Vägledning för tillämpning av EU:s dataskyddsförordning i ombudsverksamhet

INLEDNING

Den 25 maj 2018 började dataskyddsförordningen (GDPR) att tillämpas i alla EU:s medlemsstater. Dataskyddsförordningen har ställt fler och hårdare krav på de som behandlar personuppgifter och även gett de nationella tillsynsmyndigheterna utökade befogenheter och möjligheter att besluta om administrativa sanktionsavgifter. Varje företag behöver därmed ha ett klokt förhållningssätt till hur personuppgifter hanteras.

Dataskyddsförordningen är direkt tillämplig i Sverige, men kompletteras även genom lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (kallad kompletteringslagen). Vägledningen till lagstiftningen inhämtas från den s.k. artikel 29-gruppens uttalanden och publicerades i prop. 2017/18:105 Ny dataskyddslag. Vägledningen ska ses som ett levande dokument och uppdateras löpande, bl.a. när ny lagstiftning och nya föreskrifter antas och när rättspraxis tillkommer.

Sveriges Patentbyråers förening (SEPAF) har tidigare tagit fram en vägledning för tillämpningen av EU:s dataskyddsförordning genom att tillsätta en grupp med uppgift att utifrån medlemmarnas specifika verksamheter göra GDPR-sammanställning. Det är även av stor vikt för de auktoriserade patentombuden att vägledningen från SEPAF är analogt tillämpade och enhetliga med Advokatsamfundets hantering av personuppgifter. Liksom advokater följer auktoriserade patentombud liknande regler om lagring och behandling av uppgifter, samt kontroller av intressekonflikter. Regler för patentombud och auktorisation finns i lag (2010:1052) om auktorisation och Bolagsverkets föreskrift (BOLFS 2012:1) Patentombudsnämndens allmänna råd med vägledande regler om god patentombudssed. För att ge en så specifik vägledning som möjligt och som besvarar branschens utmaningar har SEPAF:s styrelse vid sitt sammanträde den 23 september 2020 beslutat att uppdatera sina vägledningsdokument för att den ska spegla gällande reglering.

Framställningen innehåller numera en innehållsförteckning och är vidare uppdelad mellan del I och del II. Del I är allmän information för alla företag inom SEPAFS verksamhetsområde. Den innehåller grundläggande information om dataskydd, hantering och säkerhet och ger exempel på registerförteckning, integritetspolicy, konsekvensbedömning och incidentrapport i bilagor. Del II innehåller fördjupad information om rättsliga grunder för databehandling, rättigheter och skyldigheter vid behandling, personuppgiftsbiträden och vad som ska gälla vid incidenter.

Uppdaterad november 2020 av Jennie Nilsson, jurist, Svensk Industriförening

Innehållsförteckning

DEL II – FÖRDJUPAD INFORMATION

DEL I
Allmän information

1. Grundläggande information för en ansvarsfull databehandling

1.1 Kortfattat om syftet bakom dataskyddsförordningen och förändringarna sedan införandet.

Dataskyddsförordningen även kallad GDPR (General Data Protection Regulation) har till syfte att ge ett stärkt skydd för de personer vars personuppgifter behandlas. Den ställer därmed fler och hårdare krav, än tidigare lagstiftning (PUL), på den som behandlar personuppgifter för egen eller annans räkning. Varje verksamhet behöver därför ha ett väl övervägt och klokt förhållningssätt till hur personuppgifter ska hanteras i verksamheten.

De största skillnaderna till följd av Dataskyddsförordningen är att samma lagstiftning nu tillämpas i hela EU. Det här har lett till en mer enhetlig rättstillämpning inom unionen. De grundläggande principerna för personuppgiftsbehandling har med dataskyddsförordningen blivit tydligare, samt att informationsskyldigheten i förhållande till de registrerade utökas och så även den registrerades rättigheter. Den personuppgiftsansvarige är dessutom skyldig att visa att dataskyddsförordningen efterlevs. Det här innebär en omfattande dokumentationsskyldighet, och krav på registerförteckning, konsekvensbedömning och gallringsrutiner.

Den mest kännbara förändringen för en personuppgiftsansvarig är att 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) kan utges vid allvarliga överträdelser, till skillnad mot tidigare reglering där överträdelser normalt enbart ledde till påpekanden från Integritetsmyndigheten[1] (tid. Datainspektionen). Förordningen ger därmed de nationella tillsynsmyndigheterna (i Sverige Integritetsmyndigheten) utökade befogenheter och en möjlighet att besluta om administrativa sanktionsavgifter.

Om din organisation anlitar personuppgiftsbiträde behöver det finnas tydliga regler mellan personuppgiftsansvarig och personuppgiftsbiträdet. Biträdets roll är att med avtal som laglig grund hantera den personuppgiftsansvariges register med personuppgifter enligt instruktioner. Det juridiska ansvaret för personuppgiftsincidenter ligger dock kvar hos den ansvarige. Personuppgiftsbiträdets roll har förtydligats under senare tid genom avgöranden från EU-domstolen.

Dataskyddsförordningens reglering visar en tydlig strävan efter proaktivt arbete. Det föreligger höga krav på personuppgiftsbehandlingen men även den omfattande skyldigheten att dokumentera, registrera, bedöma och ha tydliga rutiner. Som personuppgiftsansvarig ska inte detta enbart hanteras på ett klandervärt sätt du ska även genom register kunna visa hur du för dina register och hanterar personuppgifterna. Det ställs därmed väldigt höga krav på den ansvarige att föra register över registreringen och att detta är komplett och kontrollerbart.

