SVENSKT NÄRINGSLIV

Frågor och svar angående Dataskyddsförordningen och arbetsrätt

Förord

Denna sammanställning är ett resultat av ett gemensamt arbete utfört av en sektorgrupp inom Svenskt Näringsliv. Sektorgruppen har bestått av representanter från samtliga 12 sektorer inom Svenskt Näringsliv. Syftet är att söka besvara en mängd frågor som kommit in till de olika medlemsorganisationerna rörande dataskyddsförordningen, relaterat till arbetsrätt. Detta dokument har alltså inte ambitionen att besvara alla frågor, endast de som ställts till oss per datum för framtagande av detta dokument.

Svaren nedan är exempel på svar. Eftersom dataskyddsförordningen är ny och inte ens börjat tillämpas när denna sammanställning färdigställts ska svaren nyttjas med viss försiktighet. Nya riktlinjer förväntas komma fortlöpande varför det är viktigt att hålla sig uppdaterad. Dokumentet är indelad i 19 olika rubriker under vilka vi sorterat in frågor som hör till respektive rubrik. Frågorna är numrerade.

Den 25 maj 2018 upphör personuppgiftslagen (PUL) och ersätts med dataskyddsförordningen, dataskyddslagen och ett antal särskilda förordningar.

Mer vägledning kan fås av respektive medlemsorganisation samt från Datainspektionens hemsida www.datainspektionen.se

Innehåll

1. Allmänt

1.1. Är dataskyddsförordningen semidispositiv? Det vill säga, kan vi göra avsteg från den med stöd av kollektivavtal?

Enligt Dataskyddslagen 2 kap 3 § kan ett kollektivavtal utgöra rättslig grund för behandling av personuppgifter. Det vill säga ett kollektivavtal som innehåller bestämmelser om *när* en personuppgift får hanteras utgör rättslig grund för denna hantering. Däremot är det inte möjligt att göra inskränkningar i dataskyddsförordningens bestämmelser om skydd för den registrerade, det vill säga *hur* en hantering ska ske.

Det finns centrala kollektivavtal som har bestämmelser avseende integritetsfrågor i arbetslivet. Exempelvis kan det finnas en skyldighet för arbetsgivare att uppge särskilt angivna uppgifter vid MBL-förhandlingen innan införandet. Ett annat exempel är skyldighet att lämna kopia av anställningsbevis till facket vid nyanställning.

1.2. Vad är uppförandekoder och hur kommer de att påverka verksamheten?

En uppförandekod är riktlinjer som särskilt beskriver hur en viss verksamhet, bransch eller samhällssektor ska behandla personuppgifter i enlighet med förordningen. En uppförandekod ska förutom riktlinjer innehålla bestämmelser om hur efterlevnaden av uppförandekoden ska säkerställas.

En uppförandekod kan tas fram av en branschorganisation eller en annan organisation som företräder en viss kategori av personuppgiftsansvariga eller personuppgiftsbiträden för att visa hur man ska hantera personuppgifter i enlighet med bestämmelserna i dataskyddsförordningen. Uppförandekoden ska godkännas av Datainspektionen och bör tas fram i samråd med berörda intressenter, till exempel registrerade.

2. Dataskyddsförordningens tillämpningsområde

2.1. Omfattas personalmappar i pappersform av dataskyddsförordningen?

Om personuppgiften är helt eller delvis automatiserad är förordningen tillämplig. Även personuppgifter i manuella register omfattas av dataskyddförordningen.

Om informationen i fysiska personalmappar även finns i ett automatiserat system (exempelvis lagrad på en dator), så omfattas uppgifterna av dataskyddsförordningen.

Ska de fysiska personalmapparna läggas in i ett IT-system/scannas in/lagras på en server etc. så är uppgifterna delvis automatiserade och då omfattas uppgifterna av dataskyddsförordningen.

Fysiska personalmappar i register har tidigare ansetts falla inom personuppgiftslagens tillämpningsområde. Troligen är det samma bedömning för dataskyddsförordningen. En viss försiktighet bör tas och man bör därför ta det säkra före det osäkra och tillämpa dataskyddsförordningen.

För att det ska vara fråga om ett ”register” krävs:

- Att det är strukturerat – det vill säga sorterat enligt ett system.
- Att det är en samling av personuppgifter – det vill säga uppgifter om fler än en person som är tillgänglig enligt särskilda kriterier. Uppgifterna behöver inte vara samlade på samma ställe om det går att söka via centralt index. Samlingen ska ha en viss beständighet.
- Att uppgifterna är tillgängliga enligt särskilda kriterier, det vill säga sökbart på personuppgifter.

2.2. Är det behandling av personuppgifter om man scannar ett dokument och sparar i datorn, som bara jag har åtkomst till?

All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet räknas enligt dataskyddsförordningen som personuppgifter. Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter även om inga namn nämns. Krypterade uppgifter och olika slags elektroniska identiteter, som exempelvis IP-nummer, räknas som personuppgifter om de kan kopplas till fysiska personer.

Förordningen omfattar i princip all behandling av personuppgifter, det vill säga sådan behandling som sker i företag, i föreningar, inom myndigheter och av privatpersoner. Det finns dock undantag (artikel 2.2):

Dataskyddsförordningen ska inte tillämpas på behandling av personuppgifter i följande fall:

- Personuppgiftsbehandling som sker av en privatperson för rent personligt bruk.
- Personuppgiftsbehandling som sker i verksamhet som inte omfattas av EU-rätten (till exempel försvar och nationell säkerhet). Notera dock Dataskyddslagen 1 kap 2 och 3 §§ som preciserar dataskyddsförordningens tillämpningsområde inom detta område.
- Personuppgiftsbehandling som sker i brottsbekämpande verksamhet, som exempelvis polisen.

Dataskyddsförordningen tillämpas på all behandling av personuppgifter som utförs helt eller delvis med hjälp av datorer. Att förordningen även omfattar delvis automatiserad behandling innebär bland annat att den gäller redan när någon samlar in personuppgifter manuellt, exempelvis genom en pappersenkät, med syfte att senare registrera uppgifterna digitalt. Ett scannat dokument skickas vanligtvis till mail, vilket innebär att behandlingen är automatiserad.

Så om det scannade dokumentet sker av dig som privatperson för ett rent personligt bruk så faller det utanför dataskyddsförordningen.

Om det sker inom ramen för din tjänst i arbetslivet och det inskannade dokumentet innehåller en personuppgift så omfattas den av dataskyddsförordningen även om den enbart är för dina ögon.

2.3. Omfattas minnesanteckningar av dataskyddsförordningen?

Minnesanteckningar på datorn omfattas av dataskyddsförordningen då alla personuppgifter som sker genom en automatiserad behandling inkluderas i förordningen.

Handlar det om handskrivna minnesanteckningar så omfattas de av dataskyddsförordningen om de är sorterade i ett register. Läs mer om register i frågan ovan.

Om de inte är sorterade i ett manuellt register så omfattas inte minnesanteckningarna av dataskyddsförordningen. Exempelvis om det är en anteckningsbok utan innehållsförteckning eller sökflikar. En hög med papper på ett skrivbord anses inte vara ett register även om de är sorterade i bokstavsordning eller efternamn. Om emellertid ”högen” är beständig och inte bara tillfälligtvis sorterad kan den utgöra ett manuellt register.

I förslaget till Dataskyddslag, 5 kap § 2, anges att uppgifter i löpande text i form av minnesanteckningar inte måste lämnas ut enligt artikel 15 dataskyddsförordningen (prop. 2017/18:105 s. 107 f):

”Artikel 15 i EU:s dataskyddsförordning gäller inte personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande. Undantaget i första stycket gäller inte om personuppgifterna

1. har lämnats ut till tredje part,
2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål, eller
3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning.”

2.4. Om man hanterar personuppgifter i ett system, till exempel personalhanteringssystem, där leverantören säger att systemet följer dataskyddsförordningen, har arbetsgivaren då hamnat på ”säkra sidan” av ansvaret?

Den som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Med andra ord: de personuppgifter där ni bestämmer ändamålen med behandlingen och hur behandlingen ska gå till ansvarar ni för som personuppgiftsansvarig. På samma sätt är leverantör ansvarig för de personuppgifter som leverantör bestämmer ändamålen med och hur behandlingen ska gå till.

Biträdesavtal ska finnas mellan er och leverantören som behandlar era personuppgifter. Dataskyddsförordningen räknar upp vad ett biträdesavtal ska innehålla med bland annat detta; De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

Notera att såväl personuppgiftsansvarige som personuppgiftsbiträdet exempelvis kommer att bli skyldig att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsombud. Så i mångt och mycket måste ni båda uppfylla förordningens krav.

Rutiner bör uppställas för att granska de avtal som finns med olika leverantörer. Många avtal kan behöva kompletteras, inte minst vad gäller instruktioner till biträdet.

2.5 Får jag skicka en lönespecifikation via mail?

Uppgift om lön är inte en känslig personuppgift enligt artikel 9. Det är dock en integritetskänslig uppgift som enligt Datainspektionen har ett särskilt skyddsvärde. Utöver att en lönespecifikation kan innehålla uppgift om lön så kan det även innehålla uppgifter om sjuklön, vilket är en uppgift om hälsa och är därmed en känslig personuppgift enligt artikel 9.

Därför ska man som arbetsgivare vidta nödvändig säkerhet kring att lämna lönespecifikationer. Att skicka via mail utan något skydd är troligen inte ok. Det är därför lämpligt med exempelvis länk med personlig inloggning, lösenordsskydd etc. Många system för lönehantering erbjuder redan idag sådana lösningar. Ett alternativ är att ha någon form av plattform i vilken de anställda kan logga in på ett säkert sätt.

2.6 Får man skicka läkarintyg via mail från personalavdelningen till företagshälsovården?

En första förutsättning är att det finns en rättslig grund för att behandla läkarintyget och om det går att göra på annat sätt alternativt inte är nödvändigt, så ska arbetsgivaren inte skicka läkarintyg via mail.

I och med att läkarintyg innefattar känsliga uppgifter krävs att såväl artikel 6 som artikel 9 beaktas.

För att som arbetsgivare få skicka läkarintyg vidare så krävs det en rättslig grund enligt artikel 6. Beroende på situationen kan rätten att få behandla läkarintyget vila på olika rättsliga grunder.

Det kan till exempel vara fråga om arbetsgivarens rehabiliteringsansvar, vilket utgör en rättslig grund enligt Socialförsäkringsbalken och Arbetsmiljölagen.

Det kan även vara så att arbetstagaren begärt en ”second opinion” och vill ha arbetsgivarens hjälp med detta. I ett sådant fall kan även ett samtycke vara en

rättslig grund. Notera dock de särskilda krav som ställs på ett fullgott samtycke. (Artikel 7 och skäl 42 och 43).

Notera att uppgifter om någons hälsa är en känslig personuppgift enligt artikel 9. Det är enligt p 2 b tillåtet att hantera känsliga personuppgifter inom arbetsrätten.

Även om det är tillåtet att hantera uppgifterna bör inte känsliga personuppgifter skickas okrypterat via mail, då det troligen inte uppfyller krav på säkerhet enligt artikel 5 p.1 f.

2.7 Är det tillräckligt att en arbetsgivare, genom en policy, informerar om att arbetsgivaren kan komma att läsa arbetstagares privata mail utan att särskilt informera om detta vid varje tillfälle?

Regler för användningen av IT-system

Datorer och annan teknisk utrustning som arbetsgivaren ställer till de anställdas förfogande är arbetsredskap. Med stöd av arbetsledningsrätten har arbetsgivaren rätt att bestämma hur utrustningen på arbetsplatsen får användas. Arbetsgivaren ansvarar för organisationens informationssäkerhet och för att inga otillåtna behandlingar av personuppgifter utförs. Denne bör därför utarbeta regler och riktlinjer för användningen av datorer och datanät.

Arbetsgivaren har rätt att kontrollera om reglerna följs. Sådan kontroll av de anställda måste ha ett i förväg bestämt ändamål som är sakligt grundat i verksamheten. De anställda måste vara informerade om vilka regler som gäller, vilka kontroller som kan komma att utföras samt syftet med dessa. De anställdas intresse att få information kan förväntas vara särskilt starkt när det gäller vilka kontroller som de kan komma att utsättas för med hjälp av de insamlade uppgifterna. Information ska normalt lämnas självmant av arbetsgivaren innan uppgifterna samlas in men behöver inte lämnas vid varje enskilt kontrolltillfälle. Om arbetsgivarens ändamål exempelvis är att spåra och motverka oegentligheter och sabotage måste tydlig information lämnas till de registrerade, så att det klart framgår vad detta innebär och vilka kontroller som kan bli aktuella. Det kan inte förutsättas att den anställde känner till vad arbetsgivaren menar med ”oegentligheter” och ”missbruk”.

Arbetsgivaren har normalt sett inte rätt att läsa eller på annat sätt ta del av arbetstagarens privata e-post eller privata filer. Undantag kan gälla vid en allvarlig misstanke om illojalt eller brottsligt beteende eller en allvarlig misstanke om att den anställde använder IT-utrustningen i strid med arbetsgivarens regler och riktlinjer.

2.8 Telefonkontakter i arbetsgivarens mobiltelefon, både arbetsmässiga och privata, är det ett register? Är arbetsgivaren personuppgiftsansvarig för det registret? Räcker det med att det är ett anställningsförhållande för att få registrera i telefonen, eller krävs samtycke? Av de privata kontakterna? När blir de uppgifter som inte behövs, när behöver de gallras?

