anser att utredningen i stället borde ha avvaktat införandet av förordningen och direktivet för att

[2] KOM(2012) 11.
[3] 2 § personuppgiftslagen (1998:204).
[4] Ds 2015:44 s. 243.
[5] Se t.ex. Ds 2015:44 s. 79.
[6] Ds 2015:44 s. 82, 139 f., 155 och 172.

därefter ytterligare anpassa förslaget till de ändrade förutsättningar som detta kan medföra.

Säkerhetsfrågorna

Som utredningen konstaterar omfattas inte sådan behandling av personuppgifter som inte ingår i eller är avsedda att ingå i en samling av personuppgifter, som har strukturerats för att påtagligt underlätta sökningen efter eller sammanställningen av personuppgifter av flertalet av hanteringsreglerna i PuL.[7] Advokatsamfundet vill i detta sammanhang särskilt framhålla att inte heller en sådan behandling får kränka den registrerades personliga integritet, och de säkerhetskrav som anges i PuL gäller även för sådan behandling.[8] Även om utredningens genomgång av reglerna till skydd för den personliga integriteten är bra, detaljerad och heltäckande, saknar Advokatsamfundet en närmare analys om vilka konkreta säkerhetsåtgärder som behövs eller kan vara lämpliga.[9]

I systemen kommer t.ex. sådana personuppgifter att finnas tillgängliga som avslöjar att den registrerade genomgår psykiatrisk tvångsvård eller rättspsykiatrisk vård.[10] Dessa är särskilt känsliga personuppgifter.[11] När sådana personuppgifter förekommer blir det särskilt viktigt att vidta lämpliga säkerhetsåtgärder för att skydda mot obehörig åtkomst eller förvanskning t.ex. på grund av tekniska brister eller andra tillkortakommanden. Advokatsamfundet anser inte att utredningen ägnat dessa frågor tillräcklig uppmärksamhet och inte heller frågan om vilka konkreta åtgärder som bör vidtas för att personuppgifterna inte ska bli tillgängliga för sådana som inte behöver dem i arbetet.

Advokatsamfundet instämmer i att passmyndigheterna och Utrikesdepartementet ges möjlighet att använda modern kommunikationsteknik för att utbyta information på elektronisk väg.[12] Detta förutsätter dock att myndigheterna samtidigt är medvetna om de särskilda egenskaper som tekniken har och förutsättningarna som gäller för teknikens användande.

Säkerhetsfrågorna är av mycket stor vikt för förtroendet för rättsskipningen, vilket medför att stora krav måste ställas på att de uppgifter som används är skyddade och korrekta.[13] Det måste enligt Advokatsamfundets uppfattning därför ställas stora krav på handläggarna, de brottsbekämpande myndigheterna, samt inte minst åklagare, advokater och domstolar att vara väl insatta i hur systemen är uppbyggda och utformade, liksom vilka administrativa, organisatoriska och tekniska säkerhetsåtgärder som vidtagits, vilka särskilda risker som är förknippade därmed och hur detta kan påverka tillförlitligheten hos de uppgifter som förekommer. Om tillförlitligheten hos uppgifterna övervärderas, innebär detta en påtaglig risk för att de uppgifter som inhämtas leder till oriktiga beslut och

[7] Ds 2015:44 s. 82 och 139 f.
[8] 5 a § och 31 § PuL.
[9] Ds 2015:44 s. 73 ff.
[10] Ds 2015:44 s. 96.
[11] 13 § PuL.
[12] Ds 2015:44 s. 205.
[13] Se t.ex. prop. 2010/11:46 s. 54, SOU 2007:76 s. 19 f. och s. 111 f.

åtgärder.[14] Samtidigt kan brister härvidlag leda till minskat förtroende hos allmänheten för myndigheterna och rättstillämpningen.[15]

Om systemen har ett okänt eller stort antal åtkomstpunkter eller andra accessmöjligheter, om ett stort antal personer har tillgång eller access till systemen och tjänsterna och kan förändra uppgifter i dessa, om loggning av åtgärder eller uppföljning av sådan loggning är otillräcklig, om det förekommer ett stort antal incidenter där uppgifter försvunnit eller manipulerats, eller om det saknas kontroll över vilka slags incidenter som skett eller kan ske, utgör detta var för sig eller tillsammans sådana omständigheter som i olika hög grad måste medföra att de lagrade uppgifternas tillförlitlighet minskar. Advokatsamfundet ser med stor oro på att utredningen inte uppmärksammat detta och att det finns en påtaglig risk för att uppgifternas robusthet inte kommer att ifrågasättas, i vart fall inte i tillräcklig grad. Om detta inte uppmärksammas ökar riskerna för felbedömningar och felaktiga beslut som i sin tur medför onödiga olägenheter eller i vissa fall allvarliga konsekvenser för dem vars uppgifter behandlas.