[1] Integritetsskyddsmyndigheten är det nya namnet på Datainspektionen, från och med 1 januari 2021.

En viktig fråga ur dataskyddsperspektiv har under året varit vad som gäller vid personuppgiftsöverföringar till tredje länder. Föremål för avgörande har varit det amerikanska och europeiska dataskyddsavtalet ”Privacy Shield” som EU-domstolen underkände som laglig grund för att behandla personuppgifter i servrar i USA. Företag har tidigare kunnat ansluta sig till Privacy Shield och därmed tidigare ansetts ha ett fullgott skydd men svenska företag har istället under året ombetts att omedelbart flytta sina servrar tillbaka till EU.

Det finns mycket positivt med utvecklingen av GDPR men det råder fortfarande en hel del oro kring datasäkerhet, övervakning och integritetsintrång. Alla organisationer måste lära sig att hantera dataskyddet för att inte förlora sitt förtroendekapital. Dataskyddsförordningen har därmed skapat ett större allvar och säkerhetstänk rörande skydd och respekt för individens integritet.

1.2 En verksamhet behöver kunna besvara följande frågor

Varje verksamhet bör ha processer och dokumentation på plats för att kunna besvara nedanstående frågor. Detta för att möjliggöra att verksamheten kan bedrivas på ett sätt som är förenligt med dataskyddsförordningen:

1. Är alla i organisationen **informerade** om dataskyddsförordningen och de processer som ska tillämpas för att följa regelverket?
2. Har vi en **rättslig 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 ar **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? Exempel på sådana rättigheter är rätten att få en kopia på den information som behandlas, rätten till korrigering- eller radering av uppgifter.
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?

De typiska bristerna när det gäller efterlevnaden av dataskyddet och som återkommande påpekats i Integritetsmyndighetens tillsynsbeslut, sedan dataskyddsförordningen infördes, har varit följande:

- Rättigheten att få information om hur personuppgifterna behandlas. Det har handlat om svårigheter att få sina uppgifter raderade, få registerutdrag eller information om hur de personliga uppgifterna behandlas.
- Klagomål om att verksamheter skickar runt personuppgifter genom okrypterade mejl eller inte använder dold kopia. Det kommer även in klagomål på felaktiga brev, sms och mejlutskick.
- Avsaknad av rättslig grund för behandlingen. Många gånger finns grund för behandling men den har inte angetts på ett sätt som gör den legitim. Vanlig missuppfattning är att samtycke krävs i större omfattning än vad det gör.
- Direkt marknadsföring är ytterligare ett av klagomålen. Medborgare meddelar att de inte önskar reklamutskick men erhåller det trots upprepade meddelanden om att samtycke saknas.
- Utlämnande av uppgifter från myndighet till tredje part. Myndigheter har dock skyldighet att lämna ut allmän handling vid förfrågan och i fall där handlingen inte är belagd med sekretess.

- Uppgiftsminimering är ett klagomål som handlar om att verksamheten inte ska behandla fler uppgifter än nödvändigt utan enbart samla uppgifter som är relevanta för ändamålet. Det finns stora brister kring detta och många gånger efterfrågas fler uppgifter än vad verksamheten behöver ha om sina kunder.

Enligt dataskyddsförordningen är det verksamheten som samlat in och behandlar personuppgifterna som är ansvarig för att kunna visa att principerna för behandling av personuppgifter är uppfyllda, vilket innebär att dokumentation, tydliga processer och rutiner måste finnas på plats.

1.3 Åtgärder för en ansvarfull process

Åtgärder som bör övervägas för att på ett bra sätt kunna uppfylla förordningens krav är:

1. Kartläggning av personuppgifter och dess behandling samt upprättande av en registerförteckning.
2. Säkerställande av att det finns en rättslig grund för behandlingen eller samtycke.
3. Utbildning av personal rörande dataskyddsförordningen.
4. Se över sin information till de olika kategorierna av registrerade.
5. Verksamheten måste hantera särskilda integritetsrisker.
6. Verksamheten är skyldig att rapportera personuppgiftsincidenter till Integritetsmyndigheten och ge information till de registrerade.
7. Verksamheten bör upprätta interna styrande dokument såsom integritetspolicy etc.
8. Verksamheten bör se över sina/upprätta personuppgiftsbiträdesavtal.
9. Verksamheten behöver införa gallringsrutiner och se över hur länge personuppgifter lagras och behandlas.
10. Rutiner för att säkerställa de registrerades rättigheter bör införas.
11. Den tekniska säkerheten bör ses över.
12. Verksamheten behöver säkerställa att uppgifter som överförs till tredje land skyddas på ett adekvat sätt.
13. Verksamheten behöver anpassa uppdragsavtal, anställningsavtal m.m.
14. Verksamheten behöver se över behandlingen av särskilda kategorier av uppgifter och behandling av personnummer.
15. Telefon- och klientregister bör vara aktuella eller åtminstone motiverade.
16. Patentombuds tystnadsplikt skyddar mot att behöva lämna ut information.
17. Dataskyddsombud bör utses.