Datorer och annan teknisk utrustning som arbetsgivaren ställer till de anställdas förfogande är arbetsredskap. Med stöd av arbetsledningsrätten har arbetsgivaren rätt att bestämma hur utrustningen på arbetsplatsen får användas. Arbetsgivaren ansvarar för organisationens informationssäkerhet och för att inga otillåtna behandlingar av personuppgifter utförs. Denne bör därför utarbeta regler och riktlinjer för användningen av datorer och datanät.

Arbetsgivaren har rätt att kontrollera om reglerna följs. Sådan kontroll av de anställda måste ha ett i förväg bestämt ändamål som är sakligt grundat i verksamheten. De anställda måste vara informerade om vilka regler som gäller, vilka kontroller som kan komma att utföras samt syftet med dessa. De anställdas intresse att få information kan förväntas vara särskilt starkt när det gäller vilka kontroller som de kan komma att utsättas för med hjälp av de insamlade uppgifterna. Information ska normalt lämnas självmant av arbetsgivaren innan uppgifterna samlas in men behöver inte lämnas vid varje enskilt kontrolltillfälle. Om arbetsgivarens ändamål exempelvis är att spåra och motverka oegentligheter och sabotage måste tydlig information lämnas till de registrerade, så att det klart framgår vad detta innebär och vilka kontroller som kan bli aktuella. Det kan inte förutsättas att den anställde känner till vad arbetsgivaren menar med ”oegentligheter” och ”missbruk”.

Personuppgifter om kontakter (tredje person) i kontaktlistor m.m. kan normalt hanteras med stöd av intresseavvägning. Ett undantag från informationsplikten kan föreligga om dessa kan tänkas känna till att uppgifterna sparas i telefonboken eller dylikt, eller för att det skulle innebära en oproportionerlig ansträngning. I sådana fall kan information i stället lämnas i en generell integritetspolicy på företagets webbsida eller dylikt.

Svar från Datainspektionen 2018-04-04 gällande frågan att fackklubbarnas hantering av personuppgifter i mobiltelefoner och datorer som tillhör arbetsgivaren:

När det gäller personuppgiftsansvaret för behandlingar är frågan i grund och botten vem/vilka som bestämmer ändamål och medel för behandlingarna. Datainspektionen håller på att ta fram en mängd nytt informationsmaterial, och har inte hunnit färdigställa nytt material gällande frågan om att bedöma personuppgiftsansvar. Jag vill därför hänvisa till vad vi skrivit om personuppgiftsansvaret enligt personuppgiftslagen, se här:

https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/

Kan arbetsgivaren anses bestämma medlen för fackklubbens behandling och därmed bli PUA? Så har vi inte sett det tidigare och ingen förändring är avsedd på den punkten med den nya regleringen. Fackklubben bör därför kunna använda arbetsgivarens utrustning utan att arbetsgivaren av den anledningen blir PUA för fackklubbens behandling. Vilken dator som används är därmed oväsentligt i bedömningen av personuppgiftsansvaret. Som du skriver är fackklubben PUA för sina behandlingar.

2.9 Om en arbetstagare använder sig av fingeravtryck för inloggning i sin arbetstelefon, är arbetsgivaren då ansvarig för ett register för känsliga personuppgifter? Krävs någon särskild säkerhet då? En mobiltelefon är ju lätt att bli av med.

Om fingeravtrycket eller mätdata som framgår av fingeravtrycket sparas så är det troligen behandling av känsliga personuppgifter enligt dataskyddsförordningen. Det är troligt att mobiltelefontillverkaren eller teleoperatören inte överför uppgifterna från fingeravtrycket till sina servrar. Men behandlingen sker i en utrustning som ägs av arbetsgivaren.

En möjlig tolkning skulle vara att den anställde lämnar sitt samtycke när denne frivilligt (förutsätter att det inte är direkt eller indirekt krav från arbetsgivaren) registrerar sitt samtycke i telefonen. Men det är tveksamt om det uppfyller kraven på uttryckligt samtycke enligt artikel 9.2 a. En annan möjlig (och tveksam) tolkning är att (under förutsättning att det inte är ett direkt eller indirekt krav från arbetsgivaren) behandlingen faller under privatundantaget.

Apple har vid telefonkontakt i januari 2018 meddelat att fingeravtrycket inte sparas på sådant sätt att det kan återskapas. Det sparas, enligt Apple, således inte.

2.10. Kan man spara pärmar med anställningsavtal när dataskyddsförordningen trätt i kraft?

De omfattas av dataskyddsförordningen om det finns i register eller att det finns en koppling till ett datoriserat index.

De kan sparas om det finns en rättslig grund för detta och så länge som den är relevant. Uppgift om anställningstid kan och bör sparas så länge arbetstagaren är anställd men även därefter, eftersom en arbetstagare, som återanställs, har rätt att lägga samman all sin anställningstid hos arbetsgivaren vid upprättande av turordningslistor.

2.11. Vem äger ansvaret om en rekryteringsfirma skickar Cv:n till en rekryterare hos företaget?

Var och en svarar för sin personuppgiftsbehandling. Rekryteringsfirman måste ha stöd i både ändamål och rättslig grund för att skicka ett CV till en arbetsgivare. Det ligger naturligtvis i deras funktion att utföra en sådan behandling. När en arbetsgivare tar emot CV måste de på samma sätt ha ett ändamål, rättslig grund för hanteringen av personuppgifterna. Observera att det gäller andra krav på information till den registrerade när uppgifterna inte är insamlade från den registrerade själv (artikel 14).

2.12. Kan man lägga ansökningar från en rekryteringsprocess i en mapp som bara vi som jobbar med rekryteringen har tillgång till?

Enligt artikel 5.1 f ska personuppgifter behandlas på ett sätt som säkerställer lämplig säkerhet och i det ingår skydd mot obehörig eller otillåten behandling. (Integritet och konfidentialitet). Så svaret är att det förefaller vara en ändamålsenlig hantering.

Om det är fråga om fysiska mappar kan ifrågasättas om det ens faller in under förordningens tillämpningsområde.

2.13. Är vi som arbetsgivare skyldiga att säkerställa att anlitade konsulter (till exempel rekryteringsfirmor, företagshälsovård, försäkringsmäklare) hanterar anställdas personuppgifter i enlighet med dataskyddsförordningen?

Vid anlitande av konsulter måste det i varje enskilt fall göras en översyn av vem som är att se som personuppgiftsansvarig och vem som är att se som biträde. Den personuppgiftsansvarige ska endast anlita personuppgiftsbiträden som lämnar tillräckliga garantier, i synnerhet i fråga om sakkunskap, tillförlitlighet och resurser, för att genomföra tekniska och organisatoriska åtgärder som uppfyller kraven i förordningen (skäl 81).

Särskilt om företagshälsovård

Integritetskommittén har, mot bakgrund av ett antal beslut från Datainspektionen, beskrivit att när företagshälsovården behandlar personuppgifter inom ramen för hälso- och sjukvård är företagshälsovården personuppgiftsansvarig för den behandlingen av personuppgifter. Om företagshälsovården ges i uppdrag att hantera personuppgifter inom ramen för personaladministration är företagshälsovården dock personuppgiftsbiträde vid den behandlingen enligt kommittén (SOU 2016:41 s. 237).

Solidariska ansvaret

Huvudregeln är att det är den personuppgiftsansvarige som är skadeståndsansvarig för skada som uppstår till följd av att personuppgifter har behandlats i strid med förordningen. Ett personuppgiftsbiträde kan också bli skadeståndsansvarigt om denne har brutit mot de bestämmelser som specifikt riktar sig till biträden eller har behandlat uppgifter i strid med den ansvariges instruktioner. Den som lidit skada har i princip rätt att få ersättning för hela skadan av antingen den personuppgiftsansvarige eller personuppgiftsbiträdet. De får sedan i sin tur reglera detta sinsemellan. En personuppgiftsansvarig eller ett biträde har dock ingen skyldighet att betala ersättning om de kan visa att de inte på något sätt är ansvariga för skadan.

2.14. Hur hanterar vi överföringar av personuppgifter inom koncernen? Behöver vi träffa personuppgiftsbiträdesavtal mellan koncernbolagen?

Personuppgiftsansvaret kan placeras hos varje enskilt företag i en koncern, beroende på vem som i förordningens mening är att se som personuppgiftsansvarig. Det är de faktiska omständigheterna i det enskilda fallet som avgör vem som är personuppgiftsansvarig. Avtal där ansvaret preciseras kan ge vägledning vid bedömningen. Om två eller flera gemensamt bestämmer över en viss behandling är de personuppgiftsansvariga tillsammans enligt artikel 26.

En juridisk person eller en myndighet är personuppgiftsansvarig även om verksamheten bedrivs i filialer eller andra organisatoriska enheter. Om flera juridiska personer i en organisation (till exempel i en koncern) behöver behandla samma personuppgifter kan ansvarsfördelningen se ut på olika sätt.

Om moderbolaget ensamt bestämmer över behandlingen blir moderbolaget personuppgiftsansvarig. Om alla bolag inom en koncern gemensamt bestämmer över behandlingen blir de tillsammans ansvariga för det aktuella registret. De olika koncernbolagen kan naturligtvis samtidigt var för sig vara personuppgiftsansvariga för andra register som de självständigt bestämmer över.

För det fall ett koncernbolag anses vara personuppgiftsansvarig och något annat bolag behandlar uppgifterna för dennes räkning utgör det sistnämnda bolaget ett personuppgiftsbiträde. Det finns inget undantag för kravet på personuppgiftsbiträdesavtal i ett koncernförhållande varför ett sådant avtal ska upprättas.

Som stöd för överföring av personuppgifter mellan koncernbolag kan vad som anges i skäl 48 till förordningen tillämpas. Skäl 48 till förordningen anger att personuppgiftsansvariga som ingår i en koncern kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål, bland annat för behandling av kunders och anställdas personuppgifter.

2.15. Vissa arbetsgivare använder sig av så kallade incidentrapporteringssystem där arbetsgivaren möjliggör för arbetstagarna att skriftligen anmäla alla typer av förändringsönskemål/incidenter i företaget, alltifrån att stolar är osköna, att kaffeapparaten läcker till allvarligare arbetsmiljöproblem och diskriminering / sexuella trakasserier. Med vilken rättslig grund kan arbetsgivaren behandla personuppgifter som inkommer genom rapporteringssystemet? Olika rättsliga grunder beroende på innehåll i anmälan? Kan man hävda rättslig förpliktelse när det gäller arbetsmiljö/diskrimineringsfrågor även om anmälningar skulle kunna inhämtas på annat vis utan att personuppgifter behöver behandlas digitalt? Hur länge kan uppgifter i ett sådant system sparas?

Som frågan antyder skulle personuppgiftsbehandlingen i ett sådant system kunna vila på olika rättsliga grunder beroende på vad det är som rapporteras.

Det är möjligt att ett sådant inrapporteringssystem skulle vara genomförbart tillsammans med rutiner för en tät gallring. Vid en sådan gallring skulle en bedömning av personuppgiftsbehandlingen utifrån förordningen behöva göras och ett nytt ärende skulle kunna skapas därefter. Uppgifterna i inrapporteringssystemet skulle sedan behöva gallras.

Det kan även finnas anledning att fundera över hur rapporteringssystemet är uppbyggt och över instruktionerna kring vad som ska fyllas i. Flera fritextfält kan till exempel leda till att ”onödiga” personuppgifter lämnas.

2.16. Hur ska man hantera känsliga personuppgifter som avser medicinska underlag och rehab?

Huvudregeln i artikel 9.1 är att känsliga personuppgifter inte får behandlas. Av artikel 9.2 b framgår dock att det finns ett undantag från förbudet inom arbetsrätten. Av propositionen 2017/18:105 s. 78, Ny Dataskyddslag, framgår att det:

”…torde det stå klart att bestämmelsen i artikel 9.2 b gör det möjligt att behandla även känsliga personuppgifter när det är nödvändigt för att i vart fall arbetsgivare, arbetstagare, fackliga organisationer och arbetsgivarorganisationer ska kunna fullgöra sina skyldigheter eller utöva sina rättigheter med koppling till arbetslivet. Det är således inte bara behandling av personuppgifter som har sin rättsliga grund i arbetsrätten, i snäv bemärkelse, som omfattas. Bestämmelsen bör, precis som 16 § PUL, även kunna tillämpas vid behandling av personuppgifter som en arbetsgivare utför som en följd av lagstiftningen på socialförsäkringsområdet, till exempel i samband med en arbetstagares sjukdom och rehabilitering”

Det framhålls dock samtidigt i propositionen att det är fråga om unionsrätt, vilket gör att bedömningen kan komma att omprövas på unionsnivå.

2.17. Kopplingar mellan ändamål och rättslig grund för hantering av uppgifter inom arbetslivet.

För alla behandlingar av personuppgifter inom arbetslivet krävs att man gör en genomlysning av det laga stödet för behandling, enligt artikel 6, och även beaktar artikel 9 om det är fråga om behandling av känsliga personuppgifter.

En genomgång kan exempelvis se ut så här:

- Löneadministration – förpliktelse enligt avtal med den anställde (anställningsavtal)
- Sjuklön – rättslig förpliktelse
- Positioneringsteknik – intresseavvägning
- Medicinska uppgifter som ett led i rehabilitering – rättslig förpliktelse
- Kompetensdatabaser – intresseavvägning

Det är också viktigt att inte bara se till att det finns en rättslig grund för behandlingen. Det bör också vara tydligt hur information om behandlingen lämnas till de anställda, genom exempelvis policys eller personalhandbok.

