SVERIGES ADVOKATSAMFUND
Generalsekreteraren

Cirkulär nr 6/2018

Till ledamöterna av Sveriges advokatsamfund

Vägledning för tillämpningen av EU:s dataskyddsförordning i advokatverksamhet

Den 25 maj 2018 ska EU:s dataskyddsförordning börja tillämpas i alla EU:s medlemsstater. Dataskyddsförordningen ställer fler och hårdare krav på de som behandlar personuppgifter. Den ger vidare de nationella tillsynsmyndigheterna utökade befogenheter samt en möjlighet att besluta om administrativa sanktionsavgifter. Med anledning av den nya lagstiftningen har styrelsen för Sveriges advokatsamfund vid sitt sammanträde den 9 mars 2018 antagit bifogad vägledning.

Stockholm den 12 mars 2018

Anne Ramberg

Vägledning för tillämpningen av EU:s dataskyddsförordning i advokatverksamhet

Den 25 maj 2018 ska EU:s dataskyddsförordning (även kallad GDPR) börja tillämpas i alla EU:s medlemsstater. Dataskyddsförordningen ställer fler och hårdare krav på de som behandlar personuppgifter och ger vidare de nationella tillsynsmyndigheterna utökade befogenheter samt en möjlighet att besluta om administrativa sanktionsavgifter. Varje advokatbyrå behöver ha ett väl övervägt och klokt förhållningssätt till detta.

Styrelsen har därför beslutat att ta fram en vägledning för tillämpningen av EU:s dataskyddsförordning i advokatverksamhet och tillsatt en arbetsgrupp, bestående av advokaterna Henrik Bengtsson, Per Furberg, Björn Möller och Caroline Olstedt Carlström, som utarbetat ett förslag till vägledning.

Vägledningen består av två delar. Del I läses som en sammanfattning av vissa grundläggande åtgärder som advokatbyråer behöver vidta för en ansvarsfull databehandling i sin verksamhet, och avslutas med bilagda exempel på sådan dokumentation som bör upprättas. Del II läses som en fördjupad information.

Dataskyddsförordningen är direkt tillämplig i Sverige, men ger visst utrymme för kompletterande nationella bestämmelser. I skrivande stund har några sådana bestämmelser inte antagits. Vägledningen är således baserad på dataskyddsförordningen, den s k artikel 29-gruppens uttalanden som publicerats per den 7 mars 2018 och prop 2017/18:105 Ny dataskyddslag. Vägledningen ska ses som ett levande dokument och kommer att uppdateras löpande, bl a när ny lagstiftning och nya föreskrifter antagits och när rättspraxis tillkommit.

Styrelsen har vid sitt sammanträde den 26 januari 2018 beslutat att remittera vägledningen till de största advokatbyråerna. Sedan inkomna synpunkter beaktats har styrelsen den 9 mars 2018 beslutat att anta vägledningen.

Innehåll

DEL I

SAMMANFATTNING AV GRUNDLÄGGANDE ÅTGÄRDER FÖR EN ANSVARSFULL DATABEHANDLING

1. Grundläggande åtgärder för en ansvarsfull databehandling

1.1 Bakgrund, syfte och omfattning

Den 25 maj 2018 ska dataskyddsförordningen[1] (förordningen kallas också GDPR utifrån den engelska förkortningen) börja tillämpas i alla EU:s medlemsstater. Dataskyddsförordningen ger ett stärkt skydd för de personer vars personuppgifter behandlas (”de registrerade”). Den ställer därmed fler och hårdare krav på de som behandlar personuppgifter för egen eller annans räkning. Förordningen ger vidare de nationella tillsynsmyndigheterna[2] utökade befogenheter och en möjlighet att besluta om administrativa sanktionsavgifter. Varje advokatbyrå behöver ha ett väl övervägt och klokt förhållningssätt till detta.

Personuppgifter skyddas sedan den 1 oktober 1998 av personuppgiftslagen (1998:204) (”PuL”) och många av de principer och regler som följer av dataskyddsförordningen framgår redan av PuL. De största skillnaderna till följd av att dataskyddsförordningen träder ikraft är:

- Lagstiftningen får formen av en EU-förordning som är direkt tillämplig i alla medlemsländer, medan PuL var en nationell svensk implementering av dataskyddsdirektivet. Ambitionen är att detta ska leda till en mer enhetlig rättstillämpning inom unionen.
- De grundläggande principerna för personuppgiftsbehandling förtydligas.
- Informationsskyldighet i förhållande till de registrerade utökas.
- Rättigheter för de registrerade i förhållande till den personuppgiftsansvarige utökas.
- Den personuppgiftsansvarige blir skyldig att visa att dataskyddsförordningen efterlevs. Detta innebär omfattande dokumentationsskyldighet (exempelvis krav på registerförteckning, konsekvensbedömning och gallringsrutiner).
- Kraftfulla sanktioner (sanktionsavgift på upp till två eller fyra procent av den globala årsomsättningen för en koncern, eller – om det är högre – upp till 10 eller 20 miljoner euro) vid allvarliga överträdelser. Överträdelser av PuL har normalt lett till påpekanden från Datainspektionen och i undantagsfall till förbud.

Syftet med denna vägledning är att ge advokatbyråer och deras medarbetare närmare vägledning för hur de bör behandla personuppgifter och förfara med dokumentationskrav, informationskrav etc.

Riktlinjerna är baserade på dataskyddsförordningen, artikel 29-gruppens uttalanden[3] som publicerats per den 7 mars 2018 och prop 2017/18:105 Ny dataskyddslag[4]. Datainspektionen kommer inför dataskyddsförordningens ikraftträdande att behöva ändra Datainspektionens

[1] 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 (allmän dataskyddsförordning).

[2] I Sverige Datainspektionen, föreslagen att namnändras till Integritetsskyddsmyndigheten.

[3] Uttalandena finns tillgängliga på adressen http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

[4] Propositionen finns tillgänglig på adressen https://data.riksdagen.se/fil/B9422B71-F595-4053-9740-A1349BFE80F7

föreskrifter, vilket inte gjorts när dessa riktlinjer antagits. Artikel 29-gruppen kommer vidare att anta fler uttalanden. Riktlinjerna är därför ett levande dokument som kommer att uppdateras när ny lagstiftning och nya föreskrifter antagits.

Vägledningen består av två delar. Del I läses som en sammanfattning av vissa grundläggande åtgärder som en advokatbyrå behöver vidta för en ansvarsfull databehandling i sin verksamhet, och avslutas med bilagda exempel på sådan dokumentation som bör upprättas. Del II läses som en fördjupad information. Där behandlas grunderna för de olika kraven och de nya reglerna redogörs för i väsentliga delar.

1.2 Advokatbyrån behöver besvara följande frågor

Varje advokatbyrå bör ha processer och dokumentation på plats för att kunna besvara följande frågor:

1. Är alla i organisationen informerade om dataskyddsförordningen och de processer som ska tillämpas för att följa regelverket?
2. Har vi en laglig grund för varje behandling av personuppgifter som vi genomför?
3. För vilka ändamål behandlar vi personuppgifterna?
4. Är de registrerade medvetna om våra åtgärder med personuppgifterna?
5. Hur säkerställer vi att uppgifterna är korrekta och, vid behov, uppdaterade?
6. Gallrar vi eller anonymiserar på ett tillfredsställande sätt sådana personuppgifter som vi inte längre har skäl att behandla (såvida inte lag eller annan författning föreskriver att informationen ska bevaras)?
7. Har vi processer på plats för att kunna respektera de registrerades rättigheter såsom att få kopia på den information som behandlas, korrigering eller radering etc?
8. Uppfyller våra processer tillämpliga säkerhetskrav och har de som ges tillgång till och hanterar personuppgifter fått erforderlig utbildning för denna hantering?
9. Iakttar vi gällande dataskyddsregler när vi väljer en leverantör eller delar data med t ex klienter eller leverantörer? Har vi rätt avtalsreglering på plats?

Genom god dokumentation och etablerade processer för att hantera dessa frågor kan verksamheten bedrivas på ett sätt som är förenligt med dataskyddsförordningen. I denna vägledning lämnas exempel på viss dokumentation som bör upprättas och här återfinns också närmare information om de legala kraven.

De typiska bristerna när det gäller efterlevnaden av PuL och som återkommande påpekats i Datainspektionens tillsynsbeslut har annars varit följande.

- Otillräcklig information ges till de registrerade, eller information som inte är korrekt när det gäller exempelvis ändamålet för behandlingen.
- Personuppgiftsbiträdesavtal saknas.
- Registerförteckning saknas.
- Överföring till tredje land sker i strid med lag.
- Gallringsrutiner saknas och personuppgifter behandlas under för lång tid.

- Otillräcklig behörighetsbegränsning finns för åtkomst till data/dokument.
- Rutiner för att lämna information till de registrerade efter begäran saknas.

Med den reglerade ansvarsskyldigheten enligt dataskyddsförordningen, där advokatbyrån är ansvarig för och ska kunna visa att principerna för behandling av personuppgifter är uppfyllda, behöver sådana krav hanteras. En översiktlig genomgång av åtgärder för en ansvarsfull databehandling följer i 1.3 nedan.

1.3 Åtgärder för en ansvarsfull databehandling

Dataskyddsförordningen lägger stor vikt vid den personuppgiftsansvariges (advokatbyråns) skyldighet att kunna visa att förordningen och dess grundläggande principer för behandling av personuppgifter följs, vilket medför krav på ökad dokumentation och tydligare processer än vad som gällt enligt PuL. Nedan listas ett antal olika åtgärder som bör övervägas för att på ett bra sätt kunna uppfylla förordningens krav.

1.3.1 Advokatbyrån behöver kartlägga sin behandling av personuppgifter och skapa en registerförteckning

Advokatbyrån behöver inventera och dokumentera all behandling av personuppgifter, inbegripet hur och varför informationen samlas in, till vem uppgifterna lämnas ut samt om korrekt information har lämnats till de registrerade. Advokatbyrån behöver även undersöka med vilket rättsligt stöd en behandling av uppgifterna sker.

Detta sker enklast genom en inledande kartläggning (se bilaga 1 för exempel på registerförteckning[5] samt Del II i denna vägledning för närmare information om de grundläggande principerna för behandling av personuppgifter, registerförteckning m m). En noggrann kartläggning hjälper byrån att uppfylla dataskyddsförordningens krav, bl a på att kunna visa att förordningens bestämmelser följs. Den kan också ge underlag för andra åtgärder såsom gap-analys och uppföljning.

Typiska IT-system som förekommer i advokatverksamhet är klient- och motpartsregister, tidredovisningssystem, ärendehanteringssystem/filsystem för ord- och textbehandling, e-postsystem, medarbetares kontaktregister, kalendersystem, HR-system, system för rekrytering och utvärdering av anställda etc. De typiska ändamålen för vilka advokatbyrån behandlar personuppgifter är bedömning av jävsfrågor och penningtvättsfrågor, tillvaratagande av klients rättsliga intressen och behandling för administrativa ändamål. Andra interna ändamål är administration och uppföljning av rekrytering och anställning.

Advokatbyrån bör utse en ägare till registerförteckningen, eftersom den behöver vara ett levande dokument som uppdateras vid varje ny personuppgiftsbehandling eller när en behandling förändras eller upphör.

---

[5] Notera att det formellt sett inte är ett krav för alla organisationer att ha ett register av det slag som GDPR beskriver i Art 30. I praktiken behöver dock varje organisation *inventera* och *dokumentera* behandlingen på en lämplig nivå, varför ett artikel 30-register ändå kan vara ett praktiskt sätt.

Det finns även ett antal olika elektroniska verktyg på marknaden som kan användas för ändamålet om det är fråga om en mer omfattande verksamhet. Dessa verktyg underlättar som regel även senare den löpande förvaltningen av registret över behandlingar.

1.3.2 Advokatbyrån behöver fastställa om det finns en laglig grund för behandlingen av personuppgifter

Av dataskyddsförordningen (liksom PuL) följer att personuppgifter får behandlas endast om det finns en laglig grund för behandlingen. Vanligt förekommande lagliga grunder för en advokatbyrås behandlingar är att de är nödvändiga för att fullgöra ett avtal (t ex avtal med klient eller anställd), att de är tillåtna efter en intresseavvägning (t ex viss marknadsföring), att de är nödvändiga för att fullgöra en rättslig förpliktelse (t ex skicka information till Skatteverket eller Försäkringskassan), för att fullgöra en uppgift av allmänt intresse (t ex i egenskap av offentliga försvarare), eller sker som ett led i myndighetsutövning (t ex i egenskap av notarius publicus). Generellt sett bör samtycke som laglig grund däremot försöka undvikas där så är möjligt.

1.3.3 Advokatbyrån behöver utbilda sin personal rörande dataskyddsförordningen

Alla medarbetare som har tillgång till eller behandlar personuppgifter behöver få information och utbildning om vilka regler som gäller och hur advokatbyråns anställda ska hantera berörda frågor och interna processer. Dessa insatser bör dokumenteras i en logg och upprepas i någon form åtminstone en gång per år för alla anställda.

1.3.4 Advokatbyrån behöver se över sin information till de olika kategorierna av registrerade

Den information som nu lämnas till registrerade bör granskas. Advokatbyrån behöver anpassa informationen till dataskyddsförordningens krav på utökad information. De typiska kategorierna av registrerade är klienter, presumtiva klienter som är föremål för marknadsföringsåtgärder, leverantörer, personer som söker anställning och anställda. Informationsskyldigheten omfattar inte motparter eller tredje parter vars information behandlas i ett ärende om uppgifterna inte samlats in direkt från dem.[6] Alla registrerade har rätt till tydlig och lättförståelig information om hur deras personuppgifter behandlas, för vilka syften, om uppgifterna exporteras till tredje land samt av vem och under vilken tid de behandlas. Informationen kan lämnas i en integritetspolicy eller motsvarande som exempelvis kan publiceras på advokatbyråns hemsida eller överlämnas i tryckt form. Se ett exempel på information till den registrerade i bilaga 3.

[6] Undantag från informationsskyldigheten gäller för sådana ärenden som omfattas av advokatens tystnadsplikt enligt rättegångsbalken, se den fördjupade informationen i Del II.

1.3.5 Advokatbyrån behöver hantera särskilda integritetsrisker i advokatverksamheten

Advokatbyrån i sin egenskap av personuppgiftsansvarig behöver ha en rutin på plats för att kunna identifiera och hantera särskilda integritetsrisker inom verksamheten. Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med en viss typ av behandling av uppgifter, särskilt känsliga uppgifter, behandling i särskilt stor omfattning, användning av ny teknik eller dylikt. I vissa mer ovanliga fall kan en formaliserad s k konsekvensbedömning avseende dataskydd (ett dokument för strukturerad uppföljning) aktualiseras, exempelvis vid införande av AI-teknik eller annan avancerad teknik för behandling av personuppgifter, särskilt om tekniken används för systematisk övervakning av exempelvis byråns anställda eller av andra personer. Se närmare den fördjupade informationen i Del II samt bilaga 4.[7]

1.3.6 Advokatbyrån är skyldig att rapportera personuppgiftsincidenter till Datainspektionen och ge information till de registrerade

Det behöver införas rutiner för att upptäcka, rapportera, dokumentera och utreda personuppgiftsincidenter och för att skyndsamt hantera sådana incidenter. Det behöver införas en process för detta och det behöver säkerställas att teknisk övervakning av systemen sker på en tillräcklig nivå för att kunna upptäcka eventuella incidenter. Kraven behöver uppfyllas också i förhållande till andra som behandlar personuppgifter åt advokatbyrån (personuppgiftsbiträden) och dokumenteras i avtal. När det inte är osannolikt att en incident medför risker för enskildas fri- och rättigheter måste händelsen anmälas till Datainspektionen inom 72 timmar. Om incidenten kan leda till att personer utsätts för allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella stölder kan även de registrerade behöva informeras om händelsen så att de kan vidta nödvändiga åtgärder.

1.3.7 Advokatbyrån bör upprätta interna styrande dokument såsom integritetspolicy etc

Advokatbyrån bör ta fram en intern integritetspolicy med information om hur personuppgifter ska hanteras av alla anställda och vilka regler som gäller internt, se bilaga 2 för ett exempel på en enkel policy. Policyn bör även göras enkelt tillgänglig, t ex på intranät, samt tydligt informeras om till alla anställda som en del i den utbildning av personalen som berörts ovan.

Andra styrande dokument som behöver övervägas är t ex informationssäkerhetspolicy, gallringspolicy, instruktion till anställda om hur personuppgifter ska/inte får behandlas i e-post eller annat ostrukturerat material, checklista/mall vid anlitande av underleverantör/personuppgiftsbiträde, osv.

---

[7] Även avseende dessa konsekvensbedömningar börjar det nu dyka upp olika elektroniska verktyg på marknaden som kan användas för ändamålet. Dessa verktyg kan underlätta dokumentation och uppföljning i en mer omfattande verksamhet.

1.3.8 Advokatbyrån behöver se över avtal med underleverantörer som behandlar personuppgifter för advokatbyråns räkning (personuppgiftsbiträdesavtal)

Det är advokatbyrån som är personuppgiftsansvarig och som ansvarar för behandlingen av personuppgifter. Det här förändras inte även om behandlingen skulle utföras av ett s k personuppgiftsbiträde, d v s av någon som behandlar personuppgifter för advokatbyråns räkning (exempelvis leverantörer av molntjänster, IT-back-up och extern hantering av lönesystem). Även underleverantörer till ett personuppgiftsbiträde är att anse som personuppgiftsbiträden när de hanterar personuppgifter som advokatbyrån är ansvarig för. Advokatbyrån ansvarar för att endast anlita biträden som ger tillräckliga garantier om att lämpliga tekniska och organisatoriska åtgärder genomförs, så att behandlingen kan uppfylla kraven i förordningen och de registrerades rättigheter skyddas.