1.3.1 Kartläggning av personuppgifter och dess behandling samt upprättande av registerförteckning
Verksamheten 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. Verksamheten 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 samt Del II i denna vägledning för närmare information om de grundläggande principerna för behandling av personuppgifter, registerförteckning m.m.). En noggrann kartläggning hjälper verksamheten att uppfylla dataskyddsförordningens krav, bl.a. genom att kunna visa att förordningens bestämmelser följs. Den kan också användas som underlag för andra åtgärder såsom gap-analys och uppföljning.

Typiska IT-system som förekommer i patentverksamhet 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 patentbyråer behandlar personuppgifter är bedömning av jävsfrågor, register över uppfinnare och designers, tillvaratagande av klients rättsliga intressen och behandling för administrativa ändamål. Andra interna ändamål är administration och uppföljning av rekrytering och anställning.

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

1.3.2 Rättslig grund för behandlingen

Av dataskyddsförordningen följer att personuppgifter får behandlas endast om det finns en rättslig grund för behandlingen. Vanligt förekommande rättsliga grunder för en verksamhets behandlingar är att de är nödvändiga för att fullgöra ett avtal (t.ex. avtal med klient, kund 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, 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 då den rättsliga grunden upphör att gälla så snart samtycket återkallas.

1.3.3 Utbildning av personal

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

1.3.4 Översyn av information till de registrerade

Den information som nu lämnas till registrerade bör granskas. Verksamheten behöver anpassa informationen till dataskyddsförordningens krav på utökad information. De typiska kategorierna av registrerade är klienter och kunder, presumtiva klienter och kunder 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**.** 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 (se bilaga 3 för exempel) eller motsvarande som exempelvis kan publiceras på verksamhetens hemsida eller överlämnas i tryckt form. Se ett exempel på information till den registrerade i bilaga 2.

1.3.5 Analys av integritetsrisker

Verksamheten behöver i egenskap av personuppgiftsansvarig 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 verksamhetens anställda eller av andra personer. Se närmare i den fördjupade informationen i Del II samt bilaga 4 på exempel på konsekvensbedömning.

1.3.6 Incidentrapportering

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 verksamheten (personuppgiftsbiträden) och dokumenteras i avtal. När det inte är osannolikt att en incident medför risker för enskildas fri- och rättigheter måste händelsen anmälas till Integritetsmyndigheten inom 72 timmar. Se bilaga 5 för mall för incidentrapport. 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 Upprättande av interna styrande dokument

Verksamheten bör ta fram en intern integritetspolicy med information om hur personuppgifter ska hanteras av alla anställda och vilka regler som gäller internt, se bilaga 3 för ett exempel på en enkel policy. Policyn bör även göras enkelt tillgänglig, t.ex. på intranät, samt tydligt kommuniceras till alla anställda som ett led 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.

1.3.8 Personuppgiftsbiträdesavtal

Det är den verksamhet som samlar in och bestämmer syftet med behandlingen som är personuppgiftsansvarig och som också är ytterst ansvarig för behandlingen av personuppgifter. Detsamma gäller när behandlingen utförs av ett s.k. personuppgiftsbiträde, d.v.s. av någon som behandlar personuppgifter för verksamhetens 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 verksamheten är ansvarig för. Verksamheten 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. Vid anlitandet av ett personuppgiftsbiträde ska det upprättas ett skriftigt avtal, ett så kallat *personuppgiftsbiträdesavtal*, som reglerar behandlingen. Kraven på personuppgiftsbiträdesavtalen har i många avseenden förtydligats, vilket innebär att även befintliga avtal som regel behöver uppdateras. För personuppgiftsbiträde i ett tredje land se punkt 1.3.12.

1.3.9 Lagring och gallringsrutiner

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 anonymisering sker eller 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 av ändamålet med att exempelvis ett e-postmeddelande eller dokument 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.

1.3.10 Rutiner för att säkerställa de registrerades rättigheter

Utöver en rutin för att lämna information till registrerade, behöver verksamheten också etablera förfaranden för att hantera registrerades förfrågningar om registerutdrag, begäran om att få felaktiga uppgifter rättade eller att få uppgifter raderade, invändningar mot direktmarknadsföring eller automatiserat beslutsfattande, eller begäran om s.k. dataportabilitet (se vidare i 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.

1.3.11 Teknisk säkerhet

Verksamheten 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 som bör innehålla 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 verksamheten 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.

1.3.12 Överföringar till tredje land

Verksamheter som använder t.ex. IT-leverantörers eller andra underleverantörers produkter och tjänster (såväl extern leverantör som koncernbolag i en större verksamhet/koncern) anlitar normalt leverantörer som behandlar personuppgifter. Denna behandling är som ovan beskrivits verksamheten ansvarig för. Därmed behöver en kontroll göras av i vilken utsträckning underleverantören behandlar uppgifterna, eller bereder sig tillgång till uppgifterna från tredje land.[2] I en sådan situation behöver det

[2] Med ”tredje land” avses fortsättningsvis länder utanför EES området och länder eller territorier eller sektorer som Kommissionen har beslutat säkerställer en adekvat skyddsnivå (dessa

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).

1.3.13 Anpassning av uppdragsavtal, anställningsavtal m.m.
Alla verksamhetens befintliga avtal bör gås igenom för att göra en bedömning av huruvida de är förenliga med dataskyddsförordningen krav. Innehållet i befintliga avtal, anställningsavtal, separata personuppgiftspolicies/informationstexter etc. behöver ses över med avseende på den information som verksamheten lämnar till registrerade om hur den behandlar dennes personuppgifter. Tilläggsavtal och/eller uppdatering av separata personuppgiftspolicies/informationstexter kan således behöva upprättas och/eller kommuniceras i anslutning till vissa befintliga avtal.