Utredningen har således inte i tillräcklig grad beaktat informationsteknikens särskilda egenskaper och förutsättningarna för teknikens användande. Advokatsamfundet är därför oroligt för att värdet och tillförlitligheten hos de uppgifter som förekommer i systemen kan komma att överskattas, vilket i sin tur kan leda till oriktiga beslut och åtgärder. Advokatsamfundet anser att det därför finns ett starkt behov av att utreda vilka konkreta risker som finns i de berörda informationssystemen och vilka konkreta åtgärder som ska vidtas för att tillgodose säkerheten i systemen.

Som utredningen själv anger, föreligger större behov av att precisera eller begränsa personuppgiftsbehandlingen ju större informationsmängder och ju känsligare innehåll det är fråga om.[16] Advokatsamfundet anser det därför vara angeläget att det utreds och registreras hur många och vilka som har tillgång till all information i de berörda systemen. Därtill bör bedömas hur deras användning av personuppgifterna kontrolleras eller ska kontrolleras, t.ex. att loggning bör ske på individnivå, vilken tid åtgärderna vidtagits och vilket slags åtgärder det varit fråga om. Därtill bör frågan om logguppföljning uppmärksammas och vilka åtgärder som kan bli aktuella med anledning därav.

En annan fråga som är av väsentlig betydelse i sammanhanget gäller vilka incidenter som förekommit i systemen, vilka konsekvenser incidenterna medfört, hur och när de upptäckts, vad som orsakat incidenterna och hur de åtgärdats. Således tar utredningen t.ex. inte upp frågan om eventuella behov av brandväggar, virusskydd, larmfunktioner eller behov av kryptering. Dessa frågeställningar är av stor betydelse för bedömningen av säkerhetsfrågorna och behovet av säkerhetsåtgärder.

[14] Jfr t.ex. Svea hovrätts dom, 2006-10-02, mål nr B 8799-05.
[15] Jfr prop. 2010/11:46 s. 54 och SOU 2007:76 s. 19 f. och s. 111 f.
[16] Ds 2015:44 s. 128 f. och s. 137.

Ändamålen med behandlingen av personuppgifterna

De regler som utredningen föreslår ska gälla särskilt för sådan behandling av personuppgifter som är helt eller delvis automatiserad och där personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter, som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Utgångspunkten är reglerna i PuL. Syftet med de föreslagna reglerna är att åstadkomma att personuppgifter som förekommer i passverksamheten behandlas på ett ändamålsenligt sätt och att reglerna även ska skydda de registrerade mot att deras personliga integritet kränks vid behandlingen.[17] Advokatsamfundet har inget att erinra mot detta och välkomnar att det särskilt regleras hur personuppgifter får behandlas i passverksamheten.

Förslagets 5 § innebär att det uttryckligen ska framgå att det är Polismyndigheten som är personuppgiftsansvarig för behandlingen av personuppgifter inom passverksamheten, vilket underlättar för de registrerade att veta vart de ska vända sig med frågor och begäran om rättelse av personuppgifterna eller på annat sätt tillvarata sina rättigheter.[18] I vissa övriga situationer ska dock personuppgiftsansvaret vara delat med andra myndigheter.[19] Advokatsamfundet ser dock med viss oro på att detta kan leda till svårigheter för den enskilde att bedöma vart denne ska vända sig med frågor rörande behandlingen av dennes personuppgifter, men även att det blir oklart vilken myndighet som är ansvarig i vilket avseende. Enligt Advokatsamfundet vore det, om flera myndigheter utöver Polismyndigheten utpekats som personuppgiftsansvariga dit de enskilda kan vända sig, lämpligt att myndigheterna sinsemellan får göra upp vilken av dem som ska ha det slutliga och inbördes ansvaret.