I relation till uppgifter kring anställda finns också anledning att sätta upp tydliga gallringsrutiner. Det är viktigt att dessa beaktar alla olika aspekter på behandling av personuppgifter. Anledning till att spara personuppgifter kan finnas i allt från arbetsmiljöförordningen till upphovsrättslagen.

3. Dataskyddsombud

3.1. Vilka befattningar är aktuella som "dataskyddsansvarig" (utan att vara dataskyddsombud)?

Begreppet "dataskyddsansvarig" återfinns inte i förordningen. Om en personuppgiftsansvarig/personuppgiftsbiträde utser en dataskyddsansvarig utan avsikt att denne ska vara ett dataskyddsombud är det viktigt att detta tydligt framgår. För det fall ett dataskyddsombud utses öppnas en rättighetskatalog upp gentemot den personuppgiftsansvarige. Det är därför viktigt att vara tydlig med vad som avses vid tillsättandet av en dataskyddsansvarig.

Med anledning av att rollen "dataskyddsansvarig" inte återfinns i förordningen saknas även riktlinjer för lämplig befattning för en sådan roll. Det som kan sägas är att det inte är lämpligt att personer som skulle kunna komma att ges ett formellt juridiskt ansvar i frågor avseende bolagets behandling av personuppgifter, ges en sådan roll.

3.2. Rekryteringsprocessen

(Hela nedanstående kapitel kommer från Svenskt Näringslivs information "Personuppgiftslagen. Så berör den dig som företag" skriven av Christina Wainikka. Texten är anpassad till de förhållanden som gäller under dataskyddsförordningen)

Inledningsvis bör noteras att den så kallade missbruksregeln från Personuppgiftslagen inte gäller i och med att dataskyddsförordningen träder i kraft. Den innebar att behandling av personuppgifter som görs i ostrukturerat material, såsom löpande text i mejl eller mötesanteckningar inte omfattades av Personuppgiftslagen. Eftersom det undantaget försvinner innebär det att även behandling som görs i ostrukturerad form kräver lagligt stöd.

Arbetsgivaren är personuppgiftsansvarig för den behandling av personuppgifter som sker inom ramen för en rekryteringsprocess.

När ett företag rekryterar kommer det i kontakt med många personer. Genom hela rekryteringsprocessen måste företaget behandla personuppgifter. De kan handla om exempelvis namn och adress för de sökande.

För en del personer är rekryteringen den enda kontakt de har med företaget. En del av dessa personer blir en del av organisationen genom att de anställs. Det ställs olika krav på behandling av personuppgifter för de som blir anställda och de som inte blir anställda. Det kan därför vara bra att se på behandlingen av personuppgifter utifrån rekryteringsprocessens olika faser.

Svar på annons och spontanförfrågningar

Den första fasen i rekryteringsprocessen består ofta av att en person som är intresserad av anställningen hör av sig, per e-post, brev eller telefon. Denna kontakt kan ske på grund av att personen har sett en annons eller helt spontant. Det kan också vara så att någon tipsat personen om att höra av sig till företaget för en viss typ av anställning. I det här skedet har ofta inte någon tidigare kontakt funnits mellan personen och företaget.

En del företag väljer att hänvisa personen till att göra en formell ansökan. Företaget kan då välja att inte arkivera e-post eller brev eller att inte anteckna telefonsamtalet. I sådant fall har inga personuppgifter behandlats.

I en del fall väljer företaget att spara dessa första kontakter, med eventuella anteckningar. Det kan handla om korta anteckningar om namn, adress och vilken anställning den sökande är intresserad av. Dessa anteckningar innehåller personuppgifter och det kan vara nödvändigt att beakta dataskyddsförordningens regelverk. Om personuppgifterna antecknas på ett vanligt papper behöver inte dataskyddsförordningens hanteringsregler tillämpas.

Om personuppgifterna registreras i ett mer avancerat system, för att vara sökbara, blir dataskyddsförordningen hanteringsregler full ut tillämpbara. Personuppgifterna får registreras och de får också sparas, men bara så länge de är nödvändiga för ansökningsförfarandet och för att företaget ska kunna freda sig mot invändningar emot rekryteringsprocessen, till exempel påståenden om diskriminering. Därefter ska de gallras ut. Om företaget vill behålla uppgifterna för en längre tid, för att exempelvis användas vid en framtida rekrytering, krävs att den sökande lämnar samtycke.

Ansökan

I en del fall hanteras alla ansökningshandlingar i pappersform, då blir inte dataskyddsförordningen tillämplig.

I andra fall byggs register upp där de sökandes profil matchas på olika sätt. Tanken med registret är att underlätta gallringen och sådant register är särskilt vanligt när det är många sökanden. Den typen av hantering kräver att Dataförordningens regler följs.

Enligt hanteringsreglerna i dataskyddsförordningen får personuppgifter i ansökningarna registreras och sparas så länge det är nödvändigt.

Vad som är nödvändigt kan till exempel vara att företaget vill spara uppgifterna för att freda sig i de fall det blir en tvist om anställningsförfarandet har gått rätt till. En sökande som gallrats bort och inte fått anställning kan rikta krav mot företaget i form av skadestånd. Det kan till exempel vara fråga om en sökande som anser sig blivit diskriminerad. För att kunna hantera en sådan situation får företaget spara uppgifter från rekryteringsprocessen så länge som en sökande som inte anställts kan vidtaga rättsliga åtgärder. Det som kan avgöra tidsfristen är till exempel preskriptionsfrister. Vid diskriminering måste till exempel krav ställas mot företaget inom två år från den påtalade händelsen. Det är således möjligt att spara handlingar om rekryteringsprocessen så länge talan kan väckas och under den tid en rättslig prövning pågår.

Intervjuanteckningar

I samband med en rekryteringsprocess genomförs nästan alltid någon form av intervju. Vid intervjun görs ofta någon form av anteckningar. Dessa anteckningar kan, beroende på intervjuarens personlighet, vara tämligen ingående och personliga.

För de fall att anteckningarna systematiseras och registreras för att vara sökbara blir dataskyddsförordningen tillämplig. Anteckningarna får registreras och sparas så länge det är nödvändigt för ansökningsförfarandet. Precis som för ansökningarna gäller att de får sparas så länge som sökanden kan vidtaga rättsliga åtgärder, men

därefter ska uppgifterna gallras bort. Om företaget vill spara uppgifterna för att exempelvis använda vid framtida rekrytering krävs den sökandes samtycke (se vidare om kraven på ett fullgott samtycke). Det kan finnas anledning att spara anteckningarna, precis som själva ansökan, för att kunna bemöta rättsliga anspråk.

Referenser

I samband med rekrytering inhämtas ofta referenser från olika håll. Inhämtningen av referenser kan innebära behandling av personuppgifter inte bara om den sökande utan även om den som lämnat referensen.

För det fall att referenserna registreras och sparas, inom ramen för exempelvis en rekryteringsdatabas, krävs att dataskyddsförordningens hanteringsregler beaktas. Inom ramen för vad som är nödvändigt för ansökningsförfarandet får uppgifter från dem som lämnat referenser registreras och sparas. När det inte längre är nödvändigt ska de gallras bort. För det fall att företaget vill spara uppgifterna längre krävs samtycke från de som berörs.

Känsliga uppgifter

I samband med en rekrytering kan ibland känsliga uppgifter komma fram. Det kan till exempel gälla uppgifter om den sökandes hälsostatus. Behandling av känsliga uppgifter kräver särskild nogsamhet.

Generellt kan sägas att det är viktigt vid behandlingen av känsliga uppgifter att dessa inte kränker den som uppgifterna rör. Kränkande behandling är inte tillåten. Bedömningen av om en behandling är kränkande sker genom en samlad bedömning. I bedömningen görs en avvägning mellan hur känsliga uppgifterna är, i vilket sammanhang de förekommer, vilken spridning de fått eller riskerar att få. Det vägs också in vilket syfte som är bakom behandlingen av uppgifterna och vad behandlingen ska leda till. Bedömningen kan alltså ses som en avvägning i varje enskilt fall där personens behov av en fredad sfär vägs mot andra motstående intressen.

Lagöverträdelser

Om ett registerutdrag från belastningsregistret finns med som ett dokument i rekryteringsprocessen måste detta hanteras i enlighet med reglerna i artikel 10 i dataskyddsförordningen. Vid rekrytering kan ett sådant registerutdrag begäras för påseende. Det är dock inte tillåtet för arbetsgivaren att spara och registrera det om det inte finns rättsligt stöd för det.

När det gäller personal som ska arbeta med barn finns en särskild lag: Lag (2013:852) om registerkontroll. Enligt 1 § finns ett krav på att registerutdrag ska lämnas. Enligt 5 § får inte registerutdrag dokumenteras på annat sätt än genom en anteckning om att utdrag har visats. Detta synsätt kan gärna appliceras även för annan hantering av registerutdrag ur belastningsregistret.

Information till den registrerade

Enligt dataskyddsförordningen ska behandlingen av personuppgifter ske på ett öppet och transparant sätt i förhållande till den registrerade. Enligt artikel 12 har således den registrerade rätt att få information om personuppgiftsbehandling gällande den registrerade. Denna information ska, enligt artikel 12, ges i ett klart och tydligt språk och skriftligt, eller i någon annan form inbegripet, när så är lämpligt, i elektronisk form.

4. Drogtester

4.1. Hur ska resultatet av en genomförd drogtest hanteras?

En arbetsgivare får inte beordra ett drogtest av en anställd om detta skulle stå i strid med lag eller god sed på arbetsmarknaden.

Resultatet av ett sådant drogtest kan utgöra en känslig personuppgift enligt dataskydds-förordningen, särskilt om ett sådant test har givit positivt utslag. Detta innebär att de grundläggande principerna ska följas och att det ska finnas en rättslig grund för behandlingen.

Av artikel 35.3 b framgår att en konsekvensbedömning ska göras om man behandlar känsliga personuppgifter i stor omfattning.

Det är dock ingen uttömmande uppräkning av när konsekvensbedömning behövs och därför har 29-gruppen tagit fram en lista av kriterier som kan medföra att en sådan bedömning måste göras. Bland de kriterierna finns dels att det är fråga om känsliga uppgifter, dels att det är fråga om situationer där det råder en obalans mellan personuppgiftsansvarig och registrerad, till exempel i ett anställningsförhållande. Det finns också en mängd andra kriterier. 29-gruppen har sagt att om åtminstone två av dessa kriterier är uppfyllda bör en konsekvensbedömning göras.

Länk till Datainspektionen för mer info om konsekvensbedömning:

https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/skyldigheter-for-de-som-behandlar-personuppgifter/konsekvensbedomningar-och-forhandssamrad/vem-maste-gora-en-konsekvensbedomning/

5. Positioneringsteknik och inpasseringssystem

Allmänt

Det har blivit vanligare att arbetsgivare använder olika former av positioneringssystem för att kontrollera var fordon och anställda befinner sig. När sådana system används innebär det vanligen någon form av behandling av personuppgifter.

Även om positioneringssystemet endast möjliggör positionering av ett fordon eller en mobiltelefon går det ofta att koppla fordonet eller mobiltelefonen till en viss individ. En sådan indirekt koppling är tillräcklig för att dataskyddsförordningen ska vara tillämplig.

I relationen arbetsgivare – arbetstagare är det ofta inte möjligt att stödja sig på ett samtycke för behandlingen av personuppgifter, utan den rättsliga grunden är normalt en intresseavvägning. Arbetsgivarens intresse av att utföra behandlingen måste då väga tyngre än de anställdas intresse av skydd mot intrång i den personliga integriteten. Vid den helhetsbedömning som ska göras i dessa fall bör bland annat följande faktorer vägas in:

- Ändamålen med behandlingen
- Hur uppgifterna hanteras och hur resultatet används
- Vilken information som ges till de anställda
- Om behandlingen kan utföras på ett mindre integritetskänsligt sätt
- Vilken teknisk och administrativ säkerhet som finns för uppgifterna
- Förekomsten av fackliga överenskommelser och innehållet i dessa
- Om behandlingen följer god sed på arbetsmarknaden

Samtycke kan emellertid vara möjligt att använda sig av om arbetstagaren har valt positioneringstekniken efter att ha erbjudits ett fullgott alternativ, som till exempel manuell körjournal.

Notera att det kan krävas primärförhandling enligt Medbestämmandelagen att införa positioneringssystem och att informationen som behandlas kan utgöra känsliga personuppgifter enligt artikel 9 som kräver särskilda förutsättningar för att få behandlas.

Om positioneringssystemet köps som en tjänst av en utomstående leverantör kan denne agera som Personuppgiftsbiträde. Då krävs ett Personuppgiftsbiträdesavtal som ska ha ett visst innehåll som är reglerat i dataskyddsförordningen. Arbetsgivaren utgör i ett sådant fall Personuppgiftsansvarig.

Notera även:

- Att personalens säkerhet är ett vanligt ändamål för behandling liksom att kunna fastställa om bilen används privat eller i tjänsten
- Att ändamålen ska vara förenliga med god sed på arbetsmarknaden
- Att de kontroller som kan bli aktuella ska preciseras

- Att ge en tydlig information till de anställda. Information om att övervakning sker bör vara synlig i fordon
- Att arbetsgivaren är skyldig att föra behandlingshistorik, det vill säga loggning av de åtgärder som vidtas med personuppgifterna
- Att skapa en rutin om stickprovskontroll av behandlingshistoriken
- Att göra en konsekvensbedömning

5.1. Vi har ett inpasseringssystem till våra lokaler som vi köpt in av leverantör X – vilka uppgifter om våra anställda får vi skicka till X? Vad bör vi i övrigt tänka på i denna situation?