När advokatbyrån anlitar ett personuppgiftsbiträde ska det finnas ett skriftigt avtal, ett så kallat personuppgiftsbiträdesavtal, som reglerar behandlingen. Kraven på personuppgiftsbiträdesavtalen har i många avseenden förtydligats, vilket innebär att även befintliga sådana avtal som regel behöver uppdateras.

1.3.9 Missbruksregeln upphör att gälla

PuL:s undantag för att behandla personuppgifter i ostrukturerat material, den så kallade missbruksregeln, upphör att gälla. Advokatbyrån behöver därför undersöka om de behandlingar som äger rum idag och stöds på missbruksregeln (exempelvis e-postsystem och publicering av information på hemsida) kan förenas med dataskyddsförordningen. Nya rutiner och interna instruktioner kan behövas i denna del för att få en god kontroll över var och hur behandling sker.

1.3.10 Advokatbyrån behöver införa gallringsrutiner och se över hur länge personuppgifter lagras och behandlas

Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det innebär att uppgifter kan behöva gallras fortlöpande eller att andra åtgärder kan krävas (t ex att åtkomstbegränsningar införs). Det kan dessutom finnas krav i annan författning på att bevara uppgifter viss tid, t ex för redovisnings- eller arkivändamål. Genom en gallringspolicy eller någon annan plan för dokumenthantering kan dessa åtgärder tydliggöras och införas i verksamheten.

Även personuppgifter i ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser o s v behöver raderas när ändamålet med behandlingen är uppfyllt. För att hantera detta behöver en bedömning alltid göras för vilket ändamål exempelvis ett e-postmeddelande eller dokument ska sparas och var (t ex kundregistret, ärendet etc).

Det finns inte någon bestämd tidsperiod för hur länge personuppgifter får behandlas, utan tidsperioden måste bedömas från fall till fall utifrån det ursprungligen angivna ändamålet med behandlingen.

Nedan följer några riktlinjer som kan användas vid framtagande av gallringsrutiner för personuppgifter:

- Advokaters arkiveringsskyldighet enligt 7.12.2 Vägledande regler om god advokatsed (VRGA) innebär enligt Advokatsamfundets bedömning att det är nödvändigt med arkivhållning i tio år av handlingar som ansamlats i ett uppdrag.
- Om advokatbyrån har någon pågående relation med den registrerade kan detta påverka gallringstiden.
- Ändamålet med behandlingen kan tala för en längre gallringstid.
- Om det föreligger något rättsligt krav (exempelvis enligt bokföringslagen, penningtvättsregleringen[8] eller skattelagstiftningen) för att bevara visst underlag under viss tid ska detta beaktas.

1.3.11 Advokatbyrån behöver införa rutiner för att säkerställa de registrerades rättigheter

Utöver en rutin för att lämna information till registrerade, behöver advokatbyrån också etablera förfaranden för att hantera registrerades förfrågningar om registerutdrag, begäran om att få felaktiga uppgifter rättade eller att få uppgifter raderade, invändningar mot direkt marknadsföring eller automatiserat beslutsfattande, eller begäran om s k dataportabilitet (se vidare den fördjupade informationen i Del II nedan). Sådana etablerade förfaranden bör införas för olika kategorier av registrerade (t ex för anställda och arbetssökande, klienter och leverantörer), eftersom förutsättningarna för att tillmötesgå en begäran kan skilja sig åt mellan de olika kategorierna.

Innan utlämnande av registerutdrag eller personuppgifter i övrigt sker behöver dock mottagaren verifieras, så att det är säkerställt att informationen lämnas ut till rätt person.

1.3.12 Advokatbyrån behöver se över den tekniska säkerheten

Advokatbyrån kan behöva införa nya rutiner för informationssäkerhet och IT-system kan behöva anpassas av säkerhetsskäl. Dessa frågor kan hanteras genom ändringar i eller införande av en ny IT-policy där det bör finnas bl a generella användarregler för respektive applikation, system och verktyg och hantering av eventuella fritextfält, regler om behörighetsstyrning och åtkomstbegränsning samt bestämmelser rörande säkerhetskopiering m m.

Exempel på åtgärder som måste kontrolleras är om advokatbyrån har tillräckliga rutiner för back-up, tillräckliga brandväggar, lösenordskyddade trådlösa nätverk, uppdaterat virusskydd, lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor, skydd mot obehörig intern åtkomst, lösenordskrav, kryptering vid behov, loggning av åtkomst till och användning av IT-system m m.

---

[8] Se närmare om behandling av personuppgifter för penningtvättssyften Advokatsamfundets Penningtvättsvägledning avsnitt 15, s 50–52.

1.3.13 Advokatbyrån behöver säkerställa att uppgifter som överförs till tredje land skyddas på ett adekvat sätt[9]

Advokatbyråer som använder t ex IT-leverantörers eller andra underleverantörers produkter och tjänster (såväl extern leverantör som koncernbolag i en större advokatverksamhet/koncern) anlitar normalt leverantörer som behandlar personuppgifter. Denna behandling är advokatbyrån ansvarig för. Därmed behöver bl a en kontroll göras i vad mån underleverantören behandlar uppgifterna, eller bereder sig tillgång till uppgifterna från tredje land.[10] I en sådan situation behöver det säkerställas att överföringen till tredje land är acceptabel och att någon relevant överföringsmekanism är tillämplig på överföringen (se ovan om personuppgiftsbiträdesavtal med underleverantörer respektive den fördjupade informationen i Del II om förutsättningarna för överföring till tredje land).

1.3.14 Advokatbyrån behöver anpassa uppdragsavtal, anställningsavtal m m

En genomgång behöver göras av alla befintliga avtal som advokatbyrån har tecknat för en bedömning av om tillräckliga regleringar utifrån dataskyddsförordningens krav finns i avtalen. Innehållet i befintliga avtal, anställningsavtal, separata personuppgiftspolicyer/informationstexter etc behöver ses över med avseende på den information som advokatbyrån lämnar till registrerade om hur byrån behandlar dennes personuppgifter. Tilläggsavtal och/eller uppdatering av separata personuppgiftspolicyer/informationstexter kan således behöva upprättas och/eller kommuniceras i anslutning till vissa befintliga avtal.

Även uppdragsavtal och personuppgiftspolicyer/informationstexter gentemot klienter behöver ses över med avseende på informationen till de registrerade. Förändringar eller tillägg kan behöva göras för att lämna tydlig information om hur advokatbyrån behandlar personuppgifterna (avser såväl kontaktuppgifter till klient etc som personuppgifter som advokatbyrån kan komma att erhålla inom ramen för ett ärende) och även en ansvarsbegränsning i det här avseendet kan vid behov övervägas.[11]

Här bör observeras att behovet av information till registrerade kan skilja sig åt. Uppdragsgivaren/klienten är många gånger en juridisk person, varmed det inte är tillräckligt att lämna information om behandling till klienten. Advokatbyrån behöver därför även finna lämpligt sätt att informera de kontaktpersoner och andra hos klienten vars personuppgifter

---

[9] Med ”tredje land” avses fortsättningsvis länder utanför EES området och länder eller territorier eller sektorer som Kommissionen har beslutat säkerställer en adekvat skyddsnivå (dessa länder/territorier/sektorer är för närvarande Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Isle of Man, Israel, Jersey, Nya Zeeland, Schweiz, Uruguay, Kanada (om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling) och USA (om mottagaren har anslutit sig till Privacy Shield) Överföring av personuppgifter till tredjeländer eller territorier som anses ha en adekvat skyddsnivå kräver enligt artikel 45 (1) inte något särskilt tillstånd.

[10] D v s loggar in från annan plats belägen i tredje land.

[11] Det kan däremot ifrågasättas om en sådan ansvarsbegränsning kan upprätthållas i förhållande till de registrerade (jfr artikel 82 i dataskyddsförordningen).

behandlas hos advokatbyrån. Ett sätt kan vara att lämna över ett skriftligt dokument med information som klienten kan överlämna till berörda personer.

1.3.15 Advokatbyrån behöver se över behandlingen av särskilda kategorier av uppgifter, behandling av personnummer och uppgifter om lagöverträdelser

När advokatbyrån behandlar s k särskilda kategorier av personuppgifter (”känsliga personuppgifter”) krävs ett giltigt undantag från huvudregeln som annars föreskriver att behandling av känsliga personuppgifter är förbjuden. Känsliga personuppgifter är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska eller biometriska uppgifter, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Personnummer utgör inte per definition känsliga personuppgifter, men kräver ändå särskilda överväganden. Behandling av personnummer får bara utföras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl (3 kap 10 § förslaget till ny dataskyddslag).

Behandling av uppgifter om lagöverträdelser (fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder, men sannolikt inte uppgift om misstanke om brott[12]) får enligt 3 kap 9 §, 2 st i förslaget till dataskyddslag endast behandlas i enlighet med beslut från Datainspektionen (bestämmelsen motsvarar delvis 21 § PuL).

Ovanstående innebär att advokatbyrån särskilt behöver identifiera och dokumentera med vilket undantag och/eller mot bakgrund av vilka särskilda överväganden som den här typen av personuppgifter behandlas.

Idag gäller dock två betydelsefulla undantag som har förordnats av Datainspektionen, nämligen (i) att advokatbyråer får behandla personuppgifter om behandlingen är nödvändig för kontroll av att jävssituation inte föreligger och (ii) att advokatbyrån får behandla enstaka uppgift som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall.[13] Datainspektionen behöver ge ut nya föreskrifter i anslutning till att dataskyddsförordningen och dataskyddslagen träder ikraft och Advokatsamfundet utgår från att Datainspektionen meddelar föreskrifter som i vart fall innehåller de undantag som finns idag. Vidare föreligger även med stöd av penningtvättslagen ytterligare ett undantag där (iii) advokatbyrå har rätt att behandla personuppgifterna för att fullgöra sina rättsliga förpliktelser enligt penningtvättslagen om att undersöka risker som kan förknippas med klienten etc.[14]

I övrigt får känsliga personuppgifter även behandlas bl a om den registrerade har lämnat sitt samtycke till behandlingen, behandlingen är nödvändig för att kunna fullgöra skyldigheter

---

[12] Se prop 2017/18:105 s 98 f.

[13] Se DIFS 2010:1 1 § c) och d).

[14] 5 kap 6 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

och utöva rättigheter inom arbetsrätten, behandlingen är nödvändig för att skydda fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke etc. För förtydliganden, se den fördjupade informationen i Del II.

1.3.16 Telefon- och klientregister i advokatverksamhet

Advokatbyrån är personuppgiftsansvarig för de register som förs inom advokatverksamheten. Det här gäller exempelvis för sedvanliga telefon- och klientregister. För alla register som hålls inom ramen för advokatverksamheten måste advokatbyrån identifiera ändamål, laglig grund samt bevarandetider. Ändamålet med att hålla telefon- och klientregistren är normalt sett behandling för administrativa ändamål, för klientregistret även för undvikande av intressekonflikt, och behandlingen kan ske såväl med stöd av avtal som efter en intresseavvägning. Gallring behöver ske i registren när informationen i de olika posterna i registren inte längre är nödvändig för det uppgivna ändamålet och här bör advokatbyrån sätta en rimlig gallringstid och implementera en process som fungerar.

Eftersom klientregistret hos många advokatbyråer utgör söknyckel till arkivet behöver informationen i klientregistret bevaras under hela arkiveringsskyldigheten, jfr 7.12.2 VRGA. Klientregister är centrala för att advokater ska kunna fullgöra den intressekonfliktskontroll-skyldighet som följer av 3.3 VRGA. Enligt Advokatsamfundets uppfattning är det nödvändigt för advokater att bevara information om klienter och ärenden under i vart fall tio år från det att uppdraget slutfördes, eller den längre tid som uppdragets natur påkallar. En intressekonflikt som innebär hinder för advokaten att acceptera ett uppdrag är ofta historisk och intressekonfliktsbedömningen kan exempelvis kräva att advokaten sätter sig in i hur klientrelationer såg ut bakåt i tiden.[15]

1.3.17 Advokats tystnadsplikt

Advokatens tystnadsplikt och diskretionsplikt regleras i 8 kap 4 § rättegångsbalken men även i VRGA. Enligt 2.2.1 VRGA har en advokat tystnadsplikt avseende det som anförtrotts advokaten inom ramen för advokatverksamheten, eller som advokaten i samband därmed fått kännedom om. Undantag från tystnadsplikten gäller i vissa särskilt angivna fall. I fråga om tystnadsplikten är det advokatverksamheten som utgör ramen för tystnadsplikten. Verksamheten är dock en vidare ram än uppdraget och innebär exempelvis att även information som advokaten får från en presumtiv klient, där något uppdrag ännu inte föreligger, kan omfattas av tystnadsplikten.

Ovannämnda lagstadgade skyldighet avser dock endast verksamheten som advokat. I tillägg till detta föreskrivs en tystnadsplikt för dataskyddsombud, varom närmare nedan samt i Del II av denna vägledning.

---

[15] Här behöver dock en bedömning göras avseende vilken information som är nödvändig för att uppfylla intressekonfliktkontroll. Personuppgifter som inte behövs för sådan kontroll behöver gallras tidigare.

1.3.18 Dataskyddsombud

Privata organisationer är skyldiga att utse ett dataskyddsombud om deras kärnverksamhet består av behandling som på grund av sin karaktär, omfattning och/eller ändamål kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning. Advokatsamfundets uppfattning är att det här kravet inte gäller för sedvanlig advokatverksamhet som bedrivs på sätt som följer av lag, Advokatsamfundets stadgar och VRGA.

Om advokatbyråns kärnverksamhet däremot består av behandling i stor omfattning av särskilda kategorier av uppgifter eller personuppgifter som rör fällande domar i brottmål eller överträdelser (se den fördjupade informationen i Del II) ska ett dataskyddsombud däremot utses. Om advokatbyrån väljer att utse ett dataskyddsombud trots att den inte är skyldig att göra det blir reglerna avseende dataskyddsombud i dataskyddsförordningen tillämpliga även på det frivilligt utsedda dataskyddsombudet.

Regeringen föreslår i propositionen till dataskyddslagen att den som fullgör uppgift som dataskyddsombud enligt dataskyddsförordningen inte obehörigen ska få röja det som han eller hon vid fullgörandet av sin uppgift har fått kännedom om.

1.4 Införande

Varje advokatbyrå bör göra denna vägledning känd inom sin verksamhet, exempelvis genom att vägledningen tillhandahålls digitalt och genom att ledning eller styrelse särskilt ser till att medarbetarna uppmärksammas på innehållet och följer regelverket. Vidare bör en kontaktperson för eventuella frågor om dataskydd utses inom organisationen.

Bilaga 1

Exempel – Registerförteckning över behandling av personuppgifter

- Personuppgiftsansvarig advokatbyrå:
- Dataskyddsombud eller annan kontaktperson:

System/ accesspunkt	Behandlingens namn	Kategori av registrerade	Kategorier av mottagare av personuppgifterna	Kategori av personuppgifter	Dokumentation om överföring av personuppgifter sker till tredje land	Beskrivning av ändamålen med behandlingen	Laglig grund	Lagringstid	Dokumentation om personuppgiftsbiträden anlitas för behandlingen	Kommentarer

- Allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som advokatbyrån vidtagit för att säkerställa en säkerhetsnivå som är lämplig:

Bilaga 2

Exempel – Integritetspolicy[16]

[ADVOKATBYRÅNS] POLICY FÖR BEHANDLING AV PERSONUPPGIFTER

1 Bakgrund och syfte

1.1 [Advokatbyrån] värnar om sina klienters, partners och anställdas integritet och är alltid mån om att följa gällande dataskyddsregelverk. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

1.2 [Advokatbyrån] har därför antagit denna Policy för behandling av personuppgifter för att säkerställa att alla inom organisationen följer dataskyddsreglerna. Det här dokumentet avser att ge dig som medarbetare närmare vägledning om hur du ska behandla personuppgifter.

1.3 Den 25 maj 2018 börjar dataskyddsförordningen tillämpas. Den medför ett förstärkt skydd för de personer vars personuppgifter behandlas och den ställer fler och hårdare krav på organisationer som behandlar personuppgifter.

1.4 Om en behandling av personuppgifter skulle strida mot bestämmelserna i dataskyddsförordningen finns risken för intrång i den personliga integriteten för de registrerade, men även risken för skadat anseende för [advokatbyrån]. Vidare kan byrån dessutom bli skyldig att utge skadestånd eller påföras en administrativ sanktionsavgift på upp till tjugo miljoner euro eller 4 % av den totala globala årsomsättningen, beroende på vilket värde som är högst. För att undvika sådana konsekvenser är alla medarbetare skyldiga att följa dessa riktlinjer.

2 Tillämpningsområde och omfattning

2.1 Policyn gäller för [advokatbyråns] alla anställda och konsulter, på alla marknader och vid var tid.

2.2 [Advokatbyråns] styrelse ska se till att denna Policy efterlevs, vilket bland annat innefattar utbildning för alla anställda. Informationen till de anställda ska även innefatta information om att överträdelse av policyn kan komma att medföra t ex arbetsrättsliga konsekvenser.

---

[16] Notera att det för vissa avdelningar, särskilt i större organisationer, kan behövas kompletterande mer detaljerade arbetsinstruktioner för hanteringen av personuppgifter på avdelningen (t ex personalavdelning, marknadsavdelning o s v).