De olika ändamål för vilka personuppgifter enligt förslagets 6-7 §§ ska få behandlas i passverksamheten, är huvudsakligen väl konkretiserade och därmed förutsebara. De föreslagna reglerna anger dock vissa ändamål som inte är beskrivna på ett sådant sätt att räckvidden av dessa enkelt kan förutses. Som exempel hänvisas till Polismyndighetens brottsförebyggande eller brottsbekämpande verksamhet, som ett sådant ändamål för vilket de olika personuppgifterna ska få behandlas.[20] Ett sådant allmänt hållet ändamål är inte avgränsat, utan behandlingen av personuppgifterna kan avse alla slags moment som ingår i en sådan verksamhet. Advokatsamfundet anser därför inte att den beskrivning av de sekundära ändamålen för personuppgiftsbehandlingen är så uttömmande som utredningen gör gällande.[21]

Av förslaget framgår även att Polismyndigheten på begäran ska lämna ut uppgift i form av enskilds fotografiska bild i passregistret till vissa myndigheter, nämligen till

[17] Ds 2015:44 s. 15 ff.
[18] Ds 2015:44 s. 146 f.
[19] Ds 2015:44 s. 150 f.
[20] Ds 2015:44 s.17 och s. 158 ff.
[21] Ds 2015:44 s. 160.

Ekobrottsmyndigheten, Försvarsmakten, Kronofogdemyndigheten, Kustbevakningen, svensk ambassad, svenskt lönat konsulat, Skatteverket, Säkerhetspolisen och Tullverket.[22]

Därmed skulle personuppgifterna kunna få användas i Polismyndighetens verksamhet för spaning och kriminalunderrättelse, varvid Polismyndigheten även skulle kunna använda uppgifterna för att byta till sig information från andra länders myndigheter. De personuppgifter som lämnats ut till de olika uppräknade myndigheterna kan därefter på liknande sätt lämnas ut till andra länders myndigheter av motsvarande skäl. I en sådan situation kommer det att saknas kontroll över hur och av vilka skäl personuppgifterna senare används av sådana utländska myndigheter. Samtidigt omfattas underrättelse-verksamheten av särskilda bestämmelser om sekretess, som medför att den registrerade inte får reda på vilka uppgifter som har lämnats ut, till vem de utlämnats eller varför de utlämnats och än mindre få någon möjlighet att rätta eventuella felaktigheter.[23] Advokatsamfundet anser inte att utredningen analyserat denna problematik på erforderligt sätt.

Som utredningen framhåller får personuppgifterna inte behandlas för något ändamål som är oförenligt med det ursprungliga ändamålet (finalitetsprincipen). Även ett utlämnande av personuppgifterna till annan, måste vara förenligt med de ursprungliga ändamålen. För att avgöra om så är fallet, måste man beakta vad den som vill ha ut uppgifterna ska använda dem till och jämföra den tilltänkta användningen med de ursprungliga ändamålen.[24] Utredningen går dock inte in på hur det ska kunna kontrolleras att behandlingen inte sker i strid med finalitetsprincipen om personuppgifterna ska lämnas ut till andra myndigheter.

Tillgången till och hanteringen av personuppgifterna

Det ärendehanteringssystem som används för ansökningar om pass och nationella identitetskort är ett kombinerat system för ärendehantering och register över utfärdade pass, nationella identitetskort och vissa omständigheter som kräver passtillstånd; Resehandlingssystemet (RES). Passhandläggaren får genom RES tillgång till olika söksystem och register, såsom belastningsregistret, misstankeregistret, kriminalvårdens register, Polismyndighetens person- och adressregister jämte Polismyndighetens dataregister för personefterlysningar. Information om huruvida den som ansöker om pass förekommer i dessa register och om passhinder därmed föreligger, inhämtas enligt utredningen automatiskt.[25] Det är således fråga om att myndigheterna får *direktåtkomst* genom RES till dessa system och uppgifter, något som anses särskilt känsligt ur integritetsaspekt.[26] Även på denna grund borde utredningen enligt Advokatsamfundets uppfattning ha ägnat större uppmärksamhet åt säkerhetsfrågorna.

---

[22] Ds 2015:44 s.34 f.
[23] 18 kap. 2 § offentlighets- och sekretesslagen (2009:400).
[24] Ds 2015:44 s. 156.
[25] Ds 2015:44 s. 90 och 93 f.
[26] Jfr e-delegationens rapport – Direktåtkomst och utlämnande på medium för automatiserad behandling, s. 6 och Datainspektionens yttrande 2015-02-26, dnr 2529-2014.