Även uppdragsavtal och personuppgiftspolicies/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 verksamheten behandlar personuppgifterna (avser såväl kontaktuppgifter till klient/kund etc. som personuppgifter som verksamheten kan komma att erhålla inom ramen för ett ärende).

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. Verksamheten behöver därför även finna lämpligt sätt att informera de kontaktpersoner och andra hos klienten/kunden vars personuppgifter behandlas i verksamheten. Ett sätt kan vara att lämna över ett skriftligt dokument med information som klienten/kunden kan överlämna till berörda personer.

1.3.14 Behandling av särskilda kategorier av uppgifter och behandling av personnummer
När verksamheten 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 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).[3]

---

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 (mottagare anslutna till Privacy Shield gäller inte längre) Överföring av personuppgifter till tredjeländer eller territorier som anses ha en adekvat skyddsnivå kräver enligt artikel 45(1) inte något särskilt tillstånd.

[3] Prop. 2017/18:105

Ovanstående innebär att verksamheten 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 för advokatbyråer som har förordnats av Integritetsmyndigheten, 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. Integritetsmyndigheten behöver ge ut nya föreskrifter i anslutning till att dataskyddsförordningen och dataskyddslagen träder ikraft och Advokatsamfundet utgår från att Integritetsmyndigheten 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.

När det gäller nationella undantaget för sekretessbestämmelser så bör auktoriserade patentombud likt advokaterna omfattas av undantaget. Advokatsamfundet hänvisar till vägledande regler om god advokatsed (VRGA) där man hänvisar till egna undantag. Liknande bestämmelser anges för en god patentombudssed i BOLFS 2012:1 som där hänvisar till Patientföreningarnas riktlinjer. Anger föreningen liknande riktlinjer för detta så ska dessa likt för advokater gälla. Däremot omfattas inte varumärkesombud eller varumärkesassistenter av samma undantag.

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 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.

1.3.15 Telefon- och klientregister

Verksamheten är personuppgiftsansvarig för de register som förs hos sig. Det här gäller exempelvis för sedvanliga telefon- och klient/kundregister. För alla register som hålls inom ramen för patentbyråverksamheten måste patentbyrån 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 patentbyrån sätta en rimlig gallringstid och implementera en process som fungerar.

Eftersom klientregistret hos många patentbyråer utgör söknyckel till arkivet behöver informationen i klientregistret bevaras under hela arkiveringsskyldigheten. Klientregister är centrala för patentombudet för att kunna fullgöra den skyldighet av intressekonfliktskontroll som följer av 3 p BOLFS 2012:1.[4] En intressekonflikt innebär att ett patentombud i förekommande fall inte får anta sådant uppdrag. Likt advokatsamfundet behöver patentbyråer kunna arkivera sina ärenden under så lång tid som patentet är aktuellt, och i vart fall 10 år från att uppdraget slutfördes.

[4] Jfr 7.12.2 VRGA för advokater.

1.3.16 Patentombuds tystnadsplikt

Auktoriserade patentombuds tystnadsplikt och diskretionsplikt regleras i patentombudslagen och avser patenträttslig rådgivning. Enligt 6 § i lag (2010:1052) om auktorisation av patentombud har ett ombud tystnadsplikt inom ramen för sin verksamhet, eller vad denne fått kännedom i sin yrkesutövning.[5] Undantag från tystnadsplikten gäller enbart om uppdragsgivaren ger sitt samtycke till att informationen lämnas ut eller om det föreligger en laglig skyldighet för ombudet att lämna ut upplysningen. Tystnadsplikt i enlighet med god patentombudssed regleras i 6 p BOLFS 2012:1.

1.3.17 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. Om verksamheten 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.

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

- Enligt rådande praxis får patentbyråer arkivera ärenden i tio år från och med att de har upphört att gälla.
- Om patentbyrån 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 eller skattelagstiftningen) för att bevara visst underlag under viss tid ska detta beaktas.

[5] Jfr 2.2.1 VRGA

Bilaga 1 Exempel på registerförteckning

- Personuppgiftsansvarig verksamhet:

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

- Dataskyddsombud eller annan kontaktperson:

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

Bilaga 2 Exempel - Information till den registrerade[6]

[EXEMPEL]
Behandling av personuppgifter – information enligt Dataskyddsförordningen (2016/679/EG)

Verksamheten [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 jävskontroll.Vi behandlar uppgifterna för att genomföra obligatorisk jävskontroll, utföra och administrera uppdraget, för att tillvarata dina intressen, för redovisnings- och faktureringsändamål.

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 av att utveckla verksamheten och kommunicera med våra kontakter.

Personuppgifter kan komma att överföras mellan verksamhetens olika koncern- eller systerbolag i syfte att utföra jävskontroll, 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 verksamheten 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 ska 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 [verksamheten], 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 patentbyråns 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 [verksamheten] 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 Integritetsmyndigheten (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 SKA INFORMATION TILLHANDAHÅLLAS OM TILL VILKA LÄNDER ÖVERFÖRINGEN SKER OCH EN LÄNK TILL REGELVERK SOM GARANTERAR SKYDDET FÖR PERSONUPPGIFTERNA.]