2.3 [För vissa avsnitt finns utarbetade rutiner och formulär som ska användas vid behov. Medarbetare finner länkar till dessa rutiner och formulär angående den aktuella frågan på [intranätet under ◆].]

3 Grundläggande principer

3.1 De grundläggande principer som beskrivs nedan ska alltid iakttas när personuppgifter behandlas. [Advokatbyrån] ansvarar för och ska kunna visa att principerna efterlevs.

3.1.1 *Laglighet, skälighet, transparens* – Personuppgifter ska behandlas lagligt, korrekt och transparent i förhållande till den registrerade. Det innebär att varje typ av behandling ska baseras på en giltig s k laglig grund, såsom exempelvis fullgörande av avtal, fullgöra en rättslig förpliktelse, utföra en uppgift av allmänt intresse, berättigat intresse eller samtycke (se avsnitt 5 nedan). Kan man inte identifiera någon laglig grund som är tillämplig för behandlingen får behandlingen således inte utföras. Utgångspunkten för denna princip är tydlig kommunikation med den registrerade om bl a för vilka ändamål personuppgifterna behandlas, vilken typ av behandling som utförs, om och hur personuppgifterna delas med andra, hur länge personuppgifterna lagras och hur man kommer i kontakt med [advokatbyrån]. De registrerade ska alltså ges tydlig och transparent information om behandlingen av deras personuppgifter.

3.1.2 *Ändamålsbegränsning* – Personuppgifter får endast samlas in och på annat sätt behandlas för särskilda, uttryckligt angivna och berättigade ändamål och de får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

3.1.3 *Uppgiftsminimering* – Personuppgifter som behandlas ska vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålen. Säkerställ att uppgifterna som samlas in verkligen behövs och fråga inte efter information bara för att den kanske kan vara bra att ha.

3.1.4 *Riktighet* – personuppgifter som behandlas ska vara korrekta och om nödvändigt uppdaterade. Vidta lämpliga åtgärder för att se till att felaktiga eller ofullständiga uppgifter rättas, exempelvis rutiner för ändring av adress vid flytt med en sammanställning av system och register där adressen lagras. Undvik dock att lagra kopior av uppgifterna i många system i syfte att undvika felkällor och att ouppdaterad information sparas.

3.1.5 *Lagringsbegränsning* – Personuppgifter får inte lagras under längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs måste dessa gallras, vilket innebär att de antingen måste raderas eller avidentifieras.

3.1.6 Principen om ansvarsskyldighet innebär att [advokatbyrån] måste kunna visa att dataskyddsförordningen efterlevs. Byrån måste därför exempelvis dokumentera implementerade och planerade processer och åtgärder som avser dataskyddsfrågor.

Vidare ska det finnas ett register över alla typer av behandlingar av personuppgifter som utförs och [advokatbyrån] ska kunna redovisa ett sådant register för tillsynsmyndigheten när så krävs.

4 Personuppgifter

4.1 *Personuppgifter* är alla uppgifter som avser en identifierad eller identifierbar fysisk person och som direkt eller indirekt kan identifiera en person. Exempel på personuppgifter är namn, kontaktuppgifter, lokaliseringsuppgifter eller faktorer som är specifika för en persons fysiska, ekonomiska, kulturella eller sociala identitet. Uppgifter som enskilt inte når upp till kraven kan tillsammans ändå utgöra personuppgifter.

4.2 All behandling av personuppgifter omfattas av dataskyddsförordningen och dess regler. Med *behandling* menas en åtgärd eller kombination av åtgärder avseende personuppgifter, som utförs helt eller delvis automatiserat. Även personuppgifter i e-post och i dokument på servrar, i en enkel lista, på webbplatser och i annat ostrukturerat material omfattas.

4.3 Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa eller uppgifter om en persons sexualliv eller sexuella läggning (s k *särskilda kategorier av personuppgifter*) är som huvudregel förbjuden. För att sådan behandling ska vara tillåten krävs ett giltigt undantag från förbudet. De vanligaste undantagen är att den registrerade lämnat samtycke eller själv offentliggjort uppgifterna, för att utöva rättigheter eller fullgöra skyldigheter inom arbetsrätten, för att kunna fastställa, göra gällande eller försvara rättsliga anspråk eller för hälso- och sjukvårdsändamål.

4.4 Behandling av *personnummer* får bara utföras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

4.5 Behandling av uppgifter om *lagöverträdelser* (fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder men sannolikt inte uppgift om misstanke om brott) får endast behandlas i vissa särskilda fall. Som advokatbyrå får vi behandla personuppgifter om (i) behandlingen är nödvändig för kontroll av att jävssituation inte föreligger, (ii) enstaka uppgift som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall eller (iii) för penningtvättskontroll.

5 Laglig grund för behandlingen av personuppgifter

5.1 En behandling av personuppgifter är endast laglig om och i den mån någon av följande grunder är tillämplig.

5.1.1 Den registrerade har lämnat sitt *samtycke* till att personuppgifterna behandlas för ett eller flera specifika ändamål. Särskilda krav finns som måste vara uppfyllda för att samtycket ska vara giltigt.

5.1.2 Behandlingen är nödvändig för att *fullgöra ett avtal* i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

5.1.3 Behandlingen är nödvändig för att *fullgöra en rättslig förpliktelse* som åvilar [advokatbyrån]. Som exempel kan här nämnas kontrolluppgifter som lämnas till Skatteverket.

5.1.4 Behandlingen är nödvändig för att skydda intressen som är av *grundläggande betydelse* för den registrerade eller för en annan fysisk person (t ex när det är fara för livet).

5.1.5 Behandlingen är nödvändig för att utföra en *uppgift av allmänt intresse* (t ex som offentlig försvarare) eller som ett led i myndighetsutövning (t ex som Notarius Publicus).

5.1.6 Behandlingen är nödvändig för ändamål som rör [advokatbyråns] eller tredje parts intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, (*intresseavvägning*). Vid intresseavvägning tillkommer särskilda krav på dokumentation avseende den bedömning som gjorts.

6 Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering

6.1 Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder. Organisatoriska säkerhetsåtgärder kan innebära att behörighetskontroll används för de system som innehåller personuppgifter, loggning av åtkomst till personuppgifter eller att datorer och dylikt som innehåller personuppgifter ska förvaras så att obehörig åtkomst försvåras och inte lämnas framme. Exempel på tekniska åtgärder som måste kontrolleras är om advokatbyrån har tillräckliga back-up rutiner, tillräckliga brandväggar, lösenordskyddade trådlösa nätverk, uppdaterat virusskydd, lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor, skydd mot obehörig intern åtkomst, lösenordskrav, kryptering vid behov, loggning av, åtkomst till och användning av IT-system m m.

6.2 Personuppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Genom att upprätta och följa en gallringsrutin för respektive databas/behandling säkerställer man det strukturerade gallringsarbetet. Även personuppgifter i så kallat ostrukturerat material såsom i dokument på servrar, i en enkel lista, på webbplatser etc behöver raderas när ändamålet med behandlingen är uppfyllt.

7 Överföring till tredje land

7.1 För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda regler. Dataskyddsförordningen innebär att alla EU:s medlemsstater samt EES-länderna har ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom det området utan begränsningar. För länder utanför det området finns däremot inte några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar. Det här berör varje form av överföring av information över gränserna, t ex många online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser m m och behöver analyseras särskilt.

8 Konsekvensbedömning

8.1 [Advokatbyrån] har en särskild rutin på plats för att kunna identifiera och hantera särskilda integritetsrisker inom verksamheten och för strukturerad uppföljning. Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med en viss typ av behandling av uppgifter, särskilt känsliga uppgifter, behandling i särskilt stor omfattning, användning av ny teknik eller dylikt.

8.2 Om en ny eller ändrad personuppgiftsbehandling i visst avseende sannolikt kan komma att medföra hög risk för fysiska personers rättigheter och friheter ska rutinen följas och en bedömning göras av effekterna av de påtänkta behandlingarna för skyddet av personuppgifter innan behandlingen påbörjas.

8.3 Innan sådan personuppgiftsbehandling påbörjas ska [◆◆] kontaktas för utredning om en konsekvensbedömning krävs och vid behov utförs konsekvensbedömning tillsammans med den ansvarige genom [besvarande av vissa särskilda frågor, arbetsmöten samt riskbedömning].

9 Registerutdrag och utlämnande

9.1 Dataskyddsförordningen ger de registrerade ett flertal rättigheter vad gäller behandling av personuppgifter. Det är [advokatbyråns] uppgift att uppfylla dessa rättigheter och tillse att tillräckliga processer härför finns för att tillmötesgå de registrerade.

9.1.1 Den registrerade har rätt till *information* när personuppgifterna samlas in. Denna information ska tillhandahållas i en lättillgänglig skriftlig form med ett klart och tydligt språk. I dataskyddsförordningen föreskrivs ett antal tydliga krav som måste vara uppfyllda och kraven varierar beroende på om informationen har samlats in från den registrerade själv eller från tredje man.

9.1.2 Den registrerade har rätt att få bekräftelse på huruvida personuppgifter som tillhör denne behandlas, och i sådana fall få en kopia av personuppgifterna (*registerutdrag*). Denna rättighet gäller oberoende av den plats där personuppgifterna behandlas.

9.1.3 Om personuppgifter som behandlas är felaktiga eller ofullständiga kan den registrerade kräva *korrigering*. Om den registrerade visar att ändamålet för vilket personuppgifterna behandlas inte längre är tillåtet, nödvändigt eller rimligt under omständigheterna, ska de aktuella personuppgifterna *raderas*, om det inte finns några lagbestämmelser som anger annat.

9.1.4 Den registrerade har rätt att överföra personuppgifter som denne lämnat till [advokatbyrån] till annan personuppgiftsansvarig (rätt till *dataportabilitet*) om behandlingen stöds på de lagliga grunderna avtal eller samtycke. Personuppgifterna ska tillhandahållas den registrerade i ett strukturerat, allmänt använt och maskinläsbart format. Om det är tekniskt möjligt kan den registrerade begära att uppgifterna överförs direkt till annan personuppgiftsansvarig. Rätten gäller endast för de personuppgifter som den registrerade själv har lämnat till [advokatbyrån].

9.1.5 Den registrerade har i vissa fall rätt att kräva att [advokatbyrån] *begränsar behandlingen* av dennes personuppgifter, d v s begränsar behandlingen till vissa avgränsade syften. Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt att personuppgifterna rättas. Den registrerade kan då begära att behandlingen av personuppgifterna begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska den enskilde informeras om detta.

9.1.6 Den registrerade har rätt att *invända mot behandling* av personuppgifter som stöds på legitimt intresse som rättslig grund. Vid en invändning ska byrån upphöra med behandlingen om man inte kan visa tvingande legitima grunder för behandlingen som överväger den registrerades intressen, rättigheter och friheter eller om behandlingen av personuppgifter utförs för etablering, utövande eller försvar av rättsliga anspråk.

9.1.7 I vissa fall har den registrerade rätt att begära radering av sina personuppgifter (”*rätten att bli bortglömd*”). Ett exempel är när samtycke är den lagliga grunden för behandlingen och den registrerade återkallar sitt samtycke.

9.1.8 När personuppgifter behandlas för *direktmarknadsföring* har den registrerade rätt att när som helst invända mot behandling av personuppgifter om denne. Om en registrerad motsätter sig behandling av personuppgifter för direktmarknadsändamål ska behandling för sådana ändamål upphöra.

10 Personuppgiftsincidenter

10.1 En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring eller obehörig åtkomst till personuppgifter. Exempel på personuppgiftsincidenter kan vara stöld av kundregister, oavsiktligt avslöjande av löneinformation via e-post till fel mottagare, en anställd tar hem en okrypterad arbetsdator som senare stjäls i ett inbrott och som leder till att information om anställda eller kunder avslöjas, personuppgifter publiceras på

webben av misstag, en bärbar dator innehållande personuppgifter tappas bort eller stjäls, m m.

10.2 Personuppgiftsincidenter kan behöva anmälas till tillsynsmyndigheten inom 72 timmar från upptäckten av incidenten om det är sannolikt att det föreligger en risk för fysiska personers rättigheter och friheter. Inträffade incidenter ska dokumenteras och man kan behöva underrätta berörda registrerade.

10.3 Vid en misstänkt personuppgiftsincident kontakta omedelbart [◆◆] på [◆] eller [◆@◆]. Det är sedan [◆◆] som avgör om tillsynsmyndigheten eller de registrerade behöver underrättas.

11 Övrigt

11.1 För definitioner avseende termer som används i den här policyn hänvisas till dataskyddsförordningen.

11.2 Advokatsamfundet har utarbetat en vägledning för tillämpningen av EU:s dataskyddsförordning i advokatverksamhet, vilken [finns tillgänglig på Advokatsamfundets hemsida och vilken] hänvisas till för närmare information.

11.3 Denna policy ska uppdateras årligen eller vid behov baserat på instruktioner från [advokatbyråns] styrelse.

12 Frågor

Vid frågor som anknyter till behandling av personuppgifter, vänligen kontakta [◆◆] på [◆] eller [◆@◆].

Policy antagen av [advokatbyråns] styrelse den [◆◆] 2018.

Bilaga 3

Exempel – Information till registrerade

Nedanstående text är ett exempel avsett för vägledning. Exemplet är inte uttömmande och behöver anpassas för varje advokatbyrås enskilda verksamhet.

Närmare rekommendationer om utformning av information till de registrerade finns i Artikel 29 gruppens Vägledning om information till de registrerade enligt dataskyddsförordningen 2016/679 (Guidelines on transparency under Regulation 2016/679 [17/EN WP260]) som finns tillgängliga här.

[EXEMPEL]
Behandling av personuppgifter – information enligt Dataskyddsförordningen (2016/679/EG)
Advokatbyrån [X] är personuppgiftsansvarig för de personuppgifter avseende kontaktpersoner vi erhåller i samband med uppdrag eller som annars behandlas när uppdraget förbereds eller administreras. Du är inte skyldig att lämna personuppgifter till oss men utan att det sker kan vi inte åta oss ett uppdrag eftersom vi inte kan genomföra nödvändig jävs- och penningtvättskontroll.

Vi behandlar uppgifterna för att genomföra obligatorisk jävs- och (i förekommande fall) penningtvättskontroll, utföra och administrera uppdraget, för att tillvarata dina intressen, för redovisnings- och faktureringsändamål. Dessa uppgifter behandlas på grundval av [ANGE LAGLIG GRUND/LAGLIGA GRUNDER].

Uppgifterna kan också användas för affärs- och metodutveckling, marknadsanalys, statistik och riskhantering. Uppgifterna som behandlas i syfte att utveckla och analysera verksamheten behandlas på grundval av vårt berättigade intresse att utveckla verksamheten och kommunicera med våra kontakter.

Personuppgifter kan komma att överföras mellan advokatbyråns olika koncern- eller systerbolag i syfte att utföra jävs- och penningtvättkontroll, för informations- och kunskapsutbyte och resursallokering. Vi kommer inte att lämna ut personuppgifter till utomstående annat än i de fall då (i) det särskilt överenskommits mellan advokatbyrån och dig, (ii) då det inom ramen för ett visst uppdrag är nödvändigt för att tillvarata dina rättigheter, (iii) om det är nödvändigt för att vi skall fullgöra lagstadgad skyldighet eller efterkomma myndighetsbeslut eller beslut av domstol, eller (iv) för det fall vi anlitar utomstående tjänsteleverantörer som utför uppdrag för vår räkning. Uppgifterna kan komma att lämnas ut till domstolar, myndigheter, motparter och motpartsombud om det är nödvändigt för att tillvarata dina rättigheter.

Personuppgifterna sparas, i enlighet med den skyldighet som åvilar [advokatbyrån] enligt Vägledande regler för god advokatsed, under en tid om tio år från dagen för ärendets slutförande, eller den längre tid som påkallas av ärendets natur. Uppgifter som behandlas i syfte att utveckla, analysera och marknadsföra advokatbyråns verksamhet sparas under en tid om [ANGE TID] efter den senaste kontakten. Om du avanmäler dig från nyhetsbrev eller liknande kommer uppgifterna omedelbart att raderas.

Du har rätt att kostnadsfritt begära information från [advokatbyrån] om användningen av de personuppgifter som rör dig. Vi kommer på din begäran eller på eget initiativ rätta eller radera uppgifter som är felaktiga eller begränsa behandlingen av sådana uppgifter. Du har vidare rätt att begära att dina uppgifter inte behandlas för direktmarknadsföringsändamål. Du har också rätt att få del av dina personuppgifter i ett maskinläsbart format [eller, om det är tekniskt möjligt, att få uppgifterna överförda till en tredje part som du anvisar]. Om du är missnöjd med vår behandling kan du lämna in ett klagomål till en tillsynsmyndighet vilket i Sverige är Datainspektionen (www.datainspektionen.se). Du kan också vända dig till tillsynsmyndigheten i det land där du bor eller arbetar.

[OM UPPGIFTER FÖRS ÖVER TILL TREDJE LAND, VILKET DET KRÄVS LAGSTÖD FÖR ENLIGT ARTIKEL 44–50 SKALL INFORMATION TILLHANDAHÅLLAS OM TILL VILKA LÄNDER ÖVERFÖRINGEN SKER OCH EN LÄNK TILL PRIVACY SHIELD ELLER ANNAT REGELVERK SOM GARANTERAR SKYDDET FÖR PERSONUPPGIFTERNA.]

[OM ADVOKATFIRMAN UTSETT ETT DATASKYDDSOMBUD SKALL KONTAKTUPPGIFTER ANGES.]

Kontakta oss på [E-POSTADRESS] eller adress nedan om du har några frågor rörande vår personuppgiftsbehandling.