I enlighet med utredningens beskrivning innehåller passhandlingen ett datachip, som kan innehålla biometrisk information. Där ingår den enskildes ansiktsbild tillsammans med dennes fingeravtryck, underskrift och andra personuppgifter.[27] Syftet med detta är att underlätta fastställandet av rätt identitet hos passhandlingens innehavare. Detta betyder att det kommer att finnas personuppgifter utgörande biometrisk information i berörda informationssystem, som uppgifterna i passhandlingarnas datachip kan matchas mot. Advokatsamfundet vill i detta sammanhang uppmärksamma att Datainspektionen i flera sammanhang har uttalat att sådan biometrisk information i sig utgör känsliga personuppgifter och att särskild försiktighet måste iakttas vid behandlingen därav.[28] Mot denna bakgrund anser Advokatsamfundet att det krävs särskilda säkerhetsåtgärder för att skydda detta slags personuppgifter och att det behöver ytterligare utredas vilka konkreta åtgärder som kan behövas.

Bolaget AB Svenska Pass, som är ett privat företag, anlitas för att tillverka passen och får i denna verksamhet tillgång till personuppgifterna på sådant sätt att bolaget därmed utgör ett personuppgiftsbiträde enligt PuL.[29] Utredningen har dock enligt Advokatsamfundets uppfattning inte tillräckligt uppmärksammat detta och därför inte berört vilka krav som ska ställas på bolaget i denna egenskap för att tillgodose att personuppgifterna behandlas i enlighet med PuL och hur bolaget ska uppfylla lämpliga säkerhetskrav. Det har heller inte berörts vem av de olika personuppgiftsansvariga myndigheterna som ska ingå sådant personuppgiftsbiträdesavtal med bolaget, som krävs enligt PuL.[30] Advokatsamfundet finner därför att även denna fråga bör utredas ytterligare.

De enskildas förtroende för myndigheternas verksamhet

Utredningen konstaterar att medborgarna tillförsäkras frihet att röra sig inom riket och att lämna detta. Krav på innehav och uppvisande av pass eller bestämmelser om passhinder kan i viss utsträckning anses inskränka denna frihet. Sådana inskränkningar får endast ske i lag samtidigt som de ändamål som ligger bakom inskränkningarna måste vara godtagbara i ett demokratiskt samhälle och nödvändiga för ändamålen.[31]

Tillgången till pass kan begränsas för den som är misstänkt eller dömd för brott, den som är intagen för psykiatrisk tvångsvård, den som i samband med konkursärende ålagts att lämna ifrån sig sitt pass eller i sådant sammanhang meddelats förbud att utfärda pass, den som är skäligen misstänkt för brott där det inte föreskrivs lindrigare straff än fängelse i sex månader eller den som är efterlyst och omedelbart ska gripas.[32] Advokatsamfundet har i och för sig inget att erinra mot detta och att personuppgifterna får användas för dessa ändamål, men eftersom konsekvenserna av felaktigheter i uppgifterna kan få mycket

[27] Ds 2015:44 s. 41 och 94.
[28] Se t.ex. Datainspektionens beslut dnr 1601-2004, 535-2007, 1765-2009 och Datainspektionens yttrande 2008-11-20, dnr 1377-2008, jfr även Regeringsrättens dom 2008-12-16 i mål nr 6588-05.
[29] Ds 2015:44 s. 154 och 3 § PuL.
[30] 30 § PuL.
[31] 2 kap. 8, 20 och 21 §§ regeringsformen, Ds 2015:44 s. 44.
[32] Ds 2015:44 s. 45 och s. 50.

allvarliga konsekvenser för den enskilde, borde integritets- och säkerhetsfrågorna ha fått mycket större uppmärksamhet.

Som utredningen själv framhåller har den enskilde i praktiken ingen valmöjlighet. Om den enskilde inte frivilligt låter myndigheterna behandla personuppgifterna och lämnar fingeravtryck och bild, utfärdas inget pass och därmed inskränks den enskildes medborgerliga rörelsefrihet.[33] Dessa omständigheter borde ha utgjort ytterligare skäl för utredningen att närmare bedöma säkerhetsfrågorna och vilka säkerhetsåtgärder som kan vara lämpliga.