[OM PATENTBYRÅN UTSETT ETT DATASKYDDSOMBUD SKA KONTAKTUPPGIFTER ANGES.]

[6] Nedanstående text är ett exempel avsett för vägledning. Exemplet är inte uttömmande och behöver anpassas för varje verksamhets enskilda verksamhet.

Kontakta oss på [E-POSTADRESS] eller adress nedan om du har några frågor rörande vår personuppgiftsbehandling. Personuppgiftsansvarig är Verksamheten [X], [ORG NR], [ADRESS], [POSTADRESS], [TELEFON], [WEBBADRESS], [E-POSTADRESS].

Bilaga 3 Exempel intern integritetspolicy[7]

[VERKSAMHETENS] POLICY FÖR BEHANDLING AV PERSONUPPGIFTER

Syfte

[Verksamheten] värnar om sina klienters, partners, kunders 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.

[Verksamheten] 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.

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 [verksamheten]. Vidare kan verksamheten 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.

Tillämpningsområde och omfattning

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

[Verksamhetens] 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.

[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].]

Grundläggande principer

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

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, 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

[7] 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.

med andra, hur länge personuppgifterna lagras och hur man kommer i kontakt med [verksamheten]. De registrerade ska alltså ges tydlig och transparent information om behandlingen av deras personuppgifter.

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.

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.

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.

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.

Principen om ansvarsskyldighet innebär att [verksamheten] måste kunna visa att dataskyddsförordningen efterlevs. Verksamheten 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 [verksamheten] ska kunna redovisa ett sådant register för tillsynsmyndigheten när så krävs.

Personuppgifter

Personuppgifter är alla uppgifter som avser en identifierad eller identifierbar fysisk person, och uppgifter 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.

All behandling av personuppgifter omfattas av dataskyddsförordningen och dess regler. Med *behandling* avses 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.

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.

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.

Rättslig grund för behandlingen av personuppgifter

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

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.

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.

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

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).

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).

Behandlingen är nödvändig för ändamål som rör [verksamheten] 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.

Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering

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 verksamheten 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.

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 säkerställs 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.

Överföring till tredje land

För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) gäller särskilda regler. Dataskyddsförordningen medför att alla EU:s medlemsstater samt EES-länderna anses ha ett likvärdigt skydd för personuppgifter och personlig integritet, och därför kan personuppgifter föras över fritt inom 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. Detta avser 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. Dessa överföringar behöver analyseras särskilt.

Konsekvensbedömning

[Verksamheten] har en särskild rutin på plats för att kunna identifiera och hantera särskilda integritetsrisker inom verksamheten, samt för strukturerad uppföljning. Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med vissa typer av behandlingar av uppgifter - exempelvis avseende särskilt känsliga uppgifter; behandling i särskilt stor omfattning; användning av ny teknik eller dylikt.

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.

Innan sådan personuppgiftsbehandling påbörjas ska [*xxx på företaget*] 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*].

Registerutdrag och utlämnande

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

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.

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.

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.

Den registrerade har rätt att överföra personuppgifter som denne lämnat till [verksamheten] 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 [verksamheten].

Den registrerade har i vissa fall rätt att kräva att [verksamheten] *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.

Den registrerade har rätt att *invända mot behandling* av personuppgifter som stöds på legitimt intresse som rättslig grund. Vid en invändning ska verksamheten upphöra med behandlingen om den 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.

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.

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.

Personuppgiftsincidenter

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.

Personuppgiftsincidenter ska 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.

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

Övrigt

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

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

Frågor

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

Policy antagen av [verksamhetens] styrelse den [] 2018.

Bilaga 4 Mall för konsekvensbedömning

KONSEKVENSBEDÖMNING AVSEENDE [ ] [EXEMPELVIS: BEHANDLING AV PERSONUPPGIFTER VID UTFÖRANDE AV UPPDRAG I

PATENTBYRÅN NN]

Bakgrund

[Mot bakgrund av [Patentbyråns upphandling av … för juridiska/tekniska bedömningar]

har verksamheten bedömt att en konsekvensbedömning enligt dataskyddsförordningen bör genomföras för den personuppgiftsbehandling som förekommer i anslutning med verktyget.]

Behovet av att genomföra en konsekvensbedömning

I verksamhetens 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.]

[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]

Synpunkter från, och samråd med, andra

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

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

Identifiering av risker

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

[Räkna upp och beskriv de risker som verksamheten identifierar]

Hantering av risker

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

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

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

[Beskrivning av åtgärdsplan.]

Bilaga 5 Mall för incidentrapport

Till Integritetsmyndigheten,

Med anledning av att det den [DATUM OCH TIDPUNKT] inträffat en personuppgiftsincident inom verksamheten 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

Verksamhetens kontaktperson är [ANGE KONTAKTPERSON OCH KONTAKTUPPGIFTER] Begäran om sekretess

Verksamheten begär att Integritetsmyndigheten sekretess-markerar anmälan.