Personuppgiftsansvarig är Advokatfirman [X], [ORG NR], [ADRESS], [POSTADRESS], [TELEFON], [WEBBADRESS], [E-POSTADRESS].

Bilaga 4

Exempel – Malldokument för konsekvensbedömning

KONSEKVENSBEDÖMNING AVSEENDE [ ] [EXEMPELVIS: BEHANDLING AV PERSONUPPGIFTER VID UTFÖRANDE AV ADVOKATUPPDRAG I ADVOKATBYRÅN NN]

1. Bakgrund

[Mot bakgrund av [Advokatbyråns upphandling av AI-verktyg för juridiska bedömningar] har Advokatbyrån bedömt att en konsekvensbedömning enligt dataskyddsförordningen bör genomföras för den personuppgiftsbehandling som förekommer i anslutning till verktyget.]

2. Behovet att genomföra en konsekvensbedömning

I Advokatbyråns inledande riskanalys har följande omständigheter identifierats som talar för att en konsekvensbedömning bör genomföras:

[Identifierade risker anges, lämpligen i punktform. Ledning kan hämtas i artikel 29-gruppens vägledning.]

3. [Systematisk] beskrivning av behandlingar

En övergripande beskrivning av relevanta personuppgiftsbehandlingar följer nedan.

[Beskrivning av den personuppgiftsbehandling som förekommer, inkluderat insamling, användning, utlämnande och gallring av personuppgifter. Redogör om möjligt för hur många personer som kan komma att omfattas av behandling]

4. Synpunkter från och samråd med andra

[Vid konsekvensbedömningen har Advokatbyrån diskuterat med andra intressenter enligt vad som anges nedan.] / [Advokatbyrån har inte utsett något dataskyddsombud och har inte diskuterat med potentiellt berörda personer.]

[Redogör för de eventuella diskussioner och avstämningar som har gjorts med Advokatbyråns dataskyddsombud (i förekommande fall) och med (företrädare för) de kategorier av personer som kan komma att omfattas av Advokatbyråns behandlingar.]

5. Identifiering av risker

Advokatbyrån har identifierat följande huvudsakliga risker för de registrerades rättigheter och friheter som behöver hanteras.

[Räkna upp och beskriv de risker som Advokatbyrån identifierar]

6. Hantering av risker

Advokatbyråns bedömning är att följande åtgärder behöver vidtas för att hantera riskerna på ett relevant sätt.

[Beskrivning av relevanta åtgärder, såsom exempelvis kryptering, virusskydd, back-up-system, loggning, pseudonymisering etc.]

7. Åtgärdsplan

[Advokatbyrån har antagit följande åtgärdsplan för att hantera riskerna:] / [Det föreslås att Advokatbyrån antar följande åtgärdsplan för att hantera riskerna:]

[Beskrivning av åtgärdsplan.]

Bilaga 5

Exempel – Mall för incidentrapport

Till Datainspektionen,

Med anledning av att det den [DATUM OCH TIDPUNKT] inträffat en personuppgiftsincident hos Advokatbyrån får vi lämna följande incidentrapport.

Beskrivning av personuppgiftsincidenten

[BESKRIV PERSONUPPGIFTSINCIDENTEN, NÄR OCH VAR DEN INTRÄFFADE, VILKA KATEGORIER AV PERSONUPPGIFTER SOM ÄR BERÖRDA, DET UNGEFÄRLIGA ANTALET BERÖRDA REGISTRERADE OCH DE BEHANDLINGAR SOM PÅVERKATS. OM INCIDENTEN AVSER KLIENTINFORMATION SKA DETTA SÄRSKILT BESKRIVAS.]

Konsekvenser av personuppgiftsincidenten

[BESKRIV DE SANNOLIKA KONSEKVENSERNA FÖR DE REGISTRERADE]

Åtgärder som vidtagits med anledning av personuppgiftsincidenten

[BESKRIV DE ÅTGÄRDER SOM DEN PERSONUPPGIFTSANSVARIGE VIDTAGIT FÖR ATT BEGRÄNSA SKADAN TILL FÖLJD AV INCIDENTEN OCH ATT INCIDENTEN INTE UPPREPAS]

Kontaktperson

Advokatbyråns kontaktperson är [ANGE KONTAKTPERSON OCH KONTAKTUPPGIFTER]

Begäran om sekretess

Advokatbyrån begär att Datainspektionen sekretessmarkerar anmälan.

[DET FINNS IDAG INGA BESTÄMMELSER OM SEKRETESS FÖR INCIDENTANMÄLAN I OFFENTLIGHETS- OCH SEKRETESSLAGEN (2009:400) MEN DET HAR FÖRESLAGITS AV DATAINSPEKTIONEN]

KOMMENTAR

Av artikel 33 Dataskyddsförordningen framgår den information som incidentrapporten ska innehålla.

Artikel 29 gruppen har tagit fram Guidelines on Personal data breach notification under Regulation 2016/679.

DEL II

FÖRDJUPAD INFORMATION

2. Principer för behandling av personuppgifter

2.1 Grundläggande principer och laglig grund

Dataskyddsförordningen kommer från och med den 25 maj 2018 att vara direkt tillämplig för personuppgiftsbehandling inom EU. Förordningen ger utrymme för kompletterande nationella bestämmelser inom vissa områden. Sådana regler har föreslagits i prop 2017/18:105 Ny dataskyddslag. Samtidigt som dataskyddsförordningen ska börja tillämpas upphävs PuL. Advokatbyråerna måste således anpassa sig till den nya regleringen per den 25 maj 2018 (det finns inga övergångsregler i förordningen).

För den som ska sätta sig in i regelverket kan det vara lämpligt att börja med artikel 5 och 6. Medan det i artikel 5 anges grundläggande principer för all behandling av personuppgifter följer det av artikel 6 att varje behandling måste ha en laglig grund.[17]

I allt väsentligt gäller det som sägs i artikel 5 och 6 redan enligt PuL, med undantag för den princip om ansvarsskyldighet som införs genom artikel 5.2. Att den personuppgiftsansvarige är ansvarig för eventuella överträdelser är inte heller någon nyhet, men den personuppgiftsansvarige måste nu *kunna visa* att reglerna faktiskt efterlevs i den dagliga verksamheten. Denna princip om ansvarsskyldighet genomsyrar hela dataskyddsförordningen och innefattar krav på dokumentation av personuppgiftsbehandlingar, på öppenhet samt på införande av strategier/policyer, rutiner och organisatoriska och tekniska åtgärder för att kunna visa att dataskyddsförordningens krav uppfylls. Efterlevnaden ska byggas in som en naturlig del av den personuppgiftsansvariges verksamhet.

En annan nyhet för svensk del är att den s k missbruksregeln i 5 a § PuL som möjliggjort behandling i ostrukturerad form, inte längre gäller.[18] Att dataskyddsförordningen kommer att gälla fullt ut för behandling av personuppgifter i ostrukturerat material blir en utmaning för många.

Även de regler som i huvudsak återfanns redan i PuL kan bli en utmaning med beaktande av den framförhållning som dataskyddsförordningen kräver när efterlevnaden ska byggas in i verksamheten och den personuppgiftsansvarige ska kunna visa att dataskyddsreglerna faktiskt efterlevs. I det följande följer därför en genomgång av de lagliga grunder och principer som i första hand aktualiseras i advokatverksamhet.

---

[17] De lagliga grunder för personuppgiftsbehandling som godtas enligt artikel 6 är samtycke av den registrerade, avtalssituationer, rättslig förpliktelse som åvilar den personuppgiftsansvarige, intresseavvägning, skydd av livsviktiga intressen för den registrerade eller för en annan fysisk person, uppgift av allmänt intresse samt myndighetsutövning. De olika villkoren är i viss mån överlappande. Flera lagliga grunder kan därför vara tillämpliga avseende en och samma behandling. Därför behöver den personuppgiftsansvarige vara medveten om vilken laglig grund som man väljer. Finns det ingen laglig grund som överensstämmer med det som den personuppgiftsansvarige vill göra är behandlingen inte tillåten. Det räcker emellertid inte att finna en laglig grund för att få behandla personuppgifter. Samtliga grundläggande principer enligt artikel 5 för behandling av personuppgifter måste också följas.

[18] Missbruksregeln är ett unikt svenskt undantag från personuppgiftslagen utan motsvarighet i övriga EU, som undantar behandling av personuppgifter i ostrukturerat material (exempelvis löpande text på hemsidor, e-post och i ordbehandlingsdokument) från huvuddelen av bestämmelserna i personuppgiftslagen, förutsatt att behandlingen inte innebär en kränkning av individernas personliga integritet.

2.2 Lagliga grunder för behandling

2.2.1 Samtycke (artikel 6 a)

En laglig grund för personuppgiftsbehandling är att den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål. Dataskyddsförordningen reglerar även villkor för att ett samtycke ska anses giltigt, se artikel 7. Ett samtycke kan inte med giltig verkan lämnas i efterhand och måste således finnas där innan behandlingen påbörjas.

Denna lagliga grund för behandling är ofta inte en lämplig grund för advokatbyråers behandling av personuppgifter. Mycket av den behandling som utförs på en advokatbyrå, t ex behandling av personuppgifter om motparter, kan advokatbyråer aldrig få samtycke till att göra. En motpart skulle sannolikt aldrig lämna samtycke till sådan behandling. Till detta kommer att den registrerade ska ha rätt att när som helst återkalla sitt samtycke. Det ska dessutom vara lika lätt att återkalla som att ge sitt samtycke. En advokatbyrå kan vanligtvis inte upphöra med en behandling bara för att en registrerad återkallar sitt samtycke. Ärendet måste handläggas och t ex tidsredovisning äga rum även om klienten eller motparten återkallar sitt samtycke. Om ett samtycke återkallats faller sannolikt en intresseavvägning enligt artikel 6 f dataskyddsförordningen ut till den personuppgiftsansvariges nackdel, vilket innebär att intresseavvägningsgrunden inte längre är tillämplig.

Om en advokatbyrå behandlar personuppgifter med stöd av samtycke är utgångspunkten att man får fortsätta behandlingen med stöd av det lämnade samtycket även från och med den 25 maj 2018. Detta gäller under förutsättning att det sätt på vilket samtycket gavs överensstämmer med villkoren i dataskyddsförordningen. Eftersom kraven för inhämtande av samtycke har skärpts jämfört med PuL måste man se över tidigare samtycken, vilket sannolikt i många fall kommer att leda till att man trots allt måste inhämta förnyade samtycken.

2.2.2 Behandlingen är nödvändig för att fullgöra ett avtal (artikel 6 b)

En annan laglig grund för behandling av personuppgifter är att den är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

En för advokatverksamhet vanlig avtalssituation är att den registrerade själv är part i ett avtal där den personuppgiftsansvarige är den andra parten. Behandlingar för att fullgöra ett sådant avtal kan ske för t ex fakturering, klientregistrering och förandet av klientkonton. Ett avtal mellan en advokatbyrå och en juridisk person innebär dock inte att advokatbyrån kan behandla personuppgifter om de som är anställda hos den juridiska personen, hos klienten. De är inte parter i avtalet och en annan laglig grund för behandling av dessa personuppgifter måste finnas.

När åtgärder måste vidtas innan ett avtal träffas krävs det att den registrerade har begärt skriftligen eller muntligen att de åtgärder vidtas som gör det nödvändigt att behandla personuppgifterna. Vid en tvist har den personuppgiftsansvarige bevisbördan för att den

registrerade har begärt behandlingen. Det krävs emellertid inte att den registrerade ingår det tänkta avtalet.

2.2.3 Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse (artikel 6 c)

Personuppgifter kan också få behandlas om det är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Enligt dataskyddsförordningen måste dock den lagliga grunden i dessa fall vara fastställd antingen i unionsrätten eller i den nationella (svenska) rätten.

Behandlingsgrunden rättsliga förpliktelser finns redan i PuL men för att tydliggöra vad som menas föreskrivs i 2 kap 1 § förslaget till dataskyddslag (se prop 2017/18:105 s 52 f) att personuppgifter får behandlas med stöd av artikel 6.1 c i dataskyddsförordningen, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning.

Denna lagliga grund kan advokatbyråer tillämpa för skyldigheter som följer av offentligrättsliga bestämmelser, t ex att redovisa källskatt eller sociala avgifter för anställda eller att inom ramen för rehabilitering av anställda göra arbetsförmågebedömningar.

2.2.4 Behandlingen är tillåten efter en intresseavvägning (artikel 6 f)

Behandling får också ske av personuppgifter om det är nödvändigt för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen – om inte den registrerades intressen eller grundläggande rättigheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn. Denna lagliga grund kallas för intresseavvägning.

Ett sådant berättigat intresse kan t ex finnas när det föreligger ett relevant och lämpligt förhållande mellan den registrerade och den personuppgiftsansvarige i situationer där den registrerade är kund hos eller arbetar för den personuppgiftsansvarige. Ett berättigat intresse kräver under alla omständigheter en noggrann bedömning, som inbegriper huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med detta rimligen kan förvänta sig att en uppgiftsbehandling för detta ändamål kan komma att ske.

Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse. Denna grund kan även användas för många delar av en advokatbyrås administrativa verksamhet, interna verksamhet, inom inköp, HR m m.

Den registrerades intressen och grundläggande rättigheter skulle i synnerhet kunna väga tyngre, enligt dataskyddsförordningen, än den personuppgiftsansvariges intressen, om personuppgifter behandlas under omständigheter där den registrerade inte rimligen kan förvänta sig någon ytterligare behandling.

2.2.5 Behandlingen är nödvändig för att skydda grundläggande intressen (artikel 6 d)

Behandling av personuppgifter får vidare ske när den är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person. Det handlar här i princip om att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Behandling av personuppgifter på grundval av en annan fysisk persons grundläggande intressen bör i princip endast äga rum om behandlingen inte uppenbart kan ha en annan laglig grund.

Enligt dataskyddsförordningen kan vissa typer av behandling tjäna både viktiga allmänna intressen, se punkten 2.2.6 nedan, och intressen som är av grundläggande betydelse för den registrerade, t ex när behandlingen är nödvändig av humanitära skäl, bl a för att övervaka epidemier och deras spridning eller i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan.[19]

2.2.6 Behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse (artikel 6 e)

Av dataskyddsförordningen följer också att en behandling av personuppgifter kan vara tillåten om den är nödvändig för att utföra en uppgift av allmänt intresse.[20] Den lagliga grunden måste emellertid i detta fall vara fastställd antingen i unionsrätten eller i den nationella (svenska) rätten, jfr avsnitt 2.2.3.[21]

Även privaträttsligt bedriven verksamhet av allmänt intresse omfattas av formuleringen och dataskyddsförordning ställer inte något krav på att de särskilda ändamålen ska vara fastställda i författning. Det räcker att grunden för behandlingen har fastställts och den måste inte vara fastställd i lag. Däremot måste grunden vara fastställd i laga ordning, på ett konstitutionellt korrekt sätt. Ett privaträttsligt organ som fullgör ett uppdrag från en myndighet avseende en sådan uppgift som är fastställd i författning, regeringsbeslut etc kan vidta nödvändiga behandlingsåtgärder på samma rättsliga grund som om myndigheten själv utfört uppgiften, d v s med stöd av artikel 6.1 e i dataskyddsförordningen.[22] I de fall där advokatbyrån själv blir personuppgiftsansvarig kan viss verksamhet vara av sådant allmänt

---

[19] Se skäl 46 till dataskyddsförordningen.

[20] Begreppet allmänt intresse är ett unionsrättsligt begrepp som inte definieras utförligt i dataskyddsförordningen och dess innebörd har ännu inte heller utvecklats av EU-domstolen (begreppet finns även i dag). Enligt dataskyddsförordningen anges att allmänintresset inbegriper hälso- och sjukvårdsändamål, såsom folkhälsa och socialt skydd och förvaltning av hälso- och sjukvårdstjänster, av civilrättslig lagstiftning, exempelvis en yrkesorganisation.

[21] I 2 kap 2 § 1 förslaget till dataskyddslag (prop 2017/18:105 s 55) anges förutsättningarna för att en uppgift av allmänt intresse ska utgöra laglig grund för behandling. Där föreskrivs att personuppgifter får behandlas med stöd av artikel 6.1 c i dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Det är alltså inte tillräckligt att uppgiften är av allmänt intresse – uppgiften måste också vara fastställd i enlighet med gällande rätt.

[22] Prop 2017/18:105 s 62.

intresse som här avses. Hur advokater ska bedriva sin verksamhet följer delvis av regler i rättegångsbalken och Advokatsamfundet som organisation har en offentligrättslig karaktär. Exempelvis är advokatens uppdrag som offentlig försvarare delvis reglerat i 21 kap rättegångsbalken.

Det är av grundläggande betydelse i en rättsstat att allmänheten har tillgång till kvalificerad och obunden juridisk rådgivning vid misstanke om brott. Principiellt behöver advokaten tillgång till samma information, inklusive personuppgifter, och på samma sätt (exempelvis elektroniskt) som åklagaren för att kunna utöva försvaret på ett fullödigt sätt och till säkerställande av en rättvis rättegång. Alla vittnen som förekommer i en förundersökning kanske inte visar sig nödvändiga för klientens försvar men inte desto mindre måste behandlingen av personuppgifter, enligt Advokatsamfundets bedömning, anses nödvändig för att utföra en uppgift av allmänt intresse.