Om leverantören är personuppgiftsbiträde regleras relationen arbetsgivare – leverantör i Personuppgiftsbiträdesavtalet. Detta avtal behöver kompletteras med instruktioner kring den konkreta behandlingen av personuppgifter. Arbetsgivaren loggar uppgifter om sina anställda vanligen med stöd av en intresseavvägning. Arbetsgivarens rättsliga grund är samma för överföringen till personuppgiftsbiträdet.

Ändamålet styr vilka uppgifter som får behandlas. Den grundläggande principen om uppgiftsminimering ska iakttas.

Om leverantör X inte är ett personuppgiftsbiträde, blir X att betrakta som personuppgiftsansvarig.

Se till att tillämpa behörighetsbegränsning så att bara behöriga personer har tillgång till informationen.

5.2. Hur ska våra medlemsföretag med "företagskonton" på till exempel Facebook tänka när det gäller den användningen i förhållande till dataskyddsförordningen?

Datainspektionens faktablad Personuppgifter i sociala medier (Avser Personuppgiftslagen men torde vara relevant även avseende dataskyddsförordningen).

- Missbruksregeln försvinner, samtliga regler gäller – hur stor påverkan får det? Troligen måste företaget söka stöd för hanteringen i en intresseavvägning.
- Företaget har ett ansvar för de uppgifter som företaget själva publicerar.
- En omständighet som medför att organisationen blir personuppgiftsansvarig är om organisationen har möjlighet att ta bort användares publiceringar. Det kan också ha betydelse om organisationen har möjlighet att stänga av kommentarsfunktionen, samt om det är organisationen själv som tillhandahåller det sociala mediet.
- Facebook, Youtube, Instagram, Linkedin, Google Plus, Flickr, Pinterest och bloggar: Organisationen är ansvarig för personuppgifter som publiceras på organisationens profil. Ansvaret omfattar både personuppgifter som organisationen själv publicerar och personuppgifter som publiceras av andra, i till exempel en kommentar på profilen. Observera att även den användare som skrivit en kommentar kan ha ett ansvar för vad den själv skrivit.
- Twitter: Organisationen ansvarar endast för personuppgifter som organisationen själv publicerat, inte personuppgifter som andra twittrande lämnar. Det beror på att organisationen inte kan påverka publiceringen av andras inlägg på Twitter.

- Observera att en organisations ansvar för personuppgifter som publiceras i ett visst socialt medium alltså är beroende av utformningen av den sociala medietjänst som används. Förändringar av tjänsten kan därför leda till att en organisations ansvar förändras.

I organisationer där det finns en förväntan att anställda är aktiva i eget namn, men kopplat till tjänsten, bör de anställda få tydlig information kring de rättsliga reglerna som gäller för olika typer av publiceringar. I en hel del fall kan det handla om ett personligt ansvar och det bör de anställda i så fall vara medvetna om.

5.3. Vilka krav kan och bör våra medlemsföretag ställa på leverantörer av IT-system exempelvis lönesystem?

Ni bör kontrollera att leverantören uppfyller relevanta krav i dataskyddsförordningen. Det är den som är personuppgiftsansvarig som har ansvaret för att systemet lever upp till kraven.

Ni bör, i upphandlingen, ställa krav på leverantören att systemet är kompatibelt med dataskyddsförordningen. Därefter ska företaget säkerställa att leverantören faktiskt lever upp till kraven och se till att leverantören ställer garantier om det, se artikel 28.1. Detta kan ske genom att det skrivs in i personuppgiftsbiträdesavtalet om det är en personuppgifts-relation, eller på annat sätt skriftligen.

Datainspektionens hemsida har listat några punkter angående privacy by design som man kan utgå ifrån i diskussionen om systemet uppfyller kraven.

- Minimera mängden personuppgifter
- Begränsa åtkomsten till personuppgifter
- Skydda uppgifterna
- Låt systemet styra användaren rätt

Detaljerad information om de olika punkterna finns på Datainspektionens hemsida:

www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/

5.4. Räknas uppgifter om lön som en känslig personuppgift?

Uppgifter om lön räknas inte som en känslig personuppgift, eller vad som i dataskydds-förordningen kallas ”särskilda kategorier av personuppgifter” (Artikel 9). Däremot har Datainspektionen tidigare uttalat, när det gäller Personuppgiftslagen, att löne-uppgifter har ett skyddsvärde ur integritetssynpunkt, varvid särskild försiktighet trots allt ska iakttas vid behandling av löneuppgifter. Det finns anledning anta att samma förhållningssätt bör iakttas även efter det att dataskyddsförordningen trätt i kraft.

Uppgifter om lön kan i anställningsförhållande förekomma i flertalet olika dokument, exempelvis i anställningsavtal, lönelistor vid förhandlingar med fackföreningar inom ramen för lönerevision, i kontakter med Skatteverket och Försäkringskassan m.m. Hantering av lönespecifikationer inbegriper vanligtvis hantering av känsliga person-uppgifter, såsom sjukfrånvaro, vilket är viktigt att ha i åtanke vid bestämmande av rättslig grund, säkerhetsåtgärder m.m.

5.5. Vilken rättslig grund ska man använda då man till exempel anmäler anställda till kurser?

Svaret på frågan beror på vilken typ av kurs det rör sig om, vilken verksamhet arbetsgivaren bedriver och hur anställningsförhållandet mellan parterna ser ut.

Att anmäla anställda till kurser kan utgöra en skyldighet och rättighet för arbetsgivaren enligt anställningsavtalet, varvid den rättsliga grunden – fullgöra avtal – används. En arbetsgivare kan i stor utsträckning grunda personuppgiftsbehandling för fortbildning av personal på denna rättsliga grund.

Vissa arbetsgivare kan ha rättsliga skyldigheter att skicka anställda på kurser, exempelvis av säkerhetsskäl enligt viss arbetsmiljölagstiftning. Även vissa kollektivavtal föreskriver skyldigheter för arbetsgivare att sända anställda för utbildning inom specifika områden. Den rättsliga grunden – fullgöra rättslig förpliktelse – kan användas vid lagliga skyldigheter, och sannolikt även för kollektivavtalade skyldigheter då den svenska dataskyddslagen, så som förslaget ser ut idag, inbegriper kollektivavtal som en rättslig skyldighet.

Om ingen av de ovanstående rättsliga grunderna är tillämpliga i det enskilda fallet kan eventuellt samtycke användas som rättslig grund. Det måste i sådant fall finnas ett alternativ till samtycket för att det ska anses frivilligt. Vidare måste arbetsgivaren vid frågan tillse att samtycket uppfyller dataskyddsförordningens krav, det vill säga att arbetstagaren ska ha fått upplysning om ändamålet med behandlingen, informerats om att samtycket kan återkallas m.m.

Kursarrangören kan många gånger bli att betrakta som personuppgiftsansvarig för behandlingen av deltagarnas personuppgifter. Information om behandlingen som sker hos kursarrangören ska således lämnas av dem.

5.6. Kommer man vara tvungen att informera anställda om att man gör en ny slags personuppgiftsbehandling så snart man till exempel anmäler någon till en kurs, bokar hotellrum i hans/hennes namn och så vidare?

Enligt dataskyddsförordningen ska den personuppgiftsansvarige lämna information till den anställde då personuppgifterna samlas in. Olika regler gäller beroende på om personuppgifterna inhämtas från arbetstagaren själv eller från annat håll (se artiklarna 12–14). Eftersom många personuppgifter samlas in vid anställningens ingående, och arbetsgivaren i det läget kan förutse huvuddelen av de personuppgiftsbehandlingar som kommer att företas under arbetstagarens tid i företaget, kan information lämnas vid denna tidpunkt. Arbetsgivaren kan alltså lista de personuppgifter som kommer att behandlas, för vilka ändamål och med vilka rättsliga grunder. Datainspektionen har förklarat att behandlingar som naturligt hör till ändamålet anses inbegripna i den information som lämnas. Endast om personuppgifterna ska behandlas för ett annat syfte än för vilket de insamlades, behöver ny information lämnas (jfr artikel 13.3).

Information om arbetsgivarens behandling av personuppgifter kan med fördel lämnas på samma sätt som arbetsgivaren lämnar liknande information. Detta varierar mellan olika organisationer och kan ske exempelvis genom personalhandbok eller liknande.

5.7. Är reglerna om dataportabilitet relevanta i ett anställningsförhållande?

Dataportabilitet blir i regel inte tillämpligt inom arbetslivet. Rätten till dataportabilitet gäller registrerade som har tillhandahållit personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format, till en personuppgiftsansvarig. Behandlingen måste grunda sig på samtycke eller på ett avtal som den registrerade är part i.

Artikel 29-gruppen har i sina riktlinjer om rätten till dataportabilitet angett följande;

”När det gäller anställdas uppgifter gäller rätten till dataportabilitet endast om behandlingen grundas på ett avtal som den registrerade är part i. I många fall anses inte samtycke ha getts frivilligt i detta sammanhang, på grund av maktobalansen mellan arbetsgivare och anställd. Viss behandling av anställdas personuppgifter grundas i stället på den rättsliga grunden berättigat intresse, eller är nödvändig för att fullgöra specifika rättsliga förpliktelser på sysselsättningsområdet. I praktiken berör rätten till dataportabilitet av anställdas personuppgifter viss behandling (till exempel lön och ersättningar, intern rekrytering), men i många andra situationer måste man från fall till fall bedöma huruvida alla villkor för att tillämpa rätten till dataportabilitet är uppfyllda.”

Syftet är att stödja det fria flödet av personuppgifter i EU och främja konkurrensen mellan personuppgiftsansvariga. Det ska göra det lättare att byta tjänsteleverantör och kommer därför att gynna utvecklingen av nya tjänster inom den digitala inre marknaden (se vidare artikel 29-gruppens ”Riktlinjer om rätten till dataportabilitet”).

Typiska exempel på uppgifter som registrerade kan utnyttja dataportabilitet för är telefonregister innefattandes inkommande och utgående samtal, bankkontohistorik, e-postmeddelanden i en webbmejltjänst, titlar på böcker som en person har köpt från en nätbokhandel eller låtar som han eller hon har lyssnat på via en musikströmningstjänst.

5.8. Hur ska vi som företag behandla personlig dokumentation såsom läkarintyg och annan dokumentation i en rehabiliteringsprocess för att det ska vara ok enligt dataskyddsförordningen?

Läkarintyg och andra uppgifter hänförliga till en rehabiliteringsprocess omfattar i regel känsliga personuppgifter, varvid särskild försiktighet måste iakttas.

En av principerna i dataskyddsförordningen – privacy by design – innebär att personuppgiftsansvariga ska ha inbyggda mekanismer i sina IT-system för att skydda registrerades personliga integritet. En grundläggande princip inom integritetsskydd är att inte samla in mer information än vad som behövs, att inte ha den kvar längre än man behöver och inte använda den till något annat syfte än vad man samlade in den för.

Utöver uppgiftsminimering bör den personuppgiftsansvarige begränsa åtkomsten till uppgifterna så att endast de som behöver dessa för att utföra sina arbetsuppgifter har tillgång. Begränsningen kan ske genom såväl organisatoriska som tekniska åtgärder.

IT-system, särskilt sådana som innehåller känsliga personuppgifter, bör även ha nödvändiga säkerhetsfunktioner för att motstå olika typer av angrepp. Därutöver bör kryptering användas om känsliga personuppgifter överförs via Internet eller genom databaser osv. Datainspektionen har, när det gäller personuppgiftslagen, tagit fram en checklista för att arbeta med inbyggd integritet (se https://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/).

Den rättsliga grunden för behandling av ovannämnda personuppgifter är som huvudregel – att fullgöra en rättslig förpliktelse. Arbetsgivare har enligt arbetsmiljölagstiftningen ett långtgående rehabiliteringsansvar. Dessutom måste arbetsgivare betala sjuklön enligt sjuklönelagen, varvid läkarintyg behövs till grund för bedömningen i många fall.

Ovannämnda personuppgifter bör sparas under hela anställningen och den tid därefter som blir aktuell för att försvara rättsliga anspråk. Har arbetsgivaren ensidigt avslutat anställningen av skäl hänförliga till läkarintyg och rehabilitering kan arbetstagaren driva en tvist om ogiltig uppsägning/avsked och/eller skadestånd. Arbetstagaren skulle även kunna inleda en rättslig process med påståenden om att arbetsgivaren inte har fullgjort sitt rehabiliteringsansvar, varvid uppgifterna behöver sparas för att försvara sig i den frågan.

6. Anhöriga

6.1. Närmaste anhörig-uppgifter? Vilka uppgifter får vi ta in? Vilken är den rättsliga grunden?

En av grundreglerna i dataskyddsförordningen är att inte samla in mer personuppgifter än vad som är nödvändigt för ändamålet. Av den anledningen bör arbetsgivare se över hur s k anhörigblanketter är utformade. Vilken relation arbetstagaren och den anhörige har, exempelvis registrerat partnerskap som i sig avslöjar en känslig personuppgift nämligen sexuell läggning, är i regel ingen uppgift som är nödvändig för ändamålet.

Arbetsgivare som samlar in kontaktuppgifter till anhöriga har i regel som syfte att kontakta en nära anhörig vid olycksfall eller svår sjukdom för att informera den anhörige om situationen och för att söka stöd för den anställde. För att uppfylla detta ändamål torde endast namn och telefonnummer vara nödvändigt. Arbetsgivare får göra en bedömning av nödvändiga personuppgifter i varje enskilt fall.