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

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

1. Fördjupad information för en ansvarfull databehandling

1.1 Rättslig grund och principer för behandling av personuppgifter

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

Samtliga *grundläggande principer* enligt artikel 5 för behandling av personuppgifter måste följas:

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt – *transparensprincipen.*
b) Behandlingen ska vara förenlig med ändamålet – *ändamålsprincipe*n
c) Uppgifterna ska vara adekvata och relevanta – *principen om uppgiftsminimering*
d) Uppgifterna ska vara riktiga och uppdaterade – *principen om riktighet*
e) Uppgifterna ska inte förvaras under längre tid än nödvändigt – *princip om lagringsminimering*
f) Uppgifterna ska behandlas på ett sätt som säkerställer att de skyddas mot otillåten användning – *principen om integritet och konfidentialitet.*

De *rättsliga grunder* för personuppgiftsbehandling som godtas enligt artikel 6 är:

a) samtycke från den registrerade,
b) avtalssituationer,
c) rättslig förpliktelse som åvilar den personuppgiftsansvarige,
d) intresseavvägning,
e) skydd av livsviktiga intressen för den registrerade eller för en annan fysiskperson,
f) 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.

Den personuppgiftsansvarige är sedan tidigare personuppgiftslagstiftning (PUL) ansvarig för eventuella överträdelser, men måste i enlighet med GDPR även 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.

Dataskyddsförordningen gäller fullt ut för behandling av personuppgifter i ostrukturerat material, vilket blivit 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.

1.2 Laglig grund enligt artikel 6

I det följande följer därför en genomgång av de lagliga grunder och principer som kan aktualiseras i SEPAF:s medlemmars verksamhet.

1.2.1 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. Integritetsmyndigheten reglerar även villkor för att ett samtycke ska anses giltigt, se artikel 7 i dataskyddsförordningen. 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 patentbyråers behandling av personuppgifter.

Mycket av den behandling som utförs på en patentbyrå, t.ex. behandling av personuppgifter om motparter, kan en patentbyrå aldrig få samtycke till. En motpart skulle sannolikt aldrig lämna samtycke till en 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 patentbyrå 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.

1.2.2 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 vanlig avtalssituation för en verksamhet 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 förfarandet av klientkonton. Ett avtal mellan ett företag och en annan juridisk person innebär dock inte att företaget per automatik kan behandla personuppgifter om de som är anställda hos den juridiska personen. En alternativ laglig grund för behandling av dessa personuppgifter kan behövas.

1.2.3 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” 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 verksamheten 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.

1.2.4 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 för artikel 6 e nedan. Exempel på intressen som är av grundläggande betydelse för den registrerade är när behandlingen är nödvändig av t.ex. humanitära skäl (bl.a. för att övervaka epidemier och deras spridning; i humanitära nödsituationer, särskilt vid naturkatastrofer eller katastrofer orsakade av människan).

1.2.5 Behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning (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.[8] Den lagliga grunden måste emellertid i detta fall vara fastställd antingen i unionsrätten eller i den nationella (svenska) rätten, jfr punkten för artikel 6 c. 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 e i dataskyddsförordningen. I de fall där verksamheten själv blir personuppgiftsansvarig kan viss verksamhet vara av sådant allmänt intresse som här avses.

1.2.6 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

[8] Begreppet allmänt intresse är ett unionsrättsligt begrepp som inte definieras utförligt i dataskyddsförordningen och dess innebörd har ännu inte heller utvecklats av EU-domstolen 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.

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 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 ett företags 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.

1.2.7 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 en verksamhet 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 alla typer av verksamheter kan kortfattat beskrivas enligt följande:

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.

1.3 Den registrerades rättigheter

1.3.1 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).

1.3.2 Verksamhetens 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. Om uppgifterna samlas in direkt från den registrerade (d.v.s. en klient som är en privatperson) är patentbyrån enligt artikel 13 i dataskyddsförordningen skyldig att lämna nedanstående information till klienten om klientens personuppgifter behandlas.

Här följer en beskrivning av vad en informationstext i huvudsak behöver innehålla i patentbyråverksamhet:

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 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 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.[9]

Det undantag från informationsskyldighet som gäller om den registrerade redan förfogar över all information som ska lämnas (artikel 13.4) blir sällan tillämpligt i patentbyråverksamhet eftersom den registrerade sällan förfogar över all den information som ska lämnas. Informationsskyldigheten enligt dataskyddsförordningen är mer omfattande. Artikel 29-gruppen har publicerat en vägledning för information till registrerade.[10]

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 tydligt språk.

Informationen lämnas lämpligast i ett uppdragsbrev eller i ett formulär för antagande av uppdrag. Informationen kan sannolikt lämnas i en personuppgiftspolicy på företagets webbsida om patentbyrårepresentanten länkar till denna webbsida i sin uppdragsbekräftelse. Informationen bör inte lämnas som en del av företagets allmänna villkor eftersom det förmodligen innebär att tydlighetskravet inte är uppfyllt. Se det exempel som finns i bilaga 2.

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

Av artikel 15 i dataskyddsförordningen följer att den registrerade på begäran har rätt att av den personuppgiftsansvarige få bekräftat huruvida personuppgifter som rör honom eller henne behandlas och i så fall få tillgång till personuppgifterna 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.

[9] 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.
[10] Guidelines on transparency under Regulation 2016/679.

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, inbegripen 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).

1.3.4 Informationsskyldighet när uppgifter har erhållits från annan (artikel 14)
Ett generellt undantag från informationsskyldigheten, som blir av betydelse i patentbyråverksamhet, 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 patentbyrån bedömer om det finns förutsättningar för att väcka talan mot en motpart, och därvid behandlar personuppgifter avseende motparter, vittnen, eller personer som förekommer i datarummet. Om patentbyrån 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 patentbyråns klient överväger en talan. En sådan informationsskyldighet kommer i konflikt med auktoriserade patentombuds tystnadsplikt 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. Auktoriserade patentombuds tystnadsplikt enligt rättegångsbalken är en sådan tystnadsplikt som följer av artikel 14.5 (d) vilket innebär att artikel 14 inte är tillämplig i sådana situationer.