2.2.7 Behandlingen är nödvändig som ett led i myndighetsutövning (artikel 6 e)

Slutligen följer det av dataskyddsförordningen att en behandling av personuppgifter kan vara tillåten om den är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning. Även i dessa fall måste den lagliga grunden vara fastställd antingen i unionsrätten eller i den nationella (svenska) rätten, jfr avsnitt 2.2.3 och 2.2.6, och förutsättningarna anges i 2 kap 2 § 2 förslaget till dataskyddslag (se prop 2017/18:105 s 62 f). Där föreskrivs att personuppgifter får behandlas med stöd av artikel 6.1 e i dataskyddsförordningen, om behandlingen är nödvändig som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning. Det är alltså inte tillräckligt att uppgiften är av allmänt intresse – uppgiften måste också vara fastställd i enlighet med gällande rätt.

Advokater kan utföra uppgifter som innefattar myndighetsutövning exempelvis i egenskap av notarius publicus (se lagen [1981:1363] om notarius publicus). Vidare har advokatsamfundet getts vissa statliga förvaltningsuppgifter som även innefattar myndighetsutövning. Även denna lagliga grund för behandling kan således aktualiseras.

3. Särskilda kategorier av personuppgifter (känsliga personuppgifter) och uppgifter om lagöverträdelser

Behandling av s k *särskilda kategorier av personuppgifter*, tidigare benämnda känsliga personuppgifter, har genom dataskyddsförordningen uppdaterats och fått en något vidare definition. När advokatbyrå behandlar särskilda kategorier av personuppgifter krävs ett giltigt undantag från huvudregeln som annars föreskriver att behandling av de särskilda kategorierna av uppgifter är förbjuden.

Särskilda kategorier av personuppgifter är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska eller biometriska uppgifter, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Giltiga undantag från förbudet och som närmast kan vara relevanta i advokatverksamhet kan kortfattat beskrivas enligt följande:[23]

I. Registrerads uttryckliga samtycke till behandlingen av dessa uppgifter för ett eller flera specifika ändamål – såvida inte unionsrättens eller medlemsstaternas nationella rätt (svensk lagstiftning) föreskriver att förbudet inte kan upphävas av den registrerade.
II. Behandlingen är nödvändig för att den ansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten, social trygghet och socialt skydd, förutsatt att det är tillåtet enligt unionsrätten eller nationell rätt, eller ett kollektivavtal – där lämpliga skyddsåtgärder som säkerställer den registrerades rättigheter och intressen fastställs.
III. Behandlingen är nödvändig för att skydda den registrerade eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
IV. Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
V. Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.
VI. Behandlingen är nödvändig för skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling social omsorg m m.

Vissa ytterligare förtydliganden såvitt avser främst arbetsrättens område respektive hälso- och sjukvårdsuppgifter återfinns i prop 2017/18:105 s 76 ff.

Såvitt avser *behandling av uppgifter om lagöverträdelser* (fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1) föreskrivs i dataskyddsförordningen att sådan behandling endast får ske under kontroll av myndighet eller då behandlingen är tillåten enligt unionsrätten eller nationell rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.[24] Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet.

I Sverige förekommer särskilt en diskussion rörande behandling av *misstanke om brott*, där särskilt det s k tankstoppmålet[25] bör uppmärksammas. Dataskyddsutredningen har ansett att även behandling av uppgifter som avser misstanke om brott omfattas av begränsningen i

[23] För fler detaljer samt undantag se artikel 9 i dataskyddsförordningen.

[24] Artikel 10 dataskyddsförordningen.

[25] HFD 2016 ref 8 där Högsta förvaltningsdomstolen uttalat att registrering av uppgifter om fordon som förekommit i samband med obetalda tankningar ska anses innefatta en behandling av personuppgifter om lagöverträdelser som innefattar brott i den mening som avses i personuppgiftslagen. Utredningen har mot denna bakgrund, i avsaknad av klargörande EU-rättslig praxis, bedömt att misstankar om brott bör omfattas av artikel 10 i dataskyddsförordningen i samma utsträckning som de gör enligt personuppgiftslagen. Flera remissinstanser invänder mot denna bedömning och anser att den saknar stöd i dataskyddsförordningen.

10 kapitlet i förordningen. Av propositionen till dataskyddslagen framgår dock att ett antal remissinstanser ifrågasätter tolkningen.[26] Regeringen har i propositionen uttalat att ”Det är därför, som bl a Svensk Handel är inne på, inte säkert att praxis enligt personuppgiftslagen kring vilka uppgifter som omfattas av regleringen om personuppgifter som rör lagöverträdelser fortfarande är aktuell.” [27]

Regeringen har för avsikt att, som utredningen föreslår, vidaredelegera normgivningskompetens till tillsynsmyndigheten och anser att det även i fortsättningen bör finnas utrymme för särreglering som tillåter behandling av personuppgifter som rör lagöverträdelser (3 kap 9 § i förslaget till dataskyddslag). I tillägg till det så föreslås myndighet som regeringen bestämmer få även i enskilda fall besluta att andra än myndigheter får behandla sådana uppgifter. Ett sådant beslut får förenas med villkor. I propositionen anges också särskilt att det ”är regeringens uppfattning att svenska företag inte ska ges sämre möjligheter att behandla uppgifter som rör lagöverträdelser än företag i andra länder”, vilket förhoppningsvis innebär att den svenska särställningen när det gäller misstanke om brott kommer att kunna minska i betydelse.

Idag gäller två betydelsefulla undantag från 21 § PuL som innebär ett förbud för andra än myndigheter att behandla uppgift om lagöverträdelser;

(i) att advokatbyråer får behandla personuppgifter om behandlingen är nödvändig för kontroll av att jävssituation inte föreligger och

(ii) att enstaka uppgift får behandlas som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall.[28]

Advokatsamfundet utgår från att Datainspektionens föreskrifter och därmed undantagen ovan också kommer att uppdateras och förtydligas och att Datainspektionen därvid ger ut nya föreskrifter som i vart fall innehåller motsvarande undantag i anslutning till att dataskyddsförordningen och dataskyddslagen träder ikraft.

Vidare föreligger ytterligare ett undantag med stöd av 5 kap 6 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism, innebärande (iii) att en advokatbyrå har rätt att behandla personuppgifter om lagöverträdelser för att fullgöra sina rättsliga förpliktelser enligt nämnda lag, vilka bl a är att undersöka de risker som kan förknippas med klienten.

---

[26] Se prop 2017/18:105 s 97 ff. Se även SOU 1997:39 s 380 rörande faktiska iakttagelser om överträdelser.

[27] Prop 2017/18:105 s 99.

[28] Datainspektionens föreskrifter DIFS 2010:1, 1 § b) och d).

4. Den registrerades rättigheter

4.1 Skyldighet att lämna information till den registrerade (artikel 13–15)

Informationsskyldigheten kan delas upp i tre delar:

(i) Information som självmant ska tillhandahållas om informationen samlas in från den registrerade (artikel 13)
(ii) Information som självmant ska lämnas om information har erhållits från annan part än den registrerade (artikel 14)
(iii) Information som ska lämnas på den registrerades begäran (artikel 15.3 till artikel 15.7)

Det finns undantag från informationsskyldigheten i artikel 13 respektive artikel 14.

(i) Information behöver inte lämnas till den registrerade vid insamlingen av personuppgifter om den registrerade redan förfogar över informationen (se artikel 13.4 respektive artikel 14.5 a)
(ii) Har informationen erhållits från annan part än den registrerade behöver information inte lämnas om tillhandahållandet av information skulle visa sig vara omöjligt eller skulle medföra en oproportionell ansträngning (artikel 14.5 b) eller om personuppgifterna omfattas av en tystnadsplikt (artikel 14.5 d).

4.2 Advokats skyldighet att lämna information till klienten m m (artikel 13)

Dataskyddsförordningen innehåller detaljerade regler om vilken information den personuppgiftsansvarige måste lämna till den registrerade om informationen samlats in från den registrerade själv (jfr 23, 25 och 26 §§ PuL).

Om uppgifterna samlas in direkt från den registrerade (d v s en klient som är en privatperson) är advokatbyrån enligt artikel 13 i dataskyddsförordningen skyldig att lämna nedanstående information till klienten om klientens personuppgifter behandlas (vilket sker i en absolut majoritet av alla advokatverksamheter). Informationsskyldigheten är betydligt mer detaljerad än enligt 25 § PuL och det är många uppgifter som ska lämnas. Här följer en beskrivning av vad en informationstext i huvudsak behöver innehålla i advokatverksamhet:

Artikel 13.1 (grundläggande information)

a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den lagliga grunden för behandlingen.
d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.

e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

Artikel 13.2 (ytterligare information)

a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
d) Rätten att inge klagomål till en tillsynsmyndighet.
e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas. [29]

Det undantag från informationsskyldighet som gäller om den registrerade redan förfogar över all information som ska lämnas (artikel 13.4) blir sällan tillämpligt i advokatverksamhet eftersom den registrerade sällan förfogar över all den information som ska lämnas.

Datainspektionen har publicerat Allmänna råd Information till registrerade enligt PuL vilka kan tjäna till viss ledning när det gäller informationsskyldigheten.[30] De avser emellertid informationsskyldigheten enligt PuL. Informationsskyldigheten enligt dataskydds-förordningen är mera omfattande. Artikel 29-gruppen har publicerat en vägledning för information till registrerade.[31]

Informationen enligt artikel 13 ska, som följer av artikel 12.1, lämnas skriftligen och vara koncis, klar och tydlig, begriplig och i lätt tillgänglig form, med användning av klart och

[29] Information enligt artikel 13.2 (f) aktualiseras sannolikt sällan. Där anges att uppgiften ska lämnas om förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

[30] De allmänna råden finns tillgängliga på adressen https://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-inforad.pdf.

[31] Guidelines on transparency under Regulation 2016/679, tillgänglig på adressen http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 (under remissbehandling).

tydligt språk. Informationen lämnas lämpligast i ett uppdragsbrev eller i ett formulär för antagande av uppdrag. Informationen kan sannolikt lämnas i en personuppgiftspolicy på advokatbyråns webbsida om advokaten länkar till denna webbsida i sin uppdragsbekräftelse. Informationen bör inte lämnas som en del av advokatbyråns allmänna villkor eftersom det förmodligen innebär att tydlighetskravet inte är uppfyllt. Se det exempel som finns i bilaga 3 i Del I.

4.3 Information som ska lämnas efter den registrerades ansökan (artikel 15)

Av artikel 15 i dataskyddsförordningen följer att den registrerade har rätt att av den personuppgiftsansvarige, på begäran från den registrerade, få bekräftelse huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna[32] och följande information:

a. Ändamålen med behandlingen.
b. De kategorier av personuppgifter som behandlingen gäller.
c. De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.
d. Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
e. Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.
f. Rätten att inge klagomål till en tillsynsmyndighet.
g. Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.
h. Förekomsten av automatiserat beslutsfattande, inbegripet profilering

Om personuppgifterna överförs till ett tredje land eller till en internationell organisation, ska den registrerade dessutom ha rätt att få information om skyddsåtgärder som vidtagits vid överföringen i enlighet med artikel 46 (exempelvis bindande företagsbestämmelser, standardiserade avtalsklausuler mellan den personuppgiftsansvarige och mottagande enhet eller godkänd uppförandekod). Den personuppgiftsansvarige ska dessutom förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat (se artikel 15.2 och 3).

[32] Begränsningen som tidigare fanns rörande registerutdrag endast en gång per år är nu borta. Möjligen kan istället argumenteras för att ett upprepat antal sådana begäranden kan sägas vara orimligt, se nedan.

4.4 Informationsskyldighet när uppgifter har erhållits från annan (artikel 14)

Ett generellt undantag från informationsskyldigheten, som blir av betydelse i advokatverksamhet, gäller som framgått enligt artikel 14.5 (d) för konfidentiell information. Detta undantag är *endast tillämpligt när uppgifterna samlats in från annan part än den registrerade*, exempelvis när advokatbyrån bedömer om det finns förutsättningar för att väcka talan mot en motpart, utvärderar potentiella vittnesmål i en tvist eller ett brottmål, hanterar ett mål om vårdnad och umgänge, upprättar ett testamente eller hanterar dokument i ett datarum inför försäljning eller köp av företag och därvid behandlar personuppgifter avseende motparter, vittnen, familjemedlemmar, testatorer eller personer som förekommer i datarummet. Om advokatbyrån i en sådan situation skulle vara skyldig att informera den registrerade om behandlingen skulle det medföra att en motpart eller potentiella vittnen skulle informeras om att advokatens klient överväger en talan. En sådan informationsskyldighet kommer i konflikt med advokatens tystnadsplikt enligt 8 kap 4 § rättegångsbalken och lojalitetsplikt i förhållande till sin klient. Av ett undantag i artikel 14.5 (d) följer dock att informationsskyldigheten i artikel 14 inte gäller när personuppgifterna måste förbli konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt, inbegripet andra lagstadgade sekretessförpliktelser. Advokatens tystnadsplikt enligt rättegångsbalken är en sådan tystnadsplikt som följer av artikel 14.5 (d) vilket innebär att artikel 14 inte är tillämplig på advokatverksamhet.

Enligt artikel 23.1 dataskyddsförordningen finns det en möjlighet för medlemsstaterna att begränsa tillämpningsområdet för artiklarna 12–22. I propositionen föreslås en bestämmelse i 5 kap 1 § dataskyddslagen enligt vilken den registrerades rätt till information och tillgång till personuppgifter enligt artiklarna 13–15 i dataskyddsförordningen inte gäller sådana uppgifter som den personuppgiftsansvarige inte får lämna ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning. För en personuppgiftsansvarig som inte är en myndighet gäller undantaget i första stycket även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda enligt offentlighets- och sekretesslagen (2009:400). I lagmotiven[33] uttalas bl a följande:

> ”Vidare finns det situationer då även en privaträttslig aktör, som inte omfattas av författningsreglerad sekretess eller tystnadsplikt, har berättigad anledning att hemlighålla uppgifter i förhållande till den registrerade. Det kan t ex röra sig om information som samlats in inför en domstolsprocess, om det kan antas att ett utlämnande av informationen skulle försämra den personuppgiftsansvariges ställning som part i rättegången. Regeringen anser därför i likhet med utredningen att det finns ett behov av ett undantag motsvarande det som i dag finns i 27 § PUL (prop 2017/18:105 s. 107).”

Det föreslagna undantaget träffar i normalfallet information som samlats in från annan än den registrerade och sannolikt inte klientens egna personuppgifter (eftersom dessa inte omfattas av sekretess i förhållande till klienten). Detta innebär att informationsskyldigheten enligt artikel 13–15 normalt får antas gälla i förhållande till klienten men däremot inte i förhållande till tredje part. Den föreslagna regleringen i 5 kap 1 § dataskyddslagen motsvarar

[33] SOU 2017:39, s 205f. och prop 2017/18:105 s 107.

27 § PuL som varit i kraft sedan 1998. Praxis rörande 27 § PuL blir vägledande vid tillämpningen av den nya bestämmelsen (prop 2017/18:105 s 107).

För övriga rättigheter som den registrerade har enligt artikel 16 (rätt till rättelse), artikel 17 (rätt till radering), artikel 18 (rätt till begränsning av behandling), artikel 19 (anmälningsskydd avseende rättelse m m), artikel 20 (rätt till dataportabilitet) m fl föreslås inget sekretessundantag i dataskyddslagen. Antingen har frågan inte uppmärksammats eller också har det antagits att någon sådan fråga inte kan uppkomma när den registrerade inte har rätt att få information om sådana behandlingar. De sekretesskäl som anförts som grund för att Sverige undantar information som omfattas av sekretess, exempelvis information som samlats in inför en rättsprocess, gör sig lika starkt gällande även beträffande skyldigheterna i artikel 16–20 eftersom ett fullgörande av en sådan skyldighet i princip kan innebära att en personuppgiftsansvarig advokatbyrå skulle vara skyldig att bekräfta huruvida byrån behandlar personuppgifterna, vilket står i strid med tystnadsplikten enligt 8 kap 4 § rättegångsbalken. I denna del finns en möjlighet för regeringen att föreskriva undantag, men det är oklart om detta kommer att ske.

I avsaknad av sådant undantag kan alltså skyldigheten att tillmötesgå en begäran om utövande av en rättighet komma i konflikt med advokatens tystnadsplikt. Tystnadsplikten i 8 kap 4 § rättegångsbalken är av fundamental betydelse för all advokatverksamhet. Enligt Advokatsamfundets mening bör advokatens tystnadsplikt gå före en begäran om utövande av en rättighet. Tystnadsplikten bör betraktas som ett utflöde av artikel 6 i den Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) och en klients befogade förväntan på att advokaten iakttar fullständig tystnadsplikt.

4.5 Svar på begäran om tillgång till personuppgifter, begäran om rättelse, begäran att bli bortglömd, begäran om begränsning av behandling respektive rätt till dataportabilitet (artikel 15–22)

Om den personuppgiftsansvarige tar emot en begäran om någon av åtgärderna enligt artiklarna 15–22 ska denna begäran enligt artikel 12.3 besvaras utan onödigt dröjsmål och under alla omständigheter senast en månad efter att begäran mottogs. Om begäran är komplicerad eller det har kommit in ett stort antal ärenden får vid behov svarstiden förlängas till två månader. I sådana fall ska den personuppgiftsansvarige underrätta den registrerade om förlängningen inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.
Den personuppgiftsansvarige får, om denne har rimliga skäl att betvivla identiteten hos den fysiska person som lämnar in en begäran, begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet tillhandahålls.

Den information som ska lämnas ska tillhandahållas kostnadsfritt. Om en begäran från en registrerad är uppenbart ogrundad eller orimlig får den personuppgiftsansvarige antingen
a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller
b) vägra att tillmötesgå begäran.

Det är den personuppgiftsansvarige som har bevisbördan för att begäran är uppenbart ogrundad eller orimlig.