En av målsättningarna med de föreslagna lagreglerna är att tillgången till och behandlingen av personuppgifterna ska främja en effektiv passverksamhet. Detta innebär att passmyndigheterna snabbt och enkelt ska kunna upptäcka om det föreligger någon förutsättning för ett ingripande, t.ex. vid ut- eller inresa till riket. Då måste myndigheterna snabbt kunna få tillgång till uppgifterna och även kunna utbyta dem med andra myndigheter. Advokatsamfundet ser här en risk för att kravet på snabbhet och enkelhet kan ske på bekostnad av säkerheten. Detta gör det särskilt viktigt att personuppgifterna behandlas på ett säkert sätt och att det säkerställs att uppgifterna är korrekta, inte minst när resultatet kan bli att den enskildes rörelsefrihet inskränks. Ett felaktigt ingripande kan leda till långtgående följder för den enskilde, t.ex. genom att en semesterresa inte kan genomföras. Advokatsamfundet anser inte att utredningen heller har tagit tillräcklig hänsyn till och analyserat säkerhetskraven utifrån denna bakgrund.

Advokatsamfundet saknar således en närmare analys av vilka konsekvenser felaktigheter eller brister i behandlingen av personuppgifterna kan få för de enskilda och hur detta kan komma att påverka medborgarnas förtroende för passverksamheten. En sådan analys skulle även bidra till bedömningen av vilka säkerhetsåtgärder som kan vara lämpliga för att undvika sådana felaktigheter eller brister i systemen och behandlingen av uppgifterna.

Särskilt om nationella identitetskort

Utredningen bedömer att ärenden om nationella identitetskort nästan aldrig innehåller några integritetskänsliga uppgifter och anser därför att det är tillräckligt att behandlingen av personuppgifter regleras i en förordning.[34] Eftersom vissa känsliga personuppgifter trots allt kan förekomma, borde utredningen enligt Advokatsamfundets uppfattning ha gått närmare in på hur sådana uppgifter ska få behandlas och vilka åtgärder som bör vidtas för att säkerställa att uppgifterna inte heller i dessa sammanhang behandlas i strid med PuL.

[33] 6 § passlagen (1978:302) och Ds 2015:44 s. 46.
[34] Ds 2015:44 s. 211.

De föreslagna lagreglerna

1 § passdatalagen[35]

Förslaget innebär att helt manuell behandling av personuppgifter, som inte ingår i ett register eller annan samling som är tillgänglig för sökning, anses falla utanför lagens tillämpningsområde. Enligt Advokatsamfundets bedömning finns det med en sådan formulering risk för att manuella uppgifter skulle kunna anses falla utanför det skydd för den personliga integriteten som lagen ska ge. Även sådan behandling av uppgifter kan vara känslig och bli integritetskränkande. Det bör därför förtydligas att kränkande behandling är förbjuden och att de säkerhetskrav som anges i PuL ändå ska gälla.

4 § passdatalagen[36]

Hänvisningen till bestämmelserna i PuL kan förenkla för den enskilde att bedöma och tillvarata sina rättigheter. Dock får ifrågasättas om denna hänvisning är lämplig när med hänsyn till att det mycket snart kommer att införas nya regelverk på personuppgifts-området. Hänvisningen kommer därför inom kort att bli inaktuell. Samtidigt förefaller utredningen inte alls ha beaktat de förändringar som diskuteras och som sannolikt kommer att införas.

De nya reglerna kommer till skillnad från nuvarande ordning att ha företräde, vilket kommer att leda till tillämpningsproblem om utredningens förslag till ny passdatalag antas.

5 § passdatalagen[37]

Advokatsamfundet välkomnar att det förtydligas vem som är personuppgiftsansvarig, eftersom detta generellt underlättar för den enskilde att veta vart denne ska vända sig med frågor angående personuppgiftsbehandlingen. Dock kan vissa problem uppstå vid ett delat personuppgiftsansvar, eftersom det kan bli oklart vem som i själva verket är den som ska svara för behandlingen. När uppgifter lämnas ut till utlandsmyndigheterna och Utrikesdepartementet kan personuppgiftsansvaret för en och samma uppgift komma att ligga hos flera myndigheter, där var och en av dessa ansvarar för den egna behandlingen.[38] Advokatsamfundet anser det vara önskvärt att den enskilde ges möjlighet att få veta till vem av de personuppgiftsansvariga denne ska vända sig och att dessa därefter sinsemellan får avgöra vem av dem som ska ansvara.