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 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 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.

1.3.5 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 ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller vägra att tillmötesgå begäran. Det är den personuppgiftsansvarige som har bevisbördan för att begäran är uppenbart ogrundad eller orimlig.

Som framgår ovan har patentbyrån 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. Ett undantag från skyldigheten i artikel 15 följer även av 5 kap 2 § dataskyddslagen.

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.

Begäran om rättelse (artikel 16)
Av artikel 16 dataskyddsförordningen följer att den registrerade har rätt att begära att felaktiga personuppgifter rättas. Bedömningen är att det inte föreligger någon skyldighet att automatiskt behöva rätta alla uppgifter i korrespondens, inlagor, yttranden, promemorior och andra dokument då skyldigheten att rätta uppgifter bedöms i förhållande till behandlingens ändamål enligt 5.1 d.

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 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.

1.3.7 Rätten att bli glömd (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 ett 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).

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.

Patentbyråer har ingen arkiveringsskyldighet. Däremot måste patentbyråer ha tillgång till akten för att kunna bemöta ett eventuellt anspråk som riktas mot ombudet med anledning av det utförda uppdraget. En annan orsak är att patentbyråer 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.

1.3.8 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 istället 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 patentbyråverksamhet. 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).

1.3.9 Anmälningsskyldighet om personuppgifter rättas, raderas eller när 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.

1.3.10 Dataportabilitet (artikel 20)
En behandling av klientens/kundens 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. Den registrerade ska vidare 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.

Rätten till dataportabilitet omfattar som nämnts bara personuppgifter, och bara personuppgifter om klienten/kunden själv (när klienten/kunden är en fysisk person) som denne själv har tillfört ärendet. Klienten/kunden 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 patentbyrå att tillmötesgå en begäran om dataportabilitet från en motpart. Behandlingen av dennes personuppgifter grundas inte på avtal med eller samtycke från motparten.

1.3.11 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, inbegripen 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 en konsekvensbedömning alltså kan behövas. 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 övervakning av anställdas IT-användning kan utgöra en högriskbehandling. Även införandet av eventuella AI-lösningar kan motivera en konsekvensbedömning. Av artikel 35.4 framgår att Integritetsmyndigheten ska publicera en lista på behandlingar som kräver konsekvensbedömning. Av artikel 35.5 framgår att Integritetsmyndigheten även har möjlighet att publicera en lista på behandlingar som inte kräver en konsekvensbedömning. Integritetsmyndigheten anger att en behandling som

”sannolikt leder till hög risk för fysiska personers rättigheter och friheter” ska automatiskt medföra konsekvensbedömning.

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 som finns 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.

1.3.12 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. 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. Ett dataskyddsombud ska också utses om den personuppgiftsansvariges eller personuppgiftsbiträdets 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.

I detta sammanhang är det viktigt att notera att om en verksamhet 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.

1.4 Personuppgiftsansvarig och personuppgiftsbiträde

1.4.1 Personuppgiftsansvar (artikel 24)

Med personuppgiftsansvarig avses den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Inom en verksamhet är det den juridiska personen, inte enskilda personer eller anställda på företaget, som är personuppgiftsansvarig för den behandling som förekommer i verksamheten. För personer som bedriver verksamheten under enskild firma är det personen 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 uppdrag förekommer behandling av personuppgifter i större eller mindre omfattning. Det handlar dels om behandlingar för administrativa ändamål (hantering av 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.

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. 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 från verksamhet till verksamhet och från 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 patentbyråuppdrag, 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”)
- Regelbunden översyn av åtgärderna och vid behov uppdatering av åtgärderna (artikel 24.1)

Principerna om *inbyggt dataskydd* och *dataskydd som standard* har vuxit 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” för 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 patentbyråns 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 ombud 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 ombud att gå in i ett ärende, exempelvis för att täcka upp vid sjukdom. Frågan om särskild behörighetsstyrning för ärenden behöver beaktas med hänsyn till byråns storlek och organisation och karaktären av känslighet på ärendena.

1.4.2 Anlitande av personuppgiftsbiträde (artikel 28)

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

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

1.4.3 Registerförteckning (artikel 30)

Som framgått ovan är det den juridiska personen 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 (patentbyrån) 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 Integritetsmyndigheten. Det är dock värt att påpeka att registret även fyller en utmärkt intern funktion för verksamheten 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 verksamheten 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. Verksamheten 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.

1.4.4 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 behandlingsystemen 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 verksamhetens 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 företags kommunikation sker genom e-post. Säkerhetsnivån i allmän e-post kommunikation är begränsad vilket innebär att det alltid finns en risk för att andra än den avsedda mottagaren kan ta del av meddelandet. Integritetsmyndighetens har i vart fall i två tillsynsbeslut 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 patentbyrå inte bör uppställa hinder som gör det svårt eller omöjligt för en klient att få tillgång till juridisk representation eller rådgivning.

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 epostkommunikation. 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.

1.5 Personuppgiftsincidenter

1.5.1 Anmälan av personuppgiftsincident till Integritetsmyndigheten (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.