Som framgår ovan har advokatbyrån inte skyldighet att tillmötesgå en begäran enligt artikel 15 i den mån advokatens tystnadsplikt står i vägen (5 kap 1§ dataskyddslagen). Vidare ska beaktas andra individers rätt till integritet och viss information kan därvid behöva maskeras innan kopior lämnas ut.[34]

Ett undantag från skyldigheten i artikel 15 följer även av 5 kap 2 § dataskyddslagen.[35] Skyldigheten gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning eller som utgör minnesanteckning eller liknande. Detta gäller dock inte om uppgifterna har lämnats ut till tredje man, har lämnats in till arkivmyndighet, eller – såvitt avser uppgifter i löpande text som inte har fått sin slutliga utformning – om uppgifterna har behandlats under längre tid än ett år. I advokatverksamhet blir denna bestämmelse av intresse i de fall advokatsekretessen inte förhindrar ett utlämnande av information med stöd av artikel 15 i dataskyddsförordningen.

4.6 Begäran om rättelse (artikel 16)

Av artikel 16 dataskyddsförordningen följer att den registrerade har rätt att begära att felaktiga personuppgifter rättas. Denna princip gäller redan enligt 28 § PuL.

Eftersom den s k missbruksregeln i 5 a § PuL har tagits bort kan man fråga sig om artikel 16 innebär en skyldighet att rätta uppgifter i korrespondens, inlagor, yttranden, promemorior och andra dokument. Advokatsamfundets bedömning är att uppgifter i tidigare upprättade dokument av detta slag inte behöver ändras. Som framgår av artikel 5.1 d ska nämligen skyldigheten att rätta uppgifter bedömas i förhållande till behandlingens ändamål. Den information som lämnas, åsikt som uttrycks, inställning som tas i ett brev eller en inlaga måste betraktas med utgångspunkt för den tidpunkt då dokumentet upprättades. Behandlingens ändamål innefattar inte i sig att hålla personuppgifterna uppdaterade och objektivt korrekta, och det kan därför inte anses vara nödvändigt att genomföra justeringar i den här typen av dokument.

Motsvarande bedömning bör gälla även för dokument som enligt den registrerades uppfattning innehåller ofullständiga personuppgifter. I denna situation kan man även enligt bestämmelsen tillföra någon form av dokument till ärendet med ett ”kompletterande

[34] 15.4 dataskyddsförordningen.

[35] Detta undantag gäller för övrigt redan idag enligt 26 § 2 st PuL.

utlåtande” från den registrerade med de kompletteringar som den registrerade anser behövs. Beroende på omständigheterna kan den kompletterande informationen behöva beaktas i den framtida hanteringen av ärendet.

4.7 Rätten att bli bortglömd (artikel 17)

Av artikel 17 dataskyddsförordningen följer att den registrerade har rätt att utan onödigt dröjsmål få sina personuppgifter raderade om

a) personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats,
b) den registrerade återkallar det samtycke på vilket behandlingen grundar sig och det inte finns någon annan laglig grund för behandlingen,
c) den registrerade invänder mot behandlingen och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot profilerande behandling,
d) personuppgifterna har behandlats på olagligt sätt,
e) personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av, eller
f) personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster (begreppet innefattar de flesta typer av onlinetjänster).

I advokatverksamhet kommer rätten att bli bortglömd, i vart fall när det gäller digitala uppgifter som behandlas, i konflikt med arkiveringsskyldigheten i 7.12 VRGA. Av artikel 17.3 b dataskyddsförordningen följer dock att rätten att bli bortglömd inte gäller om behandlingen är nödvändig för att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse. Enligt 8 kap 4 § rättegångsbalken ska en advokat i sin verksamhet redbart och nitiskt utföra de uppdrag som anförtrotts honom och iaktta god advokatsed. Enligt 7.12.2 VRGA är en advokat skyldig att i original eller kopia arkivera de handlingar som ansamlats under utförande av ett uppdrag. Arkivhållningen ska ske under tio år eller den längre tid som uppdragets natur påkallar. Advokatsamfundet anser att bestämmelsen i 7.12.2 VRGA ska ges företräde även om en klient begär att bli bortglömd. En orsak till detta är att advokaten alltid måste ha tillgång till akten för att kunna bemöta ett eventuellt anspråk som riktas mot advokaten i anledning av det utförda uppdraget. En annan orsak är att advokaten har en skyldighet att lämna ut handlingar som tillhör klienten sedan ett uppdrag har upphört.

Om det är en motpart som framställer en begäran om att bli bortglömd gäller undantaget i artikel 17.3 e – radering behöver inte göras om behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk.

4.8 Rätt till begränsning av behandling (artikel 18)

Av artikel 18 följer att den registrerade ska ha rätt att kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:

a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.
b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

Rätten till begränsning av en behandling förefaller närmast vara en interimistisk möjlighet för den registrerade att få behandlingen begränsad i avvaktan på att behandlingen kontrolleras eller prövas. Denna rättighet förefaller inte ha några direkta implikationer för advokatverksamhet.

Det bör uppmärksammas att en begränsning av behandlingen inte förhindrar att sådana uppgifter behandlas som är nödvändiga för att fastställa, göra gällande eller försvara rättsliga anspråk (artikel 18.2).

4.9 Anmälningsskyldighet om personuppgifter rättas, eller raderas eller en behandling begränsas (artikel 19)

Om den personuppgiftsansvarige rättar en felaktig personuppgift, raderar densamma eller begränsar behandlingen av personuppgifter ska den personuppgiftsansvarige enligt artikel 19 informera varje mottagare till vilken personuppgifter har lämnats ut om åtgärden, om det inte är omöjligt eller medför en oproportionerlig ansträngning. På begäran ska den registrerade informeras om mottagarna.

Som tidigare nämnts är det Advokatsamfundets bedömning att bestämmelsen i 8 kap 4 § rättegångsbalken går före vid en konflikt med artikel 19.

4.10 Dataportabilitet (artikel 20)

En behandling av klientens personuppgifter grundas ofta på avtal (artikel 6.1 b) eller ibland på samtycke (artikel 6.1 a) vilket enligt artikel 20 dataskyddsförordningen medför en rätt till dataportabilitet. Detta innebär att den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som

tillhandahållits personuppgifterna hindrar detta. Den registrerade kan också begära att uppgifterna överförs från en personuppgiftsansvarig till en annan. Principen om rätt till dataportabilitet har stora likheter med den rätt en klient har att få del handlingar enligt 7.12.2 VRGA med den skillnaden att det inte är tillräckligt att lämnat ut handlingarna i fysiskt format utan handlingarna måste lämnas ut i ett allmänt använt och maskinläsbart format (exempelvis Word, Excel, läsbar pdf). Klienten kan begära att handlingarna lämnas över direkt till ett annat ombud.

Likheterna mellan rätten till dataportabilitet och klientens rätt att få ut handlingar enligt 7.12.2. VRGA ska dock inte överdrivas. Rätten enligt 7.12.2 omfattar allt material i ärendet, medan rätten till dataportabilitet är mycket mer begränsad. Rätten till dataportabilitet omfattar som nämnts bara personuppgifter, och bara personuppgifter om klienten själv (när klienten är en fysisk person) som denne själv har tillfört ärendet. Klienten har exempelvis inte rätt att få ut personuppgifter om motparten eller andra personer och inte heller information som kan vara skyddad av immaterialrätt eller som företagshemlighet etc (se artikel 20.4).

Det lär aldrig bli aktuellt för en advokatbyrå att tillmötesgå en begäran om dataportabilitet från en motpart. Behandlingen av dennes personuppgifter grundas inte på avtal med eller samtycke från motparten.

5. Konsekvensbedömning avseende dataskydd (artikel 35)

Av artikel 35 dataskyddsförordningen följer att den personuppgiftsansvarige ska göra en s k konsekvensbedömning avseende dataskydd före utförandet av behandlingar som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, särskilt vid användning av ny teknik. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

En bedömning är enligt artikel 35.3 alltid nödvändig om det sker

a. en systematisk och omfattande bedömning av fysiska personers personliga aspekter som grundar sig på automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer;
b. behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1 (d v s känsliga personuppgifter) eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10 (d v s uppgifter om lagöverträdelser); eller
c. systematisk övervakning av en allmän plats i stor omfattning.

Artikel 29-gruppen har utfärdat riktlinjer för när behandling sannolikt leder till en hög risk och konsekvensbedömning alltså kan behövas.[36] Av riktlinjerna framgår att en behandling med hög risk kan föreligga om behandlingen

1. innebär utvärdering eller poängsättning av individer
2. innebär automatiserat beslutsfattande
3. innebär systematisk övervakning av allmän plats
4. innefattar känsliga personuppgifter eller uppgifter om lagöverträdelser
5. omfattar ett stort antal personuppgifter
6. innebär matchning av data från flera behandlingar
7. avser registrerade som är sårbara
8. innebär en innovativ användning av tekniker, exempelvis en kombination av fingeravtryck och ansiktsigenkänning
9. medför att den registrerade får svårt att utöva sina rättigheter.

Artikel 29-gruppen anger som en tumregel att om två av kriterierna föreligger kan det finnas skäl att utföra en konsekvensbedömning. Ju fler kriterier som föreligger desto större är sannolikheten att det föreligger hög risk som föranleder en konsekvensbedömning. Skulle den personuppgiftsansvarige bedöma att det inte föreligger hög risk när två eller fler av kriterierna föreligger, bör skälen till bedömningen dokumenteras. Det förhållandet att bara ett av kriterierna föreligger utesluter inte att en konsekvensbedömning kan vara motiverad.

Advokatsamfundets bedömning är att de behandlingar som kan tänkas medföra hög risk och potentiellt medföra en skyldighet att upprätta en konsekvensbedömning avseende dataskydd som förekommer i typisk advokatverksamhet är behandlingar av känsliga uppgifter och uppgifter om lagöverträdelser (exempelvis i LVU eller LVM-mål och brottmål). Även behandlingar som innefattar poängsättning av individer exempelvis personlighets- eller begåvningstester eller s k 360-analyser kan innefatta behandling med hög risk. Även övervakning av anställdas IT-användning kan utgöra en högriskbehandling. Även införandet av eventuella AI-lösningar kan motivera en konsekvensbedömning.

Enligt Advokatsamfundets bedömning ska dock inte en konsekvensbedömning genomföras inför varje nytt ärende där känsliga uppgifter, uppgifter om lagöverträdelser etc förekommer. Att uppgifter om lagöverträdelser behandlas i ett enskilt brottmål innebär i sig inte någon skyldighet att genomföra en konsekvensbedömning. Det är det förhållandet att en brottmålsbyrå hanterar ett stort antal brottmål som skulle kunna föranleda en konsekvensbedömning för den typen av behandlingar.

---

[36]Riktlinjerna finns tillgängliga på adressen https://www.datainspektionen.se/Documents/Riktlinjer%20om%20konsekvensbed%c3%b6mning%20avseende%20dataskydd.pdf.

I skäl (91) till dataskyddsförordningen uttalas att konsekvensbedömningar inte ska vara obligatoriskt vad gäller behandling av klienters personuppgifter som utförs av ”enskilda …. juridiska ombud”. I vart fall ensampraktiserande advokater och advokatbyråer behöver därmed inte genomföra konsekvensbedömningar. Sådan behandling anses inte som storskalig i den mening som avses i artikel 35.

Enligt Advokatsamfundets bedömning bör inte det sätt på vilket advokatverksamhet organiseras tillmätas betydelse vid tillämpningen av de bestämmelser som reglerar advokatverksamhet. Enligt Advokatsamfundets uppfattning tar skäl (91) sikte på den behandling som utförs av enskilda advokater i klientärenden, även om den advokat som behandlar uppgifterna är verksam i en advokatbyrå. Inte minst det förhållandet att advokaten personligen omfattas av lagstadgad tystnadsplikt rörande klientens förhållanden talar för denna bedömning. Omfattningen av den behandling av känsliga personuppgifter och brottsuppgifter som utförs av enskilda advokater är normalt sett inte tillräckligt stor för att motivera en konsekvensbedömning, detta mot bakgrund av den sammantagna riskavvägning som följer av artikel 35.

Av artikel 35.4 framgår att Datainspektionen ska publicera en lista på behandlingar som kräver konsekvensbedömning. Av artikel 35.5 framgår att Datainspektionen även har möjlighet att publicera en lista på behandlingar som inte kräver en konsekvensbedömning. I dagsläget har inte några sådana listor publicerats.

Om den personuppgiftsansvarige kommer fram till att en behandling utgör en högriskbehandling ska en konsekvensbedömning upprättas innan behandlingen påbörjas (se artikel 35.1).

Konsekvensbedömningen ska enligt artikel 35.7 innefatta

a. en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse,
b. en bedömning av behovet av och proportionaliteten hos behandlingen i förhållande till syftena,
c. en bedömning av de risker för de registrerades rättigheter och friheter och
d. de åtgärder som planeras för att hantera riskerna, inbegripet skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna och för att visa att denna förordning efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.

Den personuppgiftsansvarige ska, när det är lämpligt, inhämta synpunkter från de registrerade eller deras företrädare om den avsedda behandlingen, utan att det påverkar skyddet av kommersiella eller allmänna intressen eller behandlingens säkerhet.
Den personuppgiftsansvarige ska också vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

En konsekvensbedömning ska som nämnts genomföras innan en behandling eller en serie av liknande behandlingar påbörjas. Enligt Advokatsamfundets bedömning krävs inte någon konsekvensbedömning för behandlingar eller serier av behandlingar – exempelvis hantering av ärenden inom advokatverksamhet – som har påbörjats före den 25 maj 2018. Artikel-29 gruppen uttalar i och för sig att detta gäller om behandlingen har kontrollerats och godkänts före den 25 maj 2018.[37] Uttalandet rör dock sådana behandlingar som är föremål för krav på förhandskontroll enligt artikel 20.1 dataskyddsdirektivet, infört i Sverige genom 41 § PuL. Advokatsamfundet menar att artikel 29-gruppens uttalande inte kan medföra krav på konsekvensbedömning för pågående behandlingar – eller serier av behandlingar – som inte är föremål för förhandskontroll enligt 41 § PuL. Skulle det däremot efter den 25 maj 2018 ske någon förändring gällande behandlingarna, exempelvis införande av nytt ärendehanteringssystem med avancerad teknik hos byrån, så kan det tänkas medföra krav på konsekvensbedömning.

6. Dataskyddsombud (artikel 37)

Av artikel 37 dataskyddsförordningen framgår under vilka förutsättningar en personuppgiftsansvarig är skyldig att utse ett dataskyddsombud. Dataskyddsombudets ställning respektive uppgifter regleras i artikel 39. I Sverige har personuppgiftsombud kunnat utses enligt 36 § PuL som har de uppgifter som följer av 38 § PuL. Ett personuppgiftsombud som utsetts enligt PuL och ett dataskyddsombud som utses enligt dataskyddsförordningen har betydande likheter.

En personuppgiftsansvarig som bedriver privat verksamhet måste enligt artikel 37 b i dataskyddsförordningen utse ett dataskyddsombud om den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller om den personuppgiftsansvariges eller person-uppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 (känsliga personuppgifter) och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10.

Det är ytterst få advokatbyråer som idag anmält personuppgiftsombud till Datainspektionen och Advokatsamfundet förutser inte någon påtaglig förändring av den situationen till följd av att dataskyddsförordningen träder i kraft. I detta sammanhang är det viktigt att notera att om advokatbyrån väljer att utse ett dataskyddsombud trots att man inte är skyldig att göra det blir reglerna avseende dataskyddsombud i dataskyddsförordningen tillämpliga även på det frivilligt utsedda dataskyddsombudet.[38] Det är än så länge oklart vad som avses med behandling av känsliga personuppgifter eller uppgifter om lagöverträdelser i stor omfattning. Advokatsamfundets preliminära bedömning är att få advokatbyråer kommer att träffas av anmälningsskyldighet enligt artikel 37 c men det återstår att se hur dataskyddsmyndigheterna bedömer ”stor omfattning”.

---

[37] Artikel 29-gruppens ovan nämnda riktlinjer om konsekvensbedömning, s 14 f.

[38] Se Artikel 29-gruppens Guidelines on Data Protection Officers (‘DPOs’) (WP 243), s 5-6.

7. Personuppgiftsansvarig och personuppgiftsbiträde

7.1 Personuppgiftsansvaret inom advokatverksamhet (artikel 24)

Med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Inom advokatverksamhet är det advokatbyrån (den juridiska personen), inte enskilda advokater eller andra anställda hos byrån, som är personuppgiftsansvarig för den behandling som förekommer hos byrån. För ensampraktiserande advokater som bedriver verksamheten under enskild firma är det advokaten själv som är personuppgiftsansvarig.

Med personuppgiftsbiträde avses den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde får endast behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige.

Inom ramen för hantering av advokatens uppdrag förekommer behandling av personuppgifter i större eller mindre omfattning. Det handlar dels om behandlingar för administrativa ändamål (hantering av penningtvättsregler, klientkonfliktkontroll, förande av klientregister, fakturering etc), dels behandlingar som är relaterade till genomförande av uppdrag (där behandling av personuppgifter kan förekomma i form av brev och e-post, avtal, PM och rättsutredningar, inlagor och yttranden till domstolar och myndigheter etc).

Grundläggande enligt dataskyddsförordningen är att klargöra vem som är personuppgiftsansvarig. Som framgår ovan är det den som bestämmer ändamål och medel för en behandling som är personuppgiftsansvarig. Vem som bestämmer över ändamålen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet. Avgörande för denna bedömning är bl a varför behandlingen utförs och vem som är initiativtagare till behandlingen. Att bestämma över medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen för behandlingen, d v s ”hur” behandlingen ska gå till, exempelvis vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifter och när uppgifter ska raderas.