[35] Ds 2015:44 s. 246.
[36] Ds 2015:44 s. 247.
[37] Ds 2015:44 s. 248.
[38] Ds 2015:44 s. 249.

6 § p. 6 passdatalagen[39]

Som ett sekundärt ändamål för behandlingen av personuppgifter anges övrigt fullgörande av passmyndigheternas och Regeringskansliets (Utrikesdepartementet) uppgifter enligt passlagen (1978:302). I detta sammanhang gäller att personuppgifterna ska få behandlas även för andra sekundära ändamål än de som anges i lagen, om det efter en prövning i det enskilda fallet bedöms att vidarebehandlingen inte kan anses oförenlig med insamlingsändamålet (finalitetsprincipen).[40]

Advokatsamfundet är bekymrat över att det härigenom skapas ett slags generalklausul eller slasktratt, som möjliggör behandling för sådana ändamål som i praktiken inte är bestämda i förväg. Ändamålet riskerar i sådant fall att bli så obestämt att det blir svårt att se hur vidarebehandlingen i praktiken skulle kunna åsidosätta finalitetsprincipen. Det kan därför ifrågasättas om detta ger något egentligt skydd. Det vore därför önskvärt att ändamålet ytterligare preciseras så att det inte kommer att tas till intäkt för vilken behandling som helst.

7 § passdatalagen[41]

Personuppgifterna ska även få behandlas i Polismyndighetens brottsförebyggande och brottsbekämpande verksamhet samt vid myndighetens upprätthållande av den allmänna ordningen och säkerheten. Även detta ändamål blir obestämt, eftersom sådan Polismyndighetens verksamhet kan komma att innehålla vad som helst som därmed kan få läggas till grund för behandlingen. Advokatsamfundet finner det otillfredsställande att detta ändamål lämnas öppet på sådant sätt och anser det önskvärt att detta ändamål ytterligare preciseras, så att det inte kommer att tas till intäkt för vilken behandling som helst.

9 § passdatalagen[42]

Polismyndigheten använder fotografierna i passregistret för att fastställa identiteten på en person, t.ex. i samband med identifiering av enskilda vid större olyckor, vid foto-konfrontationer och som ett led i spaningsarbete. Därmed blir katalogen inte exklusiv, utan även andra orsaker kan föranleda behandlingen. Uppgifterna skulle t.ex. kunna användas i utbyte för att få in uppgifter från annan myndighet i andra länder. Därav kan följa en okontrollerad spridning och behandling av uppgifterna på ett sätt som äventyrar den personliga integriteten på sätt och för ändamål som egentligen inte avsetts eller kan kontrolleras.

[39] Ds 2015:44 s. 249.
[40] Ds 2015:44 s. 250.
[41] Ds 2015:44 s. 246.
[42] Ds 2015:44 s. 251 f.

14 § passdatalagen[43]

Enligt förslaget blir det tillåtet att i löpande text behandla sådana känsliga personuppgifter som avslöjar ras eller etniskt ursprung eller som rör hälsa som sökanden eller någon annan (t.ex. en psykiater) har lämnat i ett passärende, även om uppgiften inte är nödvändig för att myndigheten ska kunna handlägga ärendet. Förutom att detta kan bli oförenligt med de nya EU-reglerna får Advokatsamfundet uppmärksamma att inte heller i detta sammanhang får behandlingen vara kränkande och att säkerhetskraven enligt 5 a § och 31 § PuL fortfarande måste uppfyllas.

15 § passdatalagen[44]

Advokatsamfundet välkomnar det föreslagna förbudet mot användandet av känsliga personuppgifter som sökbegrepp.

17 § passdatalagen[45]

Enligt utredningens förslag ska anställda och andra med uppdrag hos myndigheterna endast ges tillgång till personuppgifter utifrån vad som krävs för arbetsuppgifterna. Advokatsamfundet ifrågasätter om det verkligen finns ett behov av tillgång till personuppgifterna för alla de cirka 25 880 som utredningen nämner. Samtidigt vill Advokatsamfundet peka på nödvändigheten av behörighetskontroll, loggning och uppföljning av loggningen.