Arbetsgivare har ofta ett starkt intresse av att kunna kontakta anhöriga vid exempelvis olycksfall eller sjukdom. Arbetsgivarens intresse av att från sina anställda samla in och registrera anhörigas namn och kontaktuppgifter väger över de registrerades intresse av att uppgifterna inte behandlas. Behandlingen kan ske efter en intresseavvägning och samtycke behöver alltså inte inhämtas från de anhöriga.

Personuppgifter som behandlas måste vara riktiga och aktuella, därför bör arbetsgivaren ha rutiner för att uppdatera uppgifterna. Det kan ske genom att vid återkommande tillfällen se till att uppgifterna uppdateras, till exempel genom att ställa fråga till de anställda om uppgifterna är aktuella eller låta de anställda själva ändra kontaktinformationen.

Arbetsgivaren har en informationsskyldighet gentemot de anhöriga och bör skapa rutiner för att lämna information om personuppgiftsbehandlingen till de anhöriga. Arbetsgivaren kan exempelvis skapa en informationsblankett till den anställde för att överlämna till sin/sina anhöriga. Datainspektionen säger att behandling av namn och telefonnummer, som kan hittas på internet, i regel inte behöver informeras om.

Som vid all behandling av personuppgifter måste arbetsgivaren se till att inte fler anställda får tillgång till personuppgifterna än nödvändigt. Arbetsgivaren bör därför begränsa åtkomsten till anhöriguppgifterna så att endast befattningshavare som ansvarar för eventuell kontakt med anhöriga har tillgång till uppgifterna.

7. Bilder

7.1. Får man lägga upp bilder från personalfesten på intranätet utan samtycke?

För att få publicera bilder på anställda på Internet krävs normalt samtycke, men beroende på vilken verksamhet arbetsgivaren bedriver kan det vara tillåtet att publicera bilder efter en intresseavvägning. Det kan således vara tillåtet att publicera bilder på anställda om behandlingen är nödvändig för ändamål som rör arbetsgivarens berättigade intressen, om inte den anställdes intressen väger tyngre och kräver skydd av personuppgifter. Verksamheten kan vara av sådan art att arbetsgivaren har ett klart behov av att exempelvis kunna marknadsföra sina produkter och tjänster genom att publicera bilder på anställda som har kundorienterade arbetsuppgifter. Arbetsgivarens intresse av att publicera bilderna kan då väga tyngre än den anställdes intresse av skydd för sin personliga integritet. Om arbetstagaren invänder mot personuppgiftsbehandlingen behöver arbetsgivaren visa på tvingande berättigade skäl som väger tyngre än arbetstagarens intressen (se artikel 21.1).

Att lägga upp bilder från personalfesten på intranätet kan troligen inte anses utgöra ett klart behov hos arbetsgivaren som väger över arbetstagarens intresse att skydda sina personuppgifter. För sådan publicering krävs således samtycke.

Om arbetsgivaren endast kan använda samtycke som grund för behandlingen kan samtycket förstås återkallas varvid bildhanteringen måste upphöra. Om arbetsgivaren behandlar bilder med stöd av en intresseavvägning och den enskilde invänder mot behandlingen får arbetsgivaren endast fortsätta med bildhanteringen om det går att visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

8. Facket

8.1. Är det tillåtet enligt dataskyddsförordningen att hantera uppgift om medlemskap i fackförening?

Uppgift om medlemskap i fackförening utgör en känslig personuppgift enligt artikel 9 dataskyddsförordningen. Sådan behandling kan vara tillåten enligt exempelvis artikel 9.2 b om arbetsgivaren måste ”utöva sina särskilda rättigheter inom arbetsrätten”, om det tillåts enligt nationell rätt eller kollektivavtal. Så det finns en rätt att hantera uppgifter om fackligt medlemskap men när det gäller gallring får man anta att huvudregeln är att uppgifter om fackligt medlemskap inte ska sparas för framtida behandlingar. Flera tänkbara undantag kan dock finnas, till exempel flera likartade behandlingar som sker med korta jämna intervall, till exempel avdrag för avgift för fackligt medlemskap. Eftersom detta är en uppgift som kan ändras är det också viktigt att säkerställa att uppgifterna är korrekta, se även kraven på korrekthet enligt artikel 5.1 d.

8.2. Är facket personuppgiftsbiträde när vi lämnar LAS-lista till dem?

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Denna situation torde inte vara för handen i frågan. Istället bestämmer facket ändamålen och medlen med behandlingen och är sålunda personuppgiftsansvarig i enlighet med artikel 4.7

8.3. Vilka krav kan facket ställa på oss utifrån dataskyddsförordningen?

Dataskyddsförordningen ger inte facket några särskilda rättigheter i förhållande till företagen. De registrerade ges däremot en rad olika rättigheter. Facket kan i vissa fall stödja sig på i första hand MBL eller kollektivavtal, till exempel rörande informations- och förhandlingsskyldighet.

När det gäller kontaktpersoner hos de fackliga organisationerna kan dock viss informationsskyldighet finnas kring behandlingen av deras personuppgifter. Mycket av detta kan skötas via tydliga rutiner.

8.4. Vilken information ska man ge till den anställde i fråga om att dra av fackavgiften enligt uppbördsavtalet med IF Metall? Behöver man informera på nytt?

Den personuppgiftsansvarige ska ge den information som framgår av artikel 13–15. Den personuppgiftsansvarige bör kunna utforma informationen på sådant sätt att den även omfattar framtida likartade behandlingar.

8.5. Har ni några råd kring hur vi ska hantera personuppgifter i förhållande till vår kontakt med facken? Har vi rätt att till exempel ange personer vid för- och efternamn samt födelsedatum?

Personuppgifter får endast lämnas ut om det är förenligt med det ändamål för vilket uppgifterna samlades in. Det måste också, bland annat, finnas en giltig rättslig grund. Huruvida dataskyddsförordningens grundläggande krav (artikel 5) och specifika krav (framför allt artikel 6–11) är uppfyllda, får avgöras i det enskilda fallet.

8.6. Uppgift om facklig tillhörighet: Ett exempel kring övergång av verksamhet i enlighet med LAS §6b. Ponera att vi per 1 juli 2018 skall ta över en verksamhet vilken innefattar 80 medarbetare. Inför förhandling i enlighet med MBL § 11 så vill vår fackliga motpart veta om de har någon medlem som berörs av övergången. Vi skickar därmed personnummer på samtliga berörda medarbetare till den fackliga motparten, för medarbetare som är anställda hos oss.

Personuppgifter får endast lämnas ut om det är förenligt med det ändamål för vilket uppgifterna samlades in. Det måste också, bland annat, finnas en giltig rättslig grund. Huruvida dataskyddsförordningens grundläggande krav (artikel 5) och specifika krav (framför allt artikel 6–11) är uppfyllda, får avgöras i det enskilda fallet. Det kan i detta fall noteras att uppgift om medlemskap i fackförening utgör en känslig personuppgift enligt artikel 9 dataskyddsförordningen. Sådan behandling kan vara tillåten enligt (exempelvis) artikel 9.2 b), om det tillåts enligt nationell rätt eller kollektivavtal. Det kan också noteras att personnummer visserligen inte utgör en känslig uppgift enligt dataskyddsförordningen men ändå omgärdas av särskilda krav, se artikel 87. Ett utlämnande av personuppgifter – när namn kan vara tillräckligt – torde strida mot principen om uppgiftsminimering och därför inte vara tillåtet. Det kan finnas en skyldighet att lämna namn till facket, till exempel med stöd av ingångna kollektivavtal, rörande anställda (och blivande anställda) men som regel inte avseende de arbetstagare som är oorganiserade eller som tillhör ett annat fack än det som ställt frågan.

8.7. Enligt kollektivavtal som vi är bundna av ska vi skicka över vissa löneuppgifter till facket. Får jag göra det och i så fall på vilken grund? Skiljer det sig åt för fackliga medlemmar och icke medlemmar?

Om skyldigheten att tillhandahålla löneuppgifter till facket följer av ett kollektivavtal kan arbetsgivaren stödja sig på den rättsliga grunden i art. 6.1 c – behandling för att uppfylla en rättslig förpliktelse. En sådan förpliktelse behöver nämligen inte följa av författning utan kan även följa av kollektivavtal. (Se Dataskyddslagen 2 kap 3 §). Sannolikt innehåller kollektivavtalet en förpliktelse avseende organiserades löner.

Så om kollektivavtalet innehåller en förpliktelse att överlämna löneuppgifter till facket måste en sådan förpliktelse följas. Det gäller även avseende oorganiserade arbetstagare. Av detta följer att om kollektivavtalet *inte* innehåller en sådan förpliktelse får du heller inte skicka över personuppgifter till facket.

8.8. Vilka personuppgifter/ärendeanteckningar är tillåtna att registrera i ett HR-system? Är det OK att alltid ha en anteckning om fackligt medlemskap?

För att få behandla personuppgifter krävs ett angivet ändamål och en rättslig grund. Detta är frågor man måste ställa sig inför varje specifik behandling. Typiskt sett kan den rättsliga grunden vara fullgörande av anställningsavtalet eller en rättslig förpliktelse. Fackligt medlemskap är en känslig personuppgift och får bara behandlas om någon av de särskilt föreskrivna grunderna för detta är uppfyllda. En sådan grund inom arbetsrätten kan vara en förhandling enligt MBL, uppbörd av fackavgift eller fastställande av turordning i en uppsägningssituation. Man måste även fråga sig vem som ska ha tillgång till uppgiften i fråga. Vid till exempel uppbörd av fackavgift är det lönekontoret som behöver uppgiften, men sannolikt ingen annan. Vid upprättande av turordningslista är det HR-personen som ska upprätta listan som behöver den.

Det är också viktigt att arbetsgivaren verkligen har aktuella uppgifter. Förlitar sig arbetsgivaren på gamla anteckningar kan misstag begås beträffande exempelvis förhandlingsskyldigheten i Medbestämmandelagen.

9. Gallring

Allmänt

Personuppgifter om en anställd bör inte bevaras efter det att denne har slutat. Men ibland måste vissa uppgifter bevaras under en längre tid, till exempel om andra lagar kräver det. Arbetsgivaren får också behålla uppgifter under den tid som en tvist med en tidigare anställd kan bli aktuell. Det kan också vara nödvändigt att bevara vissa uppgifter för administrativa ändamål, till exempel utbetalning av pension från arbetsgivaren eller om man ska lämna referenser till andra arbetsgivare. Arbetsgivaren får bevara rena faktauppgifter som ”uppsägning på grund av arbetsbrist”, ”avsked” och ”uppsägning på grund av personliga skäl” samt betyg och tjänstgöringsintyg med omdömen som arbetsgivaren har gett till arbetstagaren efter det att anställningsförhållandet har upphört.

9.1. Hur länge måste uppgifter sparas?

Så länge som det är ”nödvändigt”, se artikel 5.1 e. Det kan därför inte uppställas en och samma gallringsrutin för alla typer av uppgifter. Det kan handla om lagkrav i olika typer av lagstiftning som innebär att uppgifter kan behöva rensas efter två år, tio år, 40 år eller ännu längre, beroende på vad det är för slags uppgift och vad syftet med att spara den må vara.

9.2. Måste jag spara uppgift om en anställds anställningstid?

Ja, även efter det att en anställning har upphört, eftersom Lagen om anställningsskydd (LAS) är konstruerad så att om samma individ får anställning hos samma arbetsgivare i framtiden ska anställningstiden läggas samman med den tidigare anställningstiden. Den uppgiften bör således sparas så länge som individen teoretiskt sett skulle kunna återanställas i företaget.

Sparas uppgifter med denna grund får de inte användas för andra ändamål utan att denna behandling i sig har laga stöd enligt artikel 6.

9.3. Hur länge får jag spara personuppgifter för att kunna lämna arbetsgivarintyg?

Ett arbetsgivarintyg behövs för att a-kassan ska kunna bedöma den sökandens rätt till ersättning. Det finns inga regler för när ett arbetsgivarintyg ska lämnas, men det finns en skyldighet för arbetsgivaren att utfärda ett på begäran. Ansökan om a-kassa ska göras senast nio månader från den sista dagen i den period som ansökan avser. Eftersom det är svårt att veta hur länge en anställd väntar med att ansöka bör det vara rimligt att spara informationen i cirka två år.

9.4. Om ett försäkringsbolag (ex. AFA) frågar efter uppgifter, hur länge måste vi kunna svara? Denna frist måste nämligen korrespondera med hur länge vi får spara personuppgifter.

Enligt AFA gäller följande preskriptionsregler:

Preskriptionstider i TFA-KL

För att ha rätt till ersättning från TFA-KL för sveda och värk, lyte eller annat stadigvarande men, samt olägenheter måste ett olycksfall anmälas till AFA Försäkring inom 10 år från den dag skadan inträffade. För arbetssjukdom gäller i stället att anmälan ska göras inom 10 år från det att Försäkringskassan fattade beslut om godkänd arbetsskada. Kommer ansökan om ersättning in senare, är rätten till ersättning förlorad.

När det gäller ersättning för inkomstförlust, förlust av underhåll, begravningskostnad samt annan ersättning ska ansökan om ersättning ske inom 6 år. Kommer ansökan in senare kan AFA Försäkring endast lämna ersättning för tid 6 år tillbaka från ansökningstillfället.