Det är enligt Advokatsamfundet inte någon tvekan om att det är advokatbyrån som är personuppgiftsansvarig för den behandling av personuppgifter som sker för administrativa ändamål.

Det förekommer ibland att klienter hävdar att klienten är personuppgiftsansvarig och advokatbyrån personuppgiftsbiträde för den behandling som förekommer inom ramen för hantering av ett uppdrag. Eftersom advokaten hanterar ett ärende på uppdrag av och enligt instruktioner från klienten, så måste, hävdas det, advokatbyrån anses behandla personuppgifter för klientens räkning och alltså vara personuppgiftsbiträde. Advokatsamfundets bedömning är dock att det i normalfallet är advokatbyrån som är personuppgiftsansvarig för den behandling av personuppgifter som förekommer inom ramen för uppdragen. Kärnan i advokatens uppdrag är inte behandling av personuppgifter i sig utan tillhandahållande av juridisk rådgivning eller juridiskt biträde som, beroende på uppdragets karaktär, kan innefatta behandling av personuppgifter i större eller mindre omfattning. Det är

därför också normalt advokatbyrån som bestämmer ändamålet med och medlen för behandlingen. Advokatens oberoende ställning, som gäller även i förhållande till klienten, skulle dessutom äventyras om advokaten skulle anses ha ställning som personuppgiftsbiträde med skyldighet att efterkomma klientens instruktioner beträffande personuppgiftsbehandlingen. Det är också vedertaget att det är advokatbyrån som i normalfallet är personuppgiftsansvarig.[39]

Det förekommer att advokatbyråer anlitar andra advokatbyråer, exempelvis för hantering av en viss fråga eller för rådgivning om utländsk rätt. Med stöd av det förda resonemanget agerar den anlitade byrån inte som personuppgiftsbiträde utan som personuppgiftsansvarig med eget ansvar för byråns behandling. I vissa fall kan det tänkas att det föreligger ett gemensamt personuppgiftsansvar, exempelvis om advokater från olika byråer gemensamt hanterar en tvist. Om gemensamt personuppgiftsansvar föreligger ska personuppgiftsansvaret regleras genom ett arrangemang (avtal) enligt vad som närmare följer av artikel 26.

7.2 Innebörden av personuppgiftsansvaret (artikel 24)

Enligt artikel 24.1 dataskyddsförordningen ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Åtgärderna ska genomföras med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

Artikel 24 är ett uttryck för den grundläggande principen om ansvarsskyldighet som anges i artikel 5.2, se avsnitt 2.1 ovan.

Vilka åtgärder som ska genomföras beror som framgår ovan på en helhetsbedömning av en rad olika omständigheter. Enkelt uttryckt gäller att ju mer integritetskänsliga behandlingar det är fråga om desto mer omfattande åtgärder behöver genomföras. I praktiken kan behovet vara olika mellan byrå till byrå och mellan ärende till ärende. Nedan anges ett antal åtgärder som kan aktualiseras:

- Upprättande av policyer, rutiner och processer för personuppgiftsbehandling (artikel 24.2); det kan typiskt sett röra sig om policy för behandling av de anställdas personuppgifter och en policy för behandling av personuppgifter inom ramen för advokatuppdrag, där särskilt fokus bör sättas på behandling av känsliga personuppgifter och andra mer integritetskänsliga personuppgifter
- Genomförande av tekniska och organisatoriska säkerhetsåtgärder
- Dokumentation av personuppgiftsbehandling i form av registerförteckningar
- Genomförande av konsekvensbedömningar
- Genomförande av principer om inbyggt dataskydd och dataskydd som standard (”privacy by design” och ”privacy by default”)

[39] Se exempelvis artikel 29-gruppens Opinion 1/2010 on the concepts of “controller” and “processor” [WP169] s 28 och s 10.

- Regelbunden översyn av åtgärderna och vid behov uppdatering av åtgärderna (artikel 24.1)

Principerna om inbyggt dataskydd och dataskydd som standard har växt fram i praxis, men berörs numera uttryckligen i artikel 25.1 och 25.2. Enkelt uttryckt ska system, processer och rutiner utformas på ett sätt som gör att dataskyddsförordningen och dess dataskyddsprinciper införlivas som ett naturligt inslag i den dagliga verksamheten; lämpliga tekniska och organisatoriska åtgärder ska vidtas för att uppnå detta. Omfattningen av åtgärderna beror på en helhetsbedömning enligt vad som framgår av artikel 25.1. En typ av åtgärd som särskilt lyfts fram är pseudonymisering, d v s att exempelvis namn på personer behandlas i avidentifierad form (t ex en viss nummerkombination), men att det finns en separat ”nyckel” att ”låsa upp” identiteten vid behov.

Åtgärderna ska säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas vad gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Särskilt viktigt är att fler personuppgifter inte ska behandlas än vad som behövs för behandlingens ändamål och att personuppgifterna inte görs tillgängliga för ett obegränsat antal fysiska personer.

När det gäller personuppgiftsbehandling som förekommer i advokatens enskilda uppdrag, såsom vid upprättande av inlagor, avtal, rättsutredningar etc, är det svårt att tänka sig tekniska åtgärder som säkerställer att exempelvis principen om uppgiftsminimering uppfylls. Vilka personuppgifter som behöver behandlas och varför de behöver behandlas är i stor utsträckning styrt av uppdragets karaktär. Det verktyg som finns är närmast att utfärda policyer eller annan information och utbildning om vikten att beakta dataskyddsförordningens grundläggande principer.

En typ av tekniska åtgärder som skulle kunna tänkas är att införa krav på särskilda behörigheter i byråns ärendehanteringssystem, så att endast den eller de advokater som hanterar ett visst ärende har behörighet att ta del av och använda de handlingar som rör ett visst ärende; därmed uppnås ett skydd för de personuppgifter som kan ingå i handlingarna. Enligt Advokatsamfundets bedömning bör man dock inte ställa upp detta som ett generellt krav, då det kan finnas fullt legitima behov för andra än ärendets advokater att gå in i ett ärende, exempelvis för att täcka upp vid sjukdom. Frågan om särskild behörighetsstyrning för ärenden behöver beaktas med hänsyn till advokatbyråns storlek och organisation och karaktären av känslighet på ärendena. I sammanhanget bör dessutom 2.2.2 VRGA uppmärksammas; det är inte tillåtet att göra sig underrättad om ärenden som man inte arbetar med, om det inte finns godtagbara skäl.

7.3 Anlitande av personuppgiftsbiträde (artikel 28)

Det är inte ovanligt att advokatbyråer anlitar tredje man för att hantera delar av verksamheten, genom uppdragsavtal eller genom molntjänster. Det kan exempelvis röra sig om hantering av byråns HR-verksamhet eller IT-infrastruktur eller e-posthantering. Sådan hantering innefattar regelmässigt att uppdragstagaren/molntjänstleverantören behandlar personuppgifter för advokatbyråns räkning.

Av artikel 28.1 dataskyddsförordningen följer att den personuppgiftsansvarige måste säkerställa att anlitade personuppgiftsbiträden ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Avtal med ett personuppgiftsbiträde ska vara skriftligt. Dataskyddsförordningen uppställer mer omfattande krav på avtalets innehåll än vad som gäller enligt PuL. Avtalet ska innehålla i vart fall följande:

- Biträdet får endast behandla personuppgifter enligt den personuppgiftsansvariges dokumenterade instruktioner.
- Biträdet ska åläggas sekretess.
- Säkerhetsåtgärder ska vidtas.
- Biträdet får inte anlita annan för behandling av personuppgifterna utan godkännande av den personuppgiftsansvarige.
- Biträdet ska beroende på omständigheterna hjälpa den personuppgiftsansvarige att hantera begäran från registrerad om utövande av dennes rättigheter.
- Biträdet ska beroende på omständigheterna hjälpa den personuppgiftsansvarige att hantera personuppgiftsincidenter, konsekvensbedömningar och förhandssamråd.
- Exit-hantering; biträdet ska vid biträdesförhållandets upphörande återlämna eller radera alla personuppgifter i enlighet med den personuppgiftsansvariges val.
- Audit-möjlighet; biträdet ska lämna den information och möjliggöra den granskning som krävs för att den personuppgiftsansvarige ska kunna kontrollera biträdets hantering.

Advokatbyråer bör göra en genomgång av befintliga biträdesavtal och vid behov anpassa dem till dataskyddsförordningens krav.

7.4 Advokatbyråns registerförteckning (artikel 30)

Som framgått ovan är det advokatbyrån som är personuppgiftsansvarig för den behandling av personuppgifter som sker för administrativa ändamål. Personuppgiftsansvariga är enligt dataskyddsförordningen skyldiga att föra ett register över sina behandlingar av personuppgifter (artikel 30.1). Vad som ska finnas med i förteckningen framgår uttryckligen i förordningen;

- kontaktuppgifter för personuppgiftsansvarig (advokatbyrån) respektive företrädare samt, i förekommande fall, dataskyddsombud,
- ändamålen med behandlingen,
- en beskrivning av kategorierna av registrerade och kategorierna av personuppgifter,
- eventuella externa mottagare av personuppgifterna och om uppgifter förs över till tredjeland samt
- information om överföringar av personuppgifter till tredje land.

Om möjligt ska även de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter anges samt en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som vidtagits (artikel 32.1).

Även personuppgiftsbiträden är skyldiga att föra förteckning över sina behandlingar, varvid vissa modifierade krav gäller avseende innehållet (artikel 30.2).

Registren ska upprättas skriftligen, inbegripet i elektronisk form. På begäran ska den personuppgiftsansvarige eller personuppgiftsbiträdet göra registret tillgängligt för Datainspektionen. Det är dock värt att påpeka att registret även fyller en utmärkt intern funktion för advokatbyrån där man genom ett uppdaterat register uppnår god ordning och kontroll, vilket underlättar regelefterlevnaden. Exempel på innehåll i en registerförteckning återfinns i bilaga 1.

För att kunna upprätta en registerförteckning behöver advokatbyrån genomföra en kartläggning av samtliga de personuppgiftsbehandlingar som förekommer i verksamheten. Det här gäller således både nya och gamla behandlingar och såväl stora IT-system som enklare excel-filer. I praktiken innebär inventeringen en detaljerad kartläggning av alla register, system och dokument där personuppgifter förekommer. Dokument eller filer av likartad karaktär och för ett enhetligt syfte kan dock anges som en behandling, för att möjliggöra en rimlig arbetsinsats.

I samband med kartläggningen bör säkerställas att det finns ett fastställt ändamål med personuppgiftsbehandlingen, att behandlingen sker i enlighet med gällande dataskyddsprinciper, samt att behandlingen är laglig m m. Genom att dokumentera personuppgiftsbehandlingen säkerställs uppfyllnad av dataskyddsförordningens krav på att kunna visa att förordningens bestämmelser följs.

Advokatbyrån bör utse ”ägarskap” för registerförteckningen eftersom den behöver vara ett levande dokument som uppdateras regelbundet. Vid varje ny personuppgiftsbehandling eller när en behandling förändras eller upphör behöver förteckningen uppdateras.

Det kan nämnas att ovannämnda skyldigheter avseende registerförteckning visserligen inte gäller för företag som sysselsätter färre än 250 personer, såvida inte den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter eller personuppgifter om fällande domar i brottmål samt överträdelser. Enligt Advokatsamfundets uppfattning är detta undantag dock inte tillämpligt på advokatbyråer som regelmässigt behandlar personuppgifter samt uppgifterna ofta omfattar särskilda kategorier av uppgifter och/eller uppgifter om fällande domar i brottmål.

8. Säkerhet i samband med behandlingen (artikel 32)

Enligt artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. Åtgärderna ska vidtas med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter.

Bestämmelsen pekar ut följande typer av åtgärder som bör övervägas:

- pseudonymisering och kryptering av personuppgifter
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Den typ av åtgärder som det i praktiken kan handla om är krypteringsskydd på bärbara datorer, smarta telefoner och surfplattor, kryptering av advokatbyråns trådlösa nätverk, regelbunden säkerhetskopiering och backupsystem, virusskydd, inloggning med krav på viss komplexitet på lösenord som bör bytas med viss regelbundenhet. IT-aktiviteter bör loggas och följas upp med tydlig information till personalen om att detta förekommer.

Ett särskilt problemområde av stor praktisk betydelse vad gäller säkerhet vid behandling av personuppgifter är kommunikation med e-post. En mycket stor del av advokatbyråernas kommunikation sker genom e-post. Säkerhetsnivån i allmän e-postkommunikation är begränsad vilket innebär att det alltid finns en risk för att andra än den avsedda mottagaren kan ta del av meddelandet.

Datainspektionens har i vart fall i två tillsynsbeslut rörande PuL[40] ansett att kommuner som överför känsliga personuppgifter och andra personuppgifter av integritetskänslig natur över öppna nät måste skydda uppgifterna på ett sådant sätt att obehöriga inte kan ta del av uppgifterna. Samtidigt finns det motstående intresse att klienter ska ges ”access to justice” enligt artikel 6 EKMR som innebär att en advokat inte bör uppställa hinder som gör det svårt eller omöjligt för en klient att få tillgång till juridisk representation eller rådgivning.

[40] Datainspektionens beslut Dnr 1082-2006 respektive Datainspektionens beslut Dnr 1161-2007.

Advokatsamfundet anser generellt att en advokatbyrå ska inhämta godkännande från klienten till att kommunicera med e-post. Detta gäller alldeles oavsett om kommunikationen kan förväntas innehålla känsliga personuppgifter eller inte. Det är idag praktiskt svårt att i förhållande till alla klienter anordna krypterad e-postkommunikation. Långt ifrån alla, såväl advokater som klienter, har tillgång till den teknik som krävs. Eftersom artikel 32 föreskriver att den personuppgiftsansvarige ska beakta den senaste utvecklingen och genomförandekostnaderna och behandlingens sammanhang är kryptering, med beaktande av vilka tekniska möjligheter som idag finns och kostnaderna och de praktiska problemen för en advokatbyrå att införa krypterad kommunikation i förhållande till klienter och andra, ur ekonomisk och praktisk synvinkel inte ett genomförbart alternativ. Vid bedömningen enligt artikel 32 bör också vägas in att klienter kan ha behov av att snabbt och enkelt få tillgång till ett juridiskt ombud och att det i en sådan situation kan innebära en risk för rättsförlust för klienten om klienten först skulle behöva installera ett krypteringsprogram för att alls kunna kommunicera med sitt ombud och skicka ombudet underlag för den juridiska bedömningen eller representationen. Den viktiga roll som advokater har när det gäller att ge klienter ”access to justice” talar för att den intresseavvägning mellan risk för integritetsintrång och motstående praktiska och ekonomiska intressen bör utfalla så att krypterad kommunikation i de allra flesta fall inte är nödvändig.

Ett godkännande från klienten att använda e-post ”läker” en del av dataskyddsproblematiken. Om ett e-postmeddelande innehåller känsliga personuppgifter om en motpart, om en klients anställda eller om andra personer, kan inte en viss risk att advokatbyrån kan drabbas av ingripanden med stöd av dataskyddsförordningen om meddelandet kommer i orätta händer uteslutas. Ett sätt att öka säkerheten är att lösenordsskydda dokument som skickas per e-post. Lösenordet måste då utväxlas på annat sätt än genom e-post, exempelvis muntligen eller genom SMS. Ett annat sätt kan vara att kommunicera genom digitala brevlådor.

Det kan dock över tid antas att enkelt tillgängliga funktioner för säker e-post och liknande etableras så att det kan krävas att de ska användas utan att klientens ”access to justice” riskerar att trädas förnär.

9. Personuppgiftsincidenter

9.1 Anmälan av personuppgiftsincident till Datainspektionen (artikel 33)

Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Det kan exempelvis röra sig om ett dataintrång, en s k phishing-attack, en borttappad eller stulen persondator eller att en anställd obehörigen har tagit del av eller röjt personuppgifter. Ett exempel kan också vara hur en anställd olovligen eller annars utan godtagbara skäl bereder sig tillgång till eller för annan person gör tillgänglig information i ärenden de inte ska få ta del av.[41]

[41] Jfr 2.2.2 VRGA.

Enligt artikel 33.1 ska en personuppgiftsincident anmälas till Datainspektionen utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att vetskap om incidenten fåtts. Om anmälningen inte görs inom 72 timmar ska man, när anmälan görs, lämna en motivering till förseningen. Om det inte är möjligt att lämna all informationen samtidigt, får informationen lämnas i omgångar utan onödigt ytterligare dröjsmål (artikel 33.4).

Om ett personuppgiftsbiträde får vetskap om en personuppgiftsincident ska biträdet underrätta den personuppgiftsansvarige om incidenten ”utan onödigt dröjsmål”. Någon särskild tidsrymd anges inte, men det bör vara fråga om en ganska omgående underrättelse.

En anmälan behöver inte göras om det är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter. Om det exempelvis har förekommit ett dataintrång, men kryptering har hindrat intrångsgöraren från att få åtkomst till uppgifterna så behöver anmälan inte göras.

Anmälningen ska innehålla åtminstone följande information (artikel 33.3):

a) Beskrivning av personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs.
b) Namn och kontaktuppgifter på personuppgiftsombudet eller annan där ytterligare information kan erhållas.
c) Beskrivning av de sannolika konsekvenserna av incidenten.
d) Beskrivning av de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.

Observera att alla personuppgiftsincidenter måste dokumenteras, även om anmälningsskyldighet inte skulle föreligga. När en incident inte har anmälts till Datainspektionen är det lämpligt att dokumentera bedömningen till att anmälan inte ansetts nödvändig.