Enligt artikel 33.1 ska en personuppgiftsincident anmälas till Integritetsmyndigheten utan onödigt dröjsmål och 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 Integritetsmyndigheten 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.[11]

1.5.2 Information om personuppgiftsincidenten till den registrerade (artikel 34)

Utöver skyldigheten att anmäla personuppgiftsincidenter till Integritetsmyndigheten 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 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:

1. Kryptering eller annan skyddsåtgärd har förhindrat åtkomst eller tillgång till personuppgifterna, eller
2. 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
3. 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 ett auktoriserat patentombuds skyldighet att iaktta tystnadsplikt och lojalt beakta klientens intressen. Detta är fallet om den registrerade som omfattas av incidenten är någon annan än patentbyråns klient, exempelvis en motpart. Dataskyddsförordningen innehåller inget undantag från informationsskyldigheten för det fall att behandlingen omfattas av lagreglerad tystnadsplikt. På

[11] Se Guidelines on Personal data breach notification under Regulation 2016/679.

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 ombudet skyldig att informera de registrerade om personuppgiftsincidenter, i den utsträckning som följer av dataskyddsförordningen.

Det bör observeras att Integritetsmyndigheten kan förelägga den personuppgiftsansvarige att informera de registrerade om att en personuppgiftsincident har inträffat (artikel 34.4). Integritetsmyndigheten 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.

1.6 Överföring av personuppgifter till tredjeländer eller internationella organisationer

1.6.1 Tredjelandsöverföringar

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 patentombudssekretessen 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 sekretessens 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 det auktoriserade patentombudet, i annan utsträckning än vad som följer av tvingande svensk rätt. För överföring av personuppgifter till länder utanför EU och EES (så kallad tredjelandsöverföring) 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).

(i) Överföring av personuppgifter till tredje land får enligt dataskyddsförordningen endast ske i följande situationer och under förutsättning att övriga regler i förordningen följs:
(ii) jurisdiktionen där mottagaren är belägen anses ha en adekvat nivå på skyddet av uppgifterna,

(iii) exporterande organisation (patentbyrån) vidtar lämpliga skyddsåtgärder för att skydda för personuppgifterna eller
(iv) något undantag är tillämpligt.

1.6.2 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 2 för en uppräkning av de beslut som för närvarande föreligger.

1.6.3 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). Efter ett godkännande av Privacy Shield avtalet mellan EU och USA ogiltigförklarade EU-domstolen avtalet som laglig grund för personuppgiftshantering.

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.

1.6.4 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.[12] 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 patentbyråverksamhet). 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.

Det kan noteras att globaliseringen och kraven på normal affärsverksamhet idag ställer stora krav på ombudens tillgänglighet och att tillgång i många situationer kan kräva resor även till tredje land. Tillgång till information i byråns egna system över e-post och med egen bärbar utrustning etc. kan därvid

[12] Se för detaljer artikel 49.1, första stycket samt skäl 111–112.

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 ombudet 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 bör ombudets egna tillgång till information i det läget inte betraktas som en överföring som kräver några ytterligare åtgärder.

1.7 Redogörelse för frågor

Mot bakgrund av det ovan redogjorda har frågor gällande den generella vägledningen samlats:

1.7.1 Är ombudskapet laglig grund för att lagra personuppgifter för klienter som är juridiska personer (personuppgiftsbiträde)?

Svar:
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.

För att besvara den här frågan gällande patentombud måste en analogi till Advokatsamfundets inställning göras. 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. 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.

1.7.2 Är ombudskapet laglig grund för att lagra personuppgifter för klienter som är fysiska personer (personuppgiftsansvarig)?

Svar:
Även i detta fall skulle den rättsliga grunden vara behandling för fullgörande av avtal. Frågan huruvida ombudet skulle vara personuppgiftsbiträde eller personuppgiftsansvarig beror på uppdragsförhållandet och vilken mängd personuppgifter som ska behandlas. Advokatbyråer har i praxis ansetts ha en självständig, beslutsfattande roll gällande vilken behandling som ska ske, vilket inneburit att de ansetts vara personuppgiftsansvariga. En analogi till detta bör kunna göras för patentombud.

1.7.3 Hur länge får vi spara personuppgifter i ärenden som inte längre är aktiva (jämför bokföringslagens åtta år)?

Svar:
Det är än så länge oklart, men vi bör kunna spara ärenden i tio år från och med att de har upphört att gälla, eller så länge som vi har en legitim anledning att behålla ärendena. Ett exempel på en sådan anledning kan vara varumärken som inte används aktivt av klienten men som tillhör en klient som fortfarande är aktiv, eller ingår i en aktiv portfölj.

1.7.4 Är ombudskapet laglig grund för att lagra uppgifter om motparter och i vilken utsträckning kan sådan lagring ske (tid efter intrång, relevans)?

Svar:
Det är än så länge oklart, men vi kan anta att ombudskapet ger laglig grund att hantera och lagra uppgifter om motparter, dock inte i högre utsträckning än vad som kan anses vara nödvändigt för att utföra uppdraget.

1.7.5 Gäller client-attorney-privilege över dataskyddsförordningen vad gäller motparts möjligheter att begära ut personuppgifter?

Svar:
För auktoriserade patentombud gäller lagstadgad sekretess, vilket gäller över dataskyddsförordningen (GDP