Efterskydd i TFA-KL

Om en arbetssjukdom visar sig först efter det att den skadades anställning har upphört kan TFA-KL ändå gälla. För detta krävs dock dels att den skadade varit utsatt för skadlig inverkan i sitt arbete efter den 31 januari 1974, dels att sjukdomen visat sig innan den skadade fyllt 65 år.

Undantaget gäller om den skadade drabbats av cancer som har orsakats av exponering för asbest i arbetet. Då gäller ingen åldersgräns alls uppåt, utan sådana fall ersätts oberoende av den skadades ålder när sjukdomen visar sig.

Så man kan säga att så länge det eventuella ”kravet” inte är preskriberat finns en rättslig grund att spara personuppgifterna.

9.5. Hur länge får jag spara uppgifter från tidigare rehabiliteringsutredningar?

För att få behandla personuppgifter krävs ett angivet ändamål och en rättslig grund. Typiskt sett kan den rättsliga grunden vara fullgörande av anställningsavtalet eller en rättslig förpliktelse, men även för att kunna göra gällande rättsliga anspråk i framtiden (till exempel att säga upp en anställd) men i så fall baserat på en bedömning i det enskilda fallet. Så länge det är möjligt att hävda en rättighet eller skyldighet utifrån avtal eller rättslig förpliktelse behöver uppgifterna finnas tillgängliga. I fråga om rehabilitering finns ofta både grund för att behandla personuppgifter för att fullgöra anställningsavtalet och för att fullgöra en rättslig förpliktelse enligt författningar om rehabilitering för arbetsgivaren. Under pågående anställning behöver Arbetsgivaren således spara uppgifter om fullgjord rehabilitering sannolikt under en relativt lång period för att i efterhand kunna säkerställa att rehabiliteringen fullgjorts men även för att kunna vidta relevanta åtgärder vid nytt behov av rehabilitering. Man får dock göra skillnad från fall till fall. En uppgift om en rehabilitering vid ett benbrott är sannolikt möjlig att gallra långt tidigare än en uppgift om rehabilitering vid alkoholsjukdom, då den senare skulle kunna återaktualiseras vid återfall. Se exempelvis AFS 1994:1 11§ (med 9 §). Där står att om det är nödvändigt ska åtgärderna dokumenteras skriftligt.

https://www.av.se/globalassets/filer/publikationer/foreskrifter/arbetsanpassning-och-rehabilitering-foreskrifter-afs1994-1.pdf

9.6. Hur gallrar man säkert? Ska fysiska papper tuggas/förstöras? Finns det tekniska system/program som ni känner till som kan se till att inga digitala spår lämnas kvar? Hur kan man vara säker på att det verkligen inte finns något kvar?

Gallring ska göras med utgångspunkten att personuppgiften inte ska kunna gå att få fram efter det att den har gallrats. Fysiska dokument ska tuggas eller förstöras eller tas om hand i sekretesskyddad återvinning och ska naturligtvis inte slängas på en plats där det finns risk att de kommer obehöriga tillhanda. Vad gäller elektroniskt lagrad information finns alltid en risk för att den kan återskapas såvida inte mycket långtgående åtgärder vidtas. Det bör i de allra flesta situationer vara orimligt att kräva en fullständig säkerhet med avseende på risk för återskapande. Här får man föra en dialog med den leverantör som tillhandahåller serverutrymme, personalsystem m.m. och försäkra sig om vad som gäller.

9.7. Den stora mail-inkorgen med spontanansökningar, hur länge får mail ligga där? Behöver vi gallra?

För att få behandla personuppgifter krävs ett angivet ändamål och en rättslig grund. Vad gäller spontanansökningar skulle den rättsliga grunden kunna vara ändamål som rör den personuppgiftsansvariges intressen eller en rättslig förpliktelse (enligt diskrimineringslagen).

Enligt diskrimineringslagen kan den som gör en förfrågan om ett arbete diskrimineras, varför en person som skickat in en spontanansökan skulle kunna göra gällande diskriminering. Spontanansökan bör därför gallras efter två år från det att den kom in.

Det kan vara en fördel att ha en tydlig rutin kring hantering av spontanansökningar. För många organisationer torde det vara önskvärt att inte spara en mängd uppgifter från sådana ansökningar. Rutinen kan då vara att maila ett svar och hänvisa till att lediga tjänster annonseras på hemsidan. De inskickade handlingarna kan då rensas.

9.8. Exempel på gallringstider

Det är inte möjligt att uttala sig generellt om lagrings- och gallringstider för de personuppgifter som en arbetsgivare kan ha anledning att behandla. Behandling som är nödvändig för att fullgöra en rättslig förpliktelse förlorar sin rättsliga grund varefter möjliga anspråk mot arbetsgivaren preskriberas. Till exempel preskriberas fordringar avseende semesterlön, semesterersättning eller skadestånd med stöd av semesterlagen efter två år från utgången av det semesterår då arbetstagaren enligt lagen skulle ha fått den förmån som begäran gäller. Även förhandlingsordningar i kollektivavtal innehåller preskriptionsregler. Dessa omfattar emellertid endast medlemmar i kollektivavtalstecknande organisationer. Samtidigt blir det omotiverat merarbete att skapa olika gallringsrutiner beroende på fackligt medlemskap, något som ju också kan skifta för en individ över tid.

Några exempel:

- Anställningstid – så länge som individen teoretiskt sett skulle kunna återanställas i företaget.
- Löneuppgifter – 10 år från senaste uppgiften.
- Semester – 2 år efter semester/utbetalning av semesterlön.
- Rekrytering – 2 år efter anställningsbeslutet.

9.9. Hur länge får vi spara anställningsavtal?

Vissa uppgifter i anställningsavtalet måste sparas längre än andra. Uppgifter om anställningstid ska sparas så länge som individen teoretiskt sett skulle kunna återanställas i företaget. Däremot behöver andra uppgifter gallras för att arbetsgivare inte ska bryta mot dataskyddsförordningen, till exempel finns uppgifter som inte är försvarliga att spara mer än två år.

9.10. Hur länge ska vi spara uppgifter om inbetalning till de kollektivavtalade försäkringarna (ITP, TGL, TFA etc)

Uppgifter om premieinbetalningar registreras och sparas hos aktuell valcentral (Fora/Collectum). Sådana inbetalningar kan alltså spåras av valcentralen och behöver inte sparas av arbetsgivaren. Pensionslösning för ”tiotaggare” kan vara svårare att spåra varför en bedömning får göras i det enskilda fallet. För att kunna bemöta ett rättsligt anspråk på pension kan uppgifterna sparas fram till dagen för preskription, det vill säga tio år från det att pensionen tidigast kan göras gällande.

9.11. Hur länge får arbetsgivare spara utgivna arbetsgivarintyg?

När arbetsgivaren fullgjort skyldigheten att utge arbetsgivarintyg ska det raderas. Vill arbetsgivaren försäkra sig om bevisning om utgivet arbetsgivarintyg är inhämtning av kvittens ett mer lämpligt alternativ än att spara själva intyget

9.12. Hur länge får arbetsgivare spara uppgifter för att kunna skriva ett arbetsgivarintyg?

Rätten till ersättning bedöms på de 12 månaderna innan sökanden blir arbetslös och anmäler sig som arbetslös på arbetsförmedlingen. Men om personen till exempel är studieledig eller hemma med barn under två år utgör den tiden så kallad överhoppningsbar tid. Som huvudregel bör uppgifterna inte sparas längre än två år men uppgifterna kan i vissa fall vara relevanta längre tid än så.

9.13. Hur länge kommer vi kunna ha kvar data i våra HR system, det vill säga data som namn, personnummer, adress, anställningsdata med mera

För att få behandla personuppgifter krävs att det finns ett berättigat ändamål. Det kan handla om att behandling är nödvändig för att uppfylla en rättslig förpliktelse eller för att fullgöra anställningsavtalet. Efter avslutad anställning upphör i många fall tidigare anledningar för att spara eller på att annat sätt behandla personuppgifter om den anställde. I andra fall kan det finnas anledning att spara personuppgifterna till exempel för underlag för arbetsgivarintyg. Vid avslutad anställning ska alltså en gallring genomföras.

9.14. Hur länge kan vi spara anteckningar och dokumentation som används till grund för lönesamtal och lönerevision?

Anteckningar och dokumentation som ligger till grund för lönesamtal och lönerevision får sparas så länge som uppgifterna kan anses relevanta för just det ändamålet. Uppgifterna får inte sparas för att de kan ”vara bra att ha” eller användas för andra ändamål såsom bemanningsplanering.

9.15. Hur länge kan vi spara dokument och underlag (läkarintyg, protokoll, anteckningar med mera) angående anställd som är långtidssjukskriven?

Utgångspunkten är att underlaget kan sparas fram till att rehabiliteringen är slutförd. Vid vilken tidpunkt rehabiliteringen är slutförd är en bedömning som arbetsgivaren ska göra. Utredningen kan därefter behövas för andra ändamål, till exempel uppsägning av personliga skäl. Uppgifterna bör då gallras så att bara de uppgifter som är nödvändiga för uppsägningen lagras.

9.16. Hur länge kan vi spara dokumentation hänförlig till arbetsskada eller tillbud?

Vad gäller arbetstagarens anmälan om arbetsskada till AFA Försäkring och Försäkringskassan ska arbetsgivaren endast bekräfta anställningen. Anmälan om arbetsolyckan utgör då underlag vid eventuell förfrågan från AFA Försäkring.

Arbetsmiljöverket rekommenderar företagen att spara en kopia på anmälan. Uppgifterna bör kunna sparas så länge som ärendet är aktuellt.

Dokumentation kring arbetsolyckan bör även sparas som ett led i arbetsgivarens systematiska arbetsmiljöarbete. Den dokumentationen ska anonymiseras så långt det är möjligt.

9.17. Kan vi fortsätta behålla och behandla personuppgifter trots att den anställde har begärt att få sina personuppgifter raderade (till exempel efter att anställningen har upphört)?

En anställd har rätt att få sina personuppgifter raderade under förutsättning att arbetsgivaren inte längre har berättigade ändamål att behandla personuppgifterna eller har behandlat personuppgifterna i strid med dataskyddsförordningen. Personuppgifter som är nödvändiga att behandla för att till exempel uppfylla en avtalsrättslig skyldighet eller rättslig förpliktelse kan alltså fortsatt behandlas trots begäran om radering. I de fall behandlingen av personuppgifter grundar sig på samtycke från den registrerade får begäran om radering anses som att den registrerade återtagit samtycket. Om det saknas annat berättigat skäl för behandling ska de personuppgifterna raderas. Om behandlingen grundar sig på en intresseavvägning finns anledning att göra en förnyad bedömning av intresseavvägningen.

9.18. Gäller dataskyddsförordningen för utskrifter av till exempel mötesanteckningar som arkiveras (ej i manuellt register)?

Personuppgifter i pappersform omfattas normalt inte av dataskyddsförordningen, om de inte utgör ett manuellt register. Själva utskriften från datorn utgör däremot en behandling av personuppgifter. Utskriften i sig måste alltså vara tillåten enligt dataskyddsförordningens bestämmelser. Att exempelvis skriva ut personuppgifter i samband med att de inte längre behövs för det ändamål som de samlades in för och utskriften görs enbart för att de ändå ska bevaras är alltså förbjudet enligt dataskyddsförordningen. Om utskriften görs därför att uppgifterna kan behövas i pappersform för andra ändamål, till exempel för bokföringsändamål, är utskriften däremot tillåten. På så vis omfattas alltså utskrifter av dataskyddsförordningens bestämmelser.

9.19. Vi har fått en fråga om rätten att bli raderad (artikel 17 dataskyddsförordningen). Hur länge kan man som arbetsgivare anses vara skyldig för att uppfylla lag eller avtal spara någons personuppgifter i personalsystemet?

Rätten för den registrerade att bli raderad är inte absolut och gäller till exempel inte då arbetsgivaren som personuppgiftsansvarig måste behandla personuppgifter om anställda för att uppfylla en rättslig förpliktelse eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Till exempel har arbetsgivare en skyldighet att beakta all sammanlagd anställningstid, bland annat för att beräkna uppsägningstid eller plats i turordning. Arbetsgivaren måste då ha tillgång till uppgift om eventuella tidigare anställningar. Det gör att arbetsgivaren behöver ha tillgång till vissa uppgifter om den anställde till i vart fall uppnådd pensionsålder. För fordran på pension räknas den tioåriga preskriptionstiden från den dag fordringen tidigast kan göras gällande, det vill säga då utbetalning av pension sker. Även uppgifter om inbetalda pensionspremier kommer därför att behöva sparas under lång tid. Andra uppgifter är läkarundersökningar avseende personal som exponerats för vissa kemikalier. Enligt 3 § arbetsmiljöförordningen ska sådana uppgifter sparas i 40 år. Helt bortglömd kan arbetstagare således inte räkna med att bli. Däremot kan successivt den rättsliga grunden för och ändamålet med behandling av olika kategorier personuppgifter försvinna varför dessa måste gallras ut. Över tiden blir då allt färre uppgifter kvar om den tidigare anställde.

9.20. Hur länge, efter att en anställning har upphört, får vi spara anställningsuppgifterna? Är det något som ska sparas/slängas direkt?

Utgångspunkten enligt dataskyddsförordningen är uppgiftsminimering, vilket innebär att så få uppgifter som möjligt ska sparas och då inte längre än nödvändigt. Vad som är nödvändig tid kommer att variera med uppgifternas karaktär och ändamålet med att lagra dem. Till exempel kan arbetsgivare ha ett intresse att spara uppgifter om lön och pensionspremier under lång tid i syfte att fullgöra anställningsavtalet eller rättsliga förpliktelser när det gäller den anställdes rätt till pension. Vidare har arbetsgivaren en skyldighet att beräkna anställningstid på all sammanlagd anställningstid. Om den anställde återkommer till samma bolag måste arbetsgivaren därför ha tillgång till uppgifter om tidigare anställningar.