Underlåtenhet att anmäla en personuppgiftsincident kan leda till påförande av administrativa sanktionsavgifter och andra ingripanden.

För närmare vägledning om anmälan av personuppgiftsincidenter hänvisas till Artikel 29-gruppens vägledningsdokument.[42]

9.2 Information om personuppgiftsincidenten till den registrerade (artikel 34)

Utöver skyldigheten att anmäla personuppgiftsincidenter till Datainspektionen måste information om incidenter i vissa fall lämnas till de registrerade som drabbats. Detta är fallet om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter (artikel 34.1). Informationen ska lämnas utan onödigt dröjsmål, ska innehålla en

[42] Se Guidelines on Personal data breach notification under Regulation 2016/679 WP250.rev01.

tydlig och klar beskrivning av personuppgiftsincidentens art och i vart fall omfatta den information som anges i artikel 33.3 b–d ovan.

Information till de registrerade behöver inte lämnas om:

a) Kryptering eller annan skyddsåtgärd har förhindrat åtkomst eller tillgång till personuppgifterna, eller
b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå, exempelvis om en obehörig har lyckats tillskansa sig personuppgifter men den personuppgiftsansvarige genom snabbt agerande har förhindrat exempelvis nyttjande, spridning eller förstörelse av uppgifterna, eller
c) Det skulle inbegripa en oproportionell ansträngning att informera de registrerade. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

Det är tydligt att skyldigheten att informera de registrerade om en personuppgiftsincident kan komma i konflikt med advokatens skyldighet att iaktta tystnadsplikt och lojalt beakta klientens intressen. Detta är fallet om den registrerade som omfattas av incidenten är någon annan än advokatbyråns klient, exempelvis en motpart. Dataskyddsförordningen innehåller inget undantag från informationsskyldigheten för det fall att behandlingen omfattas av lagreglerad tystnadsplikt. På motsvarande sätt som är fallet vad gäller den registrerades rättigheter (se 4.4 ovan) kan lämnande av information om en inträffad personuppgiftsincident komma att försämra klientens ställning som part i rättegången.

Artikel 23.1 skapar möjlighet för medlemsstaterna att införa begränsningar när det gäller skyldigheten att informera de registrerade om personuppgiftsincidenter när den personuppgiftsansvarige omfattas av tystnadsplikt. Något sådan begränsning föreslås inte i propositionen och det är osäkert om regeringen kommer att utfärda någon sådan begränsning.

Skulle ingen sådan begränsning införas är advokaten skyldig att informera de registrerade om personuppgiftsincidenter, i den utsträckning som följer av dataskyddsförordningen. På motsvarande sätt som anges i 4.4 ovan är det Advokatsamfundets uppfattning att advokatens tystnadsplikt enligt 8 kap 4 § rättegångsbalken gäller framför de registrerades rättigheter enligt dataskyddsförordningen.

Det bör observeras att Datainspektionen kan förelägga den personuppgiftsansvarige att informera de registrerade om att en personuppgiftsincident har inträffat (artikel 34.4). Datainspektionen kan även besluta att något av undantagen från informationsskyldigheten i artikel 34.3 är för handen.

Underlåtenhet att informera om personuppgiftsincident, när undantag inte är för handen, kan leda till påförande av administrativa sanktionsavgifter och andra sanktioner.

10. Överföring av personuppgifter till tredjeländer eller internationella organisationer

10.1 Tredjelandsöverföringar (mobila tjänster – adresslistor – e-post)

I den pågående globaliseringen och mot bakgrund av den tekniska utveckling vi ser är det viktigt att kunna överföra information fritt till varhelst informationen behöver användas. Det här berör alla organisationer som använder någon form av tjänst där överföring av information över gränserna förekommer, t ex många vanliga online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser.

Det är dock viktigt att framhålla att upprätthållande av advokatsekretessen alltid måste gå före eventuella operationella fördelar och kostnadsbesparingar genom exempelvis användning av publika molntjänster som tillhandahålls av globala leverantörer. Det är inte ovanligt att det i avtal med molntjänstleverantörer föreskrivs att det är upp till leverantören att avgöra om kundens information ska avslöjas för främmande makts myndigheter eller annan tredje man, ibland utan att kunden informeras om sådant avslöjande. Om inte advokatsekretessens upprätthållande kan säkerställas bör klientinformation inte hanteras i den typen av tjänster. Klienten ska inte utsättas för risken att främmande makts myndigheter har tillgång till information som i förtroende avslöjats för advokaten, i annan utsträckning än vad som följer av tvingande svensk rätt.

För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring)[43] gäller särskilda regler. Genom dataskyddsförordningen har alla EU:s medlemsstater samt EES-länderna ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom EU/EES-området utan begränsningar (förutsatt naturligtvis att man uppfyller förordningens allmänna krav för tillåten behandling av personuppgifter). För länder utanför det här området finns däremot inte några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar (artikel 44).

Överföring av personuppgifter till tredje land får enligt dataskyddsförordningen endast ske i följande situationer och under förutsättning att övriga regler i förordningen följs:

(i) jurisdiktionen där mottagaren är belägen anses ha en adekvat nivå på skyddet av uppgifterna,
(ii) exporterande organisation (advokatbyrån) vidtar lämpliga skyddsåtgärder för att skydda för personuppgifterna eller
(iii) något undantag är tillämpligt.

[43] Med ”tredje land” avses fortsättningsvis länder utanför EES området och länder eller territorier eller sektorer som Kommissionen har beslutat säkerställer en adekvat skyddsnivå (dessa länder/territorier/sektorer är för närvarande Andorra, Argentina, Bailiwick of Guernsey, Färöarna, Isle of Man, Israel, Jersey, Nya Zeeland, Schweiz, Uruguay, Kanada (om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling) och USA (om mottagaren har anslutit sig till Privacy Shield). Överföring av personuppgifter till tredjeländer eller territorier som anses ha en adekvat skyddsnivå kräver enligt artikel 45 (1) inte något särskilt tillstånd.

Beslut om adekvat skyddsnivå
Om EU-kommissionen har beslutat att ett tredje land säkerställer en adekvat skyddsnivå får man föra över personuppgifter dit utan något särskilt tillstånd. Ett sådant beslut kan också gälla ett visst territorium, en internationell organisation eller en eller flera sektorer i ett tredje land. Se fotnot 43 för en uppräkning av de beslut som för närvarande föreligger.

Lämpliga skyddsåtgärder
De skyddsåtgärder som kan aktualiseras är bindande företagsregler (s k Binding Corporate Rules, BCR:s) som godkänts av tillsynsmyndigheten eller standardiserade dataskyddsbestämmelser som godkänts av EU-kommissionen, s k standardavtalsklausulerna (eller som beslutats av en tillsynsmyndighet och därefter godkänts av EU-kommissionen). Överföringen kan också grunda sig på en godkänd uppförandekod eller en godkänd certifiering under förutsättning att dessa blir rättsligt bindande och verkställbara också gentemot mottagaren av uppgifterna. Inget särskilt tillstånd krävs däremot av tillsynsmyndighet inför varje överföring. För närmare detaljer, se artikel 46–48 dataskyddsförordningen.

Tillämpliga undantag
I vissa särskilda situationer får tredjelandsöverföring ske trots att landet inte har en adekvat skyddsnivå och trots att inte lämpliga skyddsåtgärder har vidtagits (se för detaljer artikel 49.1, första stycket samt skäl 111–112). Personuppgifter kan till exempel överföras om den registrerade, efter att ha blivit informerad om riskerna, uttryckligen har lämnat sitt samtycke eller om det är nödvändigt i vissa uppräknade fall (till exempel för att fullgöra ett avtal på den registrerades begäran eller för att fastställa, göra gällande eller bevaka rättsliga anspråk, vilka har betydelse för advokatverksamhet).

Överföring av personuppgifter är också enligt artikel 49.1, andra stycket tillåten om den endast sker vid *ett enstaka tillfälle*, endast gäller ett begränsat antal registrerade och sker efter en intresseavvägning. En sådan intresseavvägning ska innebära att överföringen är nödvändig för ändamål som rör tvingande berättigade intressen hos den personuppgiftsansvarige och att den registrerades intressen eller fri- och rättigheter inte väger tyngre. Det krävs också att den personuppgiftsansvarige, efter en bedömning av samtliga omständigheter kring överföringen, har vidtagit lämpliga åtgärder för att skydda personuppgifter. Observera dock att om överföring sker i en sådan situation ska den personuppgiftsansvarige informera både tillsynsmyndigheten och de registrerade om överföringen och om de tvingande berättigade intressen som man vill uppnå.

Advokatsamfundet noterar att globaliseringen och kraven på normal affärsverksamhet idag ställer stora krav på advokats tillgänglighet och att tillgång i många situationer kan kräva att advokaten reser även till tredje land. Tillgång till information i advokatbyråns egna system över e-post och med egen bärbar utrustning etc kan därvid behövas. Som framgått i avsnittet om säkerhet i samband med behandlingen (avsnitt 8), ställs redan krav på säker hantering av informationen samtidigt som det också ställs krav på snabb tillgång och att det inte bör uppställas hinder som gör det svårt eller omöjligt för en klient att få tillgång till juridisk representation eller rådgivning även när advokaten befinner sig i tredje land etc. Med

iakttagande av lämpliga säkerhetsåtgärder och där tillgång till information endast sker genom s k vpn-tunnel eller motsvarande säkerhetsåtgärd och vid enstaka tillfällen anser Advokatsamfundet att advokats egen tillgång till information i det läget inte ska betraktas som en överföring som kräver några ytterligare åtgärder.

11. Övriga frågor

11.1 Externt dataskyddsombud

En organisation kan välja att genom uppdragsavtal lägga ut ett uppdrag som dataskyddsombud externt, t ex på en advokat. Uppdragets omfattning kan innefatta att utföra vad som krävs för att organisationen ska efterleva dataskyddsförordningen vad gäller ombudsfunktion och behöver således inte vara ett heltidsuppdrag. Dataskyddsombudet skall dock få tillräckligt med tid och resurser för att kunna utföra sitt uppdrag på ett bra sätt.

En advokat som överväger att åta sig arbete som externt dataskyddsombud behöver beakta regler rörande intressekonflikt respektive tystnadsplikt såväl enligt VRGA som enligt dataskyddsförordningen och den nationella dataskyddslagen samt offentlighets- och sekretesslagen (2009:400).[44]

Fråga har uppkommit om advokater kan åta sig uppdrag som externt dataskyddsombud. Advokatsamfundets uppfattning är att det är möjligt, förutsatt att övriga förutsättningar för antagande av uppdraget på vanligt sätt beaktas av advokatbyrån (d v s uppdrag hos övriga kollegor, risk för intressekonflikter etc). Den skyldighet att anmäla brister i hanteringen hos den personuppgiftsansvarige till Datainspektionen som åvilat ett personuppgiftsombud i vissa fall enligt PuL:s regler försvinner i och med dataskyddsförordningen, vilket också gör att eventuella invändningar om intressekonflikter i den delen faller. Uppdraget behöver dock vara noggrant beskrivet och avgränsat i ett uppdragsavtal.

Även om artikel 37.5 inte anger specifikt vilka yrkesmässiga kvalifikationer som bör övervägas vid utnämnandet av ett dataskyddsombud, framgår det av Artikel 29-gruppens vägledning för dataskyddsombud att det är särskilt relevant just med juridiska kunskaper och det läggs större vikt vid det än vid särskild teknisk kompetens. Att vägledningen tydligt lägger stor vikt vid dataskyddsombudets juridiska kunskaper föranleder Advokatsamfundet att dra slutsatsen att rollen under vissa förutsättningar kan fyllas av en advokat med relevanta kunskaper.[45] Kraven på tydlighet gentemot klienten föranleder dock att det behövs närmare preciseringar av uppdraget i uppdragsavtalet.

---

[44] Såvitt avser GDPR utgör intressekonflikt vid utseende av dataskyddsombud ett allvarligt brott mot dataskyddsreglerna och är förenat med höga administrativa sanktioner. Sanktionen kan uppgå upp till tio miljoner euro eller upp till två procent av företagets globala årsomsättning.

[45] Därigenom undviks ju också den risk för intressekonflikter som annars kan föreligga för ett dataskyddsombud som är anställd i organisationen och som därmed inte får ha andra uppgifter som kan leda till intressekonflikter enligt artikel 38.6. Ett sådant dataskyddsombud kan då i princip inte vara med och fastställa ändamålen med och medlen för behandlingen av personuppgifter.

Såvitt avser personuppgiftsansvaret för den information som behandlas inom ramen för ett uppdrag som externt dataskyddsombud gäller följande:

(i) Advokat som utför uppdrag som dataskyddsombud kan inom ramen för uppdraget använda sig av antingen sina egna (advokatbyråns) verktyg och processer i genomförandet av uppdraget, alternativt av uppdragsgivarens (klientens) verktyg och processer. Om advokaten använder sig av egna verktyg och processer och i det sammanhanget bestämmer vilka personuppgifter som ska samlas in, varifrån uppgifterna ska samlas in och hur behandlingen ska utföras i övrigt, har advokaten en så pass självständig ställning att advokatbyrån där advokaten är verksam är personuppgiftsansvarig även för behandling av uppgifter som utförs inom ramen för uppdraget som dataskyddsombud. Sedvanliga regler avseende personuppgiftsansvar för advokatbyrån blir därmed tillämpliga.[46]

(ii) Om advokaten däremot använder sig av uppdragsgivarens verktyg och processer och uppdragsgivaren istället bestämmer hur uppgifterna ska samlas in och behandlingen utföras bör uppdragsgivaren betraktas som personuppgiftsansvarig.

(iii) I tillägg torde det även vara vanligt att uppdragsgivaren (klienten) även delar vissa uppgifter med advokaten t ex i dokumentationssyfte, vilket innebär att personuppgifterna därmed förekommer hos två separata personuppgiftsansvariga och advokatbyråns sedvanliga personuppgiftsansvar blir även där tillämpligt.

11.2 Konkursförvaltning

En advokat som åtar sig arbete som extern konkursförvaltare behöver på motsvarande sätt beakta reglerna rörande behandling av personuppgifter.

Konkursförvaltaren träder in som företrädare för konkursboet och under den tid konkursen pågår är det konkursförvaltaren som sköter förvaltningen av de tillgångar och skulder som finns i konkursboet. Det är också konkursförvaltaren som bestämmer om verksamheten ska drivas vidare eller om egendomen ska säljas direkt. Konkursförvaltaren kan karaktäriseras som en fristående mellanman med ett på konkurslagen grundat uppdrag att realisera och avveckla konkursboet. Konkursförvaltaren har ensam rätt att företräda konkursboet.

Advokaten bör särskilja mellan den behandling av personuppgifter som sker inom ramen för konkursboets verksamhet, respektive den behandling som sker inom advokatfirmans normala verksamhet. Det är här således fråga om *två olika personuppgiftsansvariga*, med två olika behandlingsregister, olika integritetsskyddspolicyer etc som ska tillämpas. Till den delen som åtgärder vidtas, och behandling av personuppgifter sker, inom ramen för konkursboets verksamhet är det alltså konkursboet som är personuppgiftsansvarigt. En konkursförvaltare som tar över ett bo behöver således sätta sig in i även vilken behandling av personuppgifter som sker, vilken information som har lämnats till de registrerade och vilka ramar i övrigt som gäller för behandlingen.

---

[46] För den generella efterlevnaden av dataskyddsförordningen i övrigt, d v s i verksamheten, svarar givetvis klienten på vanligt sätt.

12. DATASKYDDSFÖRORDNINGEN – RÄTTSKÄLLOR OCH NYHETSKÄLLOR

Dataskyddsförordningen

- 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 (allmän dataskyddsförordning)

  https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/forordningstexten/

  https://www.datainspektionen.se/Documents/Dataskyddsf%C3%B6rordningen%20-%20Datainspektionen.pdf (pdf-version)

- Datainspektionens webbsidor om dataskyddsförordningen

Artikel 29-gruppens riktlinjer rörande Dataskyddsförordningens tillämpning

- Guidelines on Consent under Regulation 2016/679, wp259
- Guidelines on Transparency under Regulation 2016/679, wp260
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01
- Guidelines on Personal data breach notification under Regulation 2016/679, wp250
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, wp251
- Guidelines on the right to "data portability", wp242rev.01_en
- Guidelines on Data Protection Officers ('DPOs'), wp243rev.01_en
- Guidelines on The Lead Supervisory Authority, wp244rev.01_en
- Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, wp253
- Artikel 29-gruppens nyhetssida

Förslaget till lag med kompletterande bestämmelser till EU:s dataskyddsförordning och förslaget till förordning med kompletterande bestämmelser till EU:s dataskyddsförordning

- SOU 2017:39 Ny dataskyddslag
- Proposition 2017/18:105 Ny dataskyddslag

Förslaget till ny kamerabevakningslag

- SOU 2017:55 En ny kamerabevakningslag

Datainspektionens föreskrifter rörande personuppgiftslagen

- DIFS 2010:1 Föreskrifter om ändring av Datainspektionens föreskrifter (DIFS 1998:3) om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser m.m.; (Föreskrifterna kommer sannolikt att ändras i och med att Dataskyddsförordningen träder ikraft)

- DIFS 2013:1 Föreskrifter om ändring av Datainspektionens föreskrifter (DIFS 1998:2) i fråga om skyldigheten att anmäla behandlingar av personuppgifter till Datainspektionen; (Föreskrifterna kommer sannolikt att ändras i och med att Dataskyddsförordningen träder ikraft)