19 § passdatalagen[46]

Enligt utredningens förslag ska personuppgifter kunna lämnas ut på ett USB-minne eller en cd-skiva, eller att uppgifterna sänds via e-post eller genom någon annan form av elektroniskt kommunikationsmedel. Advokatsamfundet får i detta sammanhang påpeka att ett automatiserat förfarande kan medföra att gränserna suddas ut mellan utlämnande på medium för automatiserad behandling och direktåtkomst, vilket i sig kan vara en fara för den personliga integriteten. Samtidigt aktualiseras behovet av kryptering av person-uppgifterna för att undvika obehörig åtkomst, särskilt beträffande känsliga personuppgifter.

[43] Ds 2015:44 s. 254.
[44] Ds 2015:44 s. 255.
[45] Ds 2015:44 s. 258.
[46] Ds 2015:44 s. 259.

Avslutande synpunkter

Utredarna har enligt vad som anges i förslaget besökt och samrått med ett flertal olika myndigheter.[47] Det hade varit värdefullt om de samtidigt haft med sig sakkunniga inom det informationstekniska området och säkerhetsområdet för att därigenom kunna bedöma och ställa relevanta frågor om säkerheten, men så förefaller inte ha varit fallet. Detta ger enligt Advokatsamfundet intrycket att utredarna tagit alltför lättvindigt på säkerhets-frågorna. De sakkunniga skulle i så fall även ha kunnat bidraga med närmare kunskap om hur utformningen av systemen och myndigheternas hantering kan effektiviseras när nu detta är ett av målen bakom utredningen. Sakkunniga på säkerhets- och integritetsområdet skulle även ha kunnat tillföra värdefulla kunskaper om integritetsaspekterna, som var den andra delen av målsättningen bakom utredningen och lagförslaget.

När ett lagstiftningsarbete avser informationstekniska förhållanden är det särskilt viktigt att det även finns tillgång till teknisk sakkompetens. Denna sakkompetens kan i och för sig anlitas separat och när utredningen finner att den behövs, såsom tydligen varit fallet i den aktuella utredningen. Advokatsamfundet anser dock att det i sådana fall är lämpligt att sådan sakkompetens ingår i utredningen, särskilt eftersom det inte alltid är lätt att förutse när sådant behov föreligger. Om sakkompetensen ingår i utredningen kan det säkerställas att de tekniska aspekterna och säkerhetsfrågorna hanteras på ett lämpligt och adekvat sätt, samtidigt som utredningens innehåll och slutsatser kommer att bli mer robusta.

Advokatsamfundet får därför rekommendera att expertis inom informationsteknik och informationssäkerhet anlitas och ingår i utredningen i ett eventuellt fortsatt utredningsarbete. Sådan kompetens finns t.ex. hos Datainspektionen, Post- och telestyrelsen, Myndigheten för samhällsskydd och beredskap eller hos olika privata aktörer inom området för elektronisk kommunikation.

Såsom framgått anser Advokatsamfundet att utredningen borde ha avvaktat med sitt förslag, så att de regeländringar som kommer att bli aktuella till följd av beslut om de nya EU-reglerna på personuppgiftsområdet kunnat beaktas. Detta är den allvarligaste invändningen som Advokatsamfundet har mot förslaget, eftersom de föreslagna reglerna sannolikt kommer att behöva ändras i stora delar när den nya EU-regleringen träder i kraft respektive har implementerats.

Förutom att utredningen borde ha avvaktat beslutet om de nya EU-reglerna, anser Advokatsamfundet att förslaget inte heller tar tillräcklig hänsyn till att aktuella personuppgifter även kan vara känsliga. Därtill finner Advokatsamfundet att säkerhetsfrågorna inte har beaktats och analyserats i tillräcklig grad. Utöver detta finner Advokatsamfundet det vara otillfredsställande att förslaget öppnar för att personuppgifter behandlas för vissa mer eller mindre obestämda sekundära ändamål utan att dessa ändamål närmare analyserats och vilka konsekvenser behandlingen kan medföra. När det dessutom inte har analyserats hur tillgången till uppgifter och informationsflödet mellan

[47] Ds 2015:44 s. 38.

myndigheterna kan komma att påverka den personliga integriteten och rättssäkerheten jämte hur de föreslagna reglerna kan komma att påverka de enskildas förtroende för myndigheternas verksamhet, är detta ytterligare skäl till varför Advokatsamfundet inte kan ställa sig bakom att nuvarande förslag läggs till grund för lagstiftning.

SVERIGES ADVOKATSAMFUND

Anne Ramberg