Däremot kan andra uppgifter om utvecklingssamtal, genomgångna utbildningar, prestationer och andra omdömen relativt snabbt behöva gallras ut. Om anställningen avslutats på grund av personliga skäl eller avskedande kan det i och för sig finnas ett intresse av att behålla uppgifterna för att kunna behandla framtida misskötsamhet inom bolaget på ett likvärdigt sätt, även det en rättslig förpliktelse för arbetsgivaren. Det viktiga är att arbetsgivaren kan ange en rättslig grund och ett korrekt ändamål för behandlingen av personuppgifterna även efter det att anställningen upphört, till exempel att arbetsgivarens intresse av nämnda skäl väger över arbetstagarens intresse av att uppgifterna inte behandlas.

9.21. När en medarbetare slutar, ska vi då radera all information om utbildning eller kan vi spara den i ett år efter avslutad utbildning?

En gallringsrutin som innebär att den typen av uppgift sparas i ett år efter avslutad utbildning bör vara godtagbar. Det kan vara så att den anställde har företrädesrätt till återanställning. Samtidigt får man ställa sig frågan vad skälet kan vara till att man vill spara uppgifterna under så lång tid efter anställningen upphört. Att uppgifterna ”kan vara bra att ha” är inte ett ändamål som är förenligt med dataskyddsförordningen.

9.22. Personalärenden/misskötsamhet/erinran: Hur länge får arbetsgivare spara underlag som rör personalärenden såsom till exempel misskötsamhet, erinran etc?

Till följd av lojalitetsplikten i anställningsavtalet kan arbetsgivaren ha behov av att spara uppgifter om arbetstagares misskötsamhet. Så länge anställningen består bör det vara möjligt att behålla den typen av uppgifter förutsatt att uppgifterna är nödvändiga och relevanta för ändamålet. Samtidigt bör det finnas en begränsning avseende vilka inom bolaget som har tillgång till den typen av uppgifter. Särskilt gäller det om dokumentationen avser händelser som ligger längre bak i tiden. Behandlingen måste vara möjlig att motivera utifrån den rättsliga grunden. Typiskt sett är det svårt att åberopa omständigheter som inträffat för 5–10 år sedan i en arbetsrättslig tvist. Å andra sidan kan arbetsgivaren ha giltiga behov för att spara uppgifterna för att bedöma lämplighet vid omplacering eller befordran eller annars vid utövande av arbetsledningen.

Även om den anställde har rätt att begära radering av personuppgifter enligt artikel 17 så gäller denna inte om behandlingen är nödvändig för att arbetsgivaren ska kunna fastställa, göra gällande eller försvara rättsliga anspråk.

9.23. Hur länge kan vi spara avgångsorsaker i HR-system?

Vad är skälet till att arbetsgivaren vill spara uppgifter om varför anställningen upphörde? Uppgiften kan behövas under tiden som arbetsgivaren är skyldig att utfärda ett arbetsgivarintyg som den (tidigare) anställde kan visa upp vid ansökan om arbetslöshetsersättning. Vidare kan uppgifter om olika typer av orsaker till att anställningen avslutades sparas för att arbetsgivaren ska kunna säkerställa att lika situationer behandlas lika – det är en rättslig förpliktelse som följer av praxis enligt anställningsskyddslagen. En viss typ av misskötsamhet bör föranleda samma åtgärd från arbetsgivarens sida om någon annan anställd gör sig skyldig till sådan på nytt. Ett annat skäl kan vara att överväganden om turordning och kvalifikationer inför förhandling om turordning vid arbetsbrist ska behandlas lika. Därför finns skäl att spara uppgifter om avgångsorsaker, men då även uppgifter om kvalifikationer och prestationer för anställda. Dock bör en viss längsta tid anges, varefter möjligen anonymiserade uppgifter kan sparas. Ett lämpligt ändamål att spara uppgifterna om skälet till att en anställning upphörde för en viss anställd kan då vara det uttryckliga och berättigade ändamålet att föra en konsekvent personalpolitik över tiden. Att inte ha tillgång till uppgifter om hur personalen hanterats tidigare skulle göra det omöjligt. De uppgifter som sparas ska då vara adekvata, relevanta och inte för omfattande i förhållande till detta ändamål. Den rättsliga grunden för behandlingen är då den rättsliga förpliktelsen att inte agera godtyckligt i förhållande till sin personal.

9.24. Vad är en rimlig tidsperiod för att spara prestationsdata på individnivå innan den avidentifieras eller raderas?

Dataskyddsförordningens krav på korrekt behandling av personuppgifter går ut på att det ska finnas ett särskilt, uttryckligt angivet och berättigat ändamål för behandlingen och uppgifterna ska inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Vad som är en rimlig tidsperiod kommer därför att vara beroende av vilka ändamål arbetsgivare har för att behålla prestationsdata på individnivå. Om uppgifterna ligger till grund för beräkning av rörlig lön, bonus eller liknande kan uppgifterna behöva sparas under sådan tid som anspråk på korrigering av lön kan göras. Om uppgifterna ligger till grund för optimering av produktionsapparaten kan uppgifterna sparas under sådan tid som produktionsapparaten eller delar av den har samma uppbyggnad som då prestationsdata insamlades. Men då kanske det inte finns behov av uppgifter om identifierbara individer alternativt att uppgifterna kan pseudonymiseras.

10. Information

10.1. Vad behöver vi informera en anställd om avseende dataskydds-förordningen vid anställningstillfället?

Arbetsgivaren har en skyldighet att informera om behandlingen av de anställdas personuppgifter enligt vad som följer av förordningens artiklar 12, 13, 14. Just vid anställningstillfället kan det räcka med information avseende det som behövs för att upprätta anställningsavtalet för att sedan när den anställde tillträder sin tjänst mer utförligt informera om personuppgiftsbehandling, till exempel i samband med introduktion. Enligt artikel 12.1 ska informationen tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisas på annat sätt.

Informationen kan lämpligen tillhandahållas som en hel integritetspolicy eller dylik handling. Det viktiga är att innehållet uppfyller förordningen. Vår rekommendation är att policyn bör signeras fysiskt eller digitalt för bevisvärdet. Att endast tillhanda-hålla information på till exempel ett intranät kan uppfylla förordningens krav, men det kan göra det svårare att bevisa att den personuppgiftsansvarige uppfyllt sina skyldigheter vad gäller information till de anställda. Inför att förordningen träder i kraft ska den personuppgiftsansvarige säkerställa att informationskravet är upp-fyllt gentemot samtliga anställda.

Av artikel 14.5 b framgår att skyldigheten att lämna information enligt artikel 14 inte gäller om skyldigheten sannolikt kommer göra det omöjligt eller avsevärt försvåra uppfyllandet av målen med den behandlingen.

10.2. När jag får en arbetsansökan via mail som jag ska skicka till exempelvis chef som är med i processen, måste vi informera arbetssökande om den spridningen?

Information ska lämnas avseende behandling för rekryteringsprocessen, detta inbegriper att dela uppgifterna internt till chef som är delaktig i processen. Samtycke har lämnats i och med ansökan.

När rekryteringsprocessen är avslutad bör dock den här typen av mail rensas, då saknas stöd för behandling i form av fortsatt lagring av sådan korrespondens. Om företaget vill spara uppgifterna för framtida rekrytering måste den registrerade samtycka till detta.

10.3. Måste vi lämna ut registerutdrag till anställd under pågående utredning? Om så är fallet; i vilken omfattning?

Av propositionen till Dataskyddslagen (Prop. 2017/18:105) s. 202 framgår ang 5 kap 1 §:

”Andra stycket innebär att en personuppgiftsansvarig som inte omfattas av offentlighets- och sekretesslagens tillämpningsområde får vägra att lämna ut information till den registrerade, om en bestämmelse i den lagen hade hindrat utlämnande till den regist-rerade om den personuppgiftsansvarige hade varit en myndighet. Det kan till exempel röra sig om information som samlats in inför en facklig förhandling eller en domstols-process, om det kan antas att ett utlämnande av informationen skulle försämra den personuppgiftsansvariges ställning som part i förhandlingen eller rättegången.”

Om utlämnandet skulle på något sätt försvåra för företaget att tillvarata sin rätt inför en förhandling eller en rättslig process så behöver inte uppgifterna lämnas ut.

10.4. Utgör hantering av anställdas personuppgifter sådan icke tillfällig behandling som ger en skyldighet för våra företag att ha ett behandlingsregister?

Artikel 30.1 – Skyldighet för personuppgiftsansvarige att föra register över de behandlingar som utförts under dennes ansvar. Även avslutade behandlingar ska finnas i registret.

Artikel 30.5 – undantag vid färre än 250 anställda:

- Ska inte vara sannolikt att behandlingen medför risker för kränkning av enskildas rättigheter och friheter.
- Behandlingen ska vara tillfällig.
- Ska inte röra känsliga personuppgifter/uppgifter om lagöverträdelser.

Datainspektionen har vintern 2017/18 svarat på frågan enligt följande:

Som huvudregel ska man föra register över de behandlingar man utför. Från denna skyldighet finns undantag i artikel 30.5 i dataskyddsförordningen.

Eftersom tolkningen av dataskyddsförordningen ska vara densamma över hela EU-området har vi som nationell dataskyddsmyndighet svårt att ge ett säkert svar. Men enligt vår preliminära tolkning av undantaget från registreringsskyldigheten i artikel 30 gäller undantaget endast om samtliga tre strecksatserna nedan är uppfyllda.

Företag och organisationer som har färre än 250 anställda behöver inte registrera vissa mindre riskfyllda behandlingar, nämligen behandlingar som inte kommer medföra risk för de registrerades rättigheter och friheter, är tillfälliga och inte omfattar känsliga personuppgifter enligt artikel 9 eller personuppgifter om lagöverträdelser enligt artikel 10.

Vi har tyvärr ingen vägledning att ge när det gäller innebörden av ”tillfällig behandling”, men som vi uppfattar undantaget ska varje behandling bedömas för sig. Om någon av de behandlingar som utförs inte omfattas av undantaget måste ett register föras över den behandlingen/behandlingarna, medan de behandlingar som uppfyller de tre strecksatserna inte behöver tas med i registret. Till exempel måste den behandling som utförs i syfte att administrera löner till de anställda registreras eftersom den inte är tillfällig, samtidigt som en annan typ av behandling som utförs kanske inte behöver registreras.

Oavsett om man är skyldig att registrera en behandling eller inte behöver man ju ha full koll på vilka behandlingar man utför för att till exempel kunna informera de registrerade.

Vänliga hälsningar
Jurist, Datainspektionen

Slutsatsen kan konkret sägas vara att även om det visserligen kan vara så att det inte finns en rättslig skyldighet att ha ett behandlingsregister behövs ändå någon form av kontroll över behandlingarna som sker inom organisationen. Det enklaste sättet att få den kontrollen är trots allt genom någon form av behandlingsregister.

Formen för behandlingsregister är inte reglerad, vilket gör att det inte är nödvändigt med dyra IT-lösningar. Det kan räcka med egenskapade register över behandlingarna och de ställningstagande kring exempelvis laga stöd och rutiner som gjorts.

10.5. Vilken information måste vi ta fram och skicka till en registrerad? Alla lönespecifikationer, tidsstämplingar, etc? Eller räcker det med ett sammandrag från personalmastern och information om att det även finns information i lönesystem, behörighetsregister, tid redovisningssystem etc och att den registrerade kan återkomma om denne vill ha ytterligare utdrag?

Vi tolkar förordningen på så sätt att det *inte* endast är kategorier av personuppgifter som avses. Artikel 15.1 lyder ”tillgång till personuppgifterna”. I artikelns p. 3 framgår likaså att det är en kopia av de ”personuppgifter som är under behandling”. I ingressen (63) anges till exempel att rätten att få tillgång till uppgifter om hälsa innebär en rätt att få tillgång till uppgifter i läkarjournaler med till exempel diagnoser, undersökningsresultat och eventuella vårdbehandlingar etc. Vi anser dock att rätten inte inbegriper en rätt att få del av handlingen som sådan.

En begränsning i förordningen, som avser information som tillhandahålls enligt artiklarna 13, 14 och 15–22, är den möjlighet som den personuppgiftsansvarige har att ta ut en avgift som täcker de administrativa kostnaderna att tillhandahålla information eller vidta den åtgärd som begärs eller att vägra tillmötesgå begäran om den är uppenbart ogrundad eller orimlig (artikel 12.5 b).

En ytterligare begränsning i förordningen framgår av ingressen 63, som anger att denna rätt inte bör inverka menligt på andras rättigheter och friheter, till exempel affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Vidare följer av ingresstexten att om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser innan informationen lämnas ut. Vår bedömning är att vid icke svar eller begäran om tillgång till ”allt” måste allt lämnas med undantag av det som följer av det svenska lagförslaget.

Av förslaget till ny dataskyddslag 5 kap. 2 § framgår att den registrerades rätt till tillgång till uppgifter i artikel 15 i förordningen inte gäller personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckningar eller liknande och som inte behandlats längre än ett år.

Viktigt är att identifiera att det är rätt person som begär uppgifterna. Detta kan göras på olika sätt, såväl genom krav på att begäran skickas in via brev eller att personen ska identifiera sig via BankID. Skicka uppgifterna till folkbokföringsadressen med traditionell post.

11. Internationella frågor

11.1. Måste vi ha samtycke för att skicka uppgifter till huvudkontoret i Shanghai?

Nej, inte om annan rättslig grund för behandlingen finns. Samma problematik vid samtycke som grund inom arbetslivet. Överföring av personuppgifter till tredje land får enligt dataskyddsförordningen ske i följande situationer och under förutsättning att övriga regler i förordningen följs.

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.

Lämpliga skyddsåtgärder, till exempel standardavtalsklausuler eller bindande företagsbestämmelser, BCRs; Om det inte finns ett beslut från EU-kommissionen att ett land har en adekvat skyddsnivå får överföring ändå ske till ett tredje land om den som behandlar personuppgifterna har vidtagit lämpliga skyddsåtgärder. Dessutom måste det finnas lagstadgade rättigheter och effektiva rättsmedel för registrerade, det vill säga möjligheter för den enskilde att få behandlingen prövad i domstol.

Särskilt tillstånd av Datainspektionen; Ett sådant tillstånd kan ges om överföringen grundar sig på avtalsklausuler mellan den som för över uppgifterna och den som tar emot dem eller, om det gäller överföring mellan myndigheter, bestämmelser i administrativa överenskommelser som innehåller verkställbara och faktiska rättigheter för den registrerade. Innan tillsynsmyndigheten beslutar om tillstånd på grund av avtalsklausuler ska den begära ett yttrande från den europeiska dataskyddsstyrelsen, där företrädare för alla EU/EES-länders tillsynsmyndigheter är med.

Samtycke eller i andra särskilt angivna situationer; I vissa särskilda situationer får man föra över personuppgifter till ett land utanför EU/EES trots att landet inte har en adekvat skyddsnivå och trots att inte lämpliga skyddsåtgärder har vidtagits. Personuppgifter kan till exempel överföras om den registrerade uttryckligen har samtyckt till det efter att ha fått information om riskerna med överföringen. Överföring får också ske om det är nödvändigt i vissa uppräknade fall, till exempel för att fullgöra ett avtal på den registrerades begäran eller för att bevaka rättsliga anspråk.

Överföring vid enstaka tillfällen; Överföring av personuppgifter är också tillåten om den endast sker vid ett enstaka tillfälle (det vill säga om den inte är återkommande), 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. 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.

11.2. Om jag tar med mig datorn på en tjänsteresa till tredje land och loggar in på vår server från det landet, blir det då en överföring av personuppgifter till tredje land?

Är servern inom EU är det inte en tredjelandsöverföring.

12. Kompetensdatabas

12.1. Var går gränsen mellan löneavtalen och avtalen om kompetensutveckling i förhållande till den rättsliga grunden samtycke för att behandla personuppgifter? Till exempel uppgifter om utbildning etc. i kompetensdatabas som vanligen kräver ett samtycke?

Samtycke är inte en lämplig grund. Formulera ändamål och finn relevant rättslig grund. Löneavtal och kompetensutvecklingsavtal kan eventuellt utgöra rättslig förpliktelse. Även kompetensdatabas kan vara berättigat intresse vid till exempel behandling av rena faktauppgifter.

12.2. Hur får vi registrera olika kompetensåtgärder såsom genomgångna utbildningar i vår kompetensdatabas? Krävs det samtycke för att registrera dem? Hur är det om det är ett krav från vår ISO-certifiering att vi registrerar när arbetstagaren har genomgått viss utbildning? Måste vi informera arbetstagaren varje gång vi registrerar att den har genomgått en tilläggsutbildning? (Det krävs en utbildning så fort något på en blankett ändras, vi skull inte få göra annat än att informera och begära in samtycken)

Samma som ovan.

ISO-certifiering kan utgöra rättslig förpliktelse eller berättigat intresse beroende på ISO-certifierings rättsliga status.

Bör kunna hanteras inom ramen för övergripande ändamål, till exempel för att registrera genomförda utbildningar.

12.3. Hur ska man se på olika omdömen (samarbetsförmåga, flexibilitet m.m.) som lagras om den anställde för lönesättning? Är det ok enligt dataskyddsförordningen?

Den lagliga grunden kan vara för att uppfylla avtal eller för att fullgöra skyldighet enligt kollektivavtal (rättslig förpliktelse). Om inte någon av dessa grunder är tillämpliga kan behandling eventuellt ske efter en intresseavvägning, om berättigat intresse för arbetsgivaren att behandla väger tyngre.

12.4. Hur ska vi hantera värderingar om den anställde antecknade av chef vid till exempel utvecklings- och lönesamtal? Hur länge får vi lagra informationen?

Den lagliga grunden är berättigat intresse alt. samtycke. Uppgifterna får sparas så länge behov finns för att följa upp utvecklingssamtal, sätta lön etc.

12.5. Vilken rättslig grund kan vi använda för personuppgiftsbehandling i våra värderingssystem, exempelvis chefers utvärdering och deras återkoppling?

Berättigat intresse alt. samtycke. Om det rör sig om till exempel prestationslön kan den lagliga grunden vara för att fullgöra ett avtal.

12.6. Hur ska arbetsgivar- och branschorganisationer hantera kurser som ger behörigheter: är det upp till företagen själva att spara uppgifter om när anställda gick kurser eller kan organisationen spara detta med samtycke?

Att hantera kurser som ger behörighet är som huvudregel inte ett nödvändigt ändamål för arbetsgivar- och branschorganisationer. Ansvaret åvilar vanligtvis det enskilda företaget grundat på rättslig förpliktelse kopplat till viss behörighet. Kan även vara berättigat intresse för företaget att anställda genomgår viss kurs. Företaget är ansvarig för att hantera och spara uppgifter avseende sina anställda.

12.7. Hur skall vi hantera den lönestatistik som samlas in och hanteras delvis av Svenskt Näringsliv?

Med stöd av lagen (2001:99) om den officiella statistiken och statistikförordningen har den statistikansvariga myndigheten Medlingsinstitutet delegerat till Svenskt Näringsliv att genomföra insamlandet av uppgifter för att kunna skapa nationell lönestatistik. Utöver detta uppdrag finns kompletterande bestämmelser i kollektivavtal mellan Svenskt Näringslivs medlemsorganisationer och deras respektive fackliga motparter avseende personuppgiftshantering för statistikändamål. Syftet med behandlingen är att skapa underlag för den officiella statistiken i Sverige samt underlag för de kollektivavtalsbaserade löneförhandlingarna.

Inga obehöriga har tillgång till personuppgifterna och de anonymiseras när de övergår till att vara statistik.

13. Missbruksregeln försvinner

13.1. Hur får vi hantera mail och med vilket innehåll?

I Personuppgiftslagen § 5a har funnits ett undantag beträffande behandling av personuppgifter som görs i ostrukturerad form, såsom löpande text i mejl (den så kallade missbruksregeln). Denna regel försvinner när dataskyddsförordningen införs i maj 2018. Detta betyder att om ett mejl med löpande text innehåller personuppgifter, så kräver en sådan behandling lagligt stöd enligt dataskyddsförordningen.

Dataskyddsförordningen anger inga särskilda regler för e-posthantering. Om man behandlar personuppgifter genom e-post ska reglerna i förordningen tillämpas. Liksom för all annan behandling behöver arbetsgivaren bestämma för vilket ändamål personuppgifterna behandlas, fastställa rättslig grund m.m.

Arbetsgivare måste särskilt bedöma om uppgifterna som mailas är känsliga. Särskild försiktighet måste iakttas vid behandling av känsliga personuppgifter, exempelvis uppgifter om etnicitet, hälsa och fackföreningsmedlemskap.

Även sådana uppgifter som Datainspektionen betraktar som integritetskänsliga, exempelvis personnummer och löneuppgifter, bör behandlas med särskild försiktighet.

Det finns alltid en risk att andra än den avsedda mottagaren får del av uppgifterna när information skickas via e-post. Det kan således föreligga skäl att vidta särskilda säkerhetsåtgärder.

De säkerhetsåtgärder en arbetsgivare kan behöva vidta är exempelvis följande. Utfärda interna policys som reglerar vilka typer av personuppgifter som får översändas per e-post och vilka digitala lösningar som ska användas vid hantering av känsliga personuppgifter, exempelvis kryptering eller inloggning med lösenord. Tillse att policydokumenten är kända inom organisationen och följa upp att instruktionerna och reglerna efterlevs.

Sammanfattningsvis:

Datainspektionen rekommenderar:

- När ni mottagit och läst e-posten, bedöm om uppgifterna ska bevaras och var det i så fall ska ske för att uppfylla de krav som gäller för just dessa uppgifter.
- Skicka inte känsliga personuppgifter i oskyddad e-post.
- Informera på er webb i samband med e-postadressen hur ni behandlar personuppgifter eller länka därifrån till er integritetspolicy.
- Om ni skickar svarsmejl eller autosvar, bifoga en standardtext där ni informerar den som skickat e-post om hur ni behandlar personuppgifter eller länka till en integritetspolicy på er webbplats.
- Informera alla i er organisation om reglerna och rutinerna för hur ni behandlar personuppgifter i er organisation. Se också till att rutinerna hålls levande.

14. Registerutdrag

14.1. Registerutdrag ur HR-system, vad gäller övergripande? Ex: när missbruksregeln försvinner, hur bör företagen hantera intern e-postkommunikation i ett personalärende? Finns risk för att berörd arbetstagare kan begära registerutdrag av till exempel e-post där personuppgifter förekommer?

Den registrerade (individen) har enligt artikel 15 i dataskyddsförordningen rätt att begära ut information om vilka personuppgifter som behandlas av den personuppgiftsansvarige (så kallat registerutdrag).

Vid begäran om registerutdrag är det viktigt att säkerställa säkerhetsrutiner för hur utdrag ska lämnas ut. Ett viktigt led i detta är identifiering av den registrerade. Det är viktigt att identiteten bekräftas på den person som begär registerutdrag, för att säkerställa att inga personuppgifter sprids till felaktig person.

14.2. Vad får begäras ut i ett registerutdrag?

Något undantag motsvarande det som finns för exempelvis rätten till radering för att kunna fastställa, försvara och göra gällande rättsliga anspråk kan inte utläsas av förordningen vad gäller rätten till tillgång i artikel 15.

Vi tolkar förordningen på så sätt att det inte endast är kategorier av personuppgifter som avses. I artikelns p. 3 framgår likaså att det är en kopia av de ”personuppgifter som är under behandling”. I ingressen (63) anges till exempel att rätten att få tillgång till uppgifter om hälsa innebär en rätt att få tillgång till uppgifter i läkarjournaler med till exempel diagnoser, undersökningsresultat och eventuella vårdbehandlingar etc. Vi anser dock att rätten inte inbegriper en rätt att få del av handlingen som sådan.

En begränsning i förordningen, som avser information som tillhandahålls enligt artiklarna 13, 14 och 15–22 är den möjlighet som den personuppgiftsansvarige har att ta ut en avgift som täcker de administrativa kostnaderna att tillhandahålla information eller vidta den åtgärd som begärs eller att vägra tillmötesgå begäran om den är uppenbart ogrundad eller orimlig (artikel 12.5 b).

En ytterligare begränsning i förordningen framgår av ingressen 63, som anger att denna rätt inte bör inverka menligt på andras rättigheter och friheter, till exempel affärshemligheter eller immateriell äganderätt och särskilt inte på upphovsrätt som skyddar programvaran. Vidare följer av ingresstexten att om den personuppgiftsansvarige behandlar en stor mängd uppgifter om den registrerade bör den personuppgiftsansvarige kunna begära att den registrerade lämnar uppgift om vilken information eller vilken behandling en framställan avser innan informationen lämnas ut. Vår bedömning är att vid icke svar eller begäran om tillgång till ”allt” måste allt lämnas med undantag av det som följer av det svenska lagförslaget.

Av förslaget till ny dataskyddslag 5 kap. 2 § framgår att den registrerades rätt till tillgång till uppgifter i artikel 15 i förordningen inte gäller personuppgifter i löpande text som inte fått sin slutliga utformning när begäran gjordes eller som utgör minnes anteckningar eller liknande och som inte behandlats längre än ett år.

15. Personuppgiftsbiträde

Allmänt

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

En nyhet i förordningen är att några av de skyldigheter som tidigare har gällt för den personuppgiftsansvarige nu även gäller för personuppgiftsbiträdet, till exempel kraven på att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsombud.

Även personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig. Den personuppgiftsansvarige och personuppgiftsbiträdet måste upprätta ett så kallat biträdesavtal. Dataskyddsförordningen räknar upp vad ett sådant biträdesavtal ska innehålla.

15.1. Kan facket vara personuppgiftsbiträde?

En facklig organisation hanterar inte personuppgifter för arbetsgivarens räkning och är/kan inte vara personuppgiftsbiträde i den relationen. Arbetsgivaren hanterar uppgifter om fackligt medlemskap för sin egen räkning, eftersom arbetsgivaren har egna rättigheter och skyldigheter i förhållande till bland annat sina avtalsmotparter, det vill säga de kollektivavtalsslutande fackföreningarna och deras medlemmar, precis som facket.

15.2. Företagshälsovård. Var går gränsen mellan personuppgiftsbiträde och företagshälsovårdens egen behandling där företagshälsovården är personuppgiftsansvarig?

Ett personuppgiftsbiträde får endast hantera personuppgifter för den personuppgiftsansvariges räkning i enlighet med ett personuppgiftsbiträdesavtal som ska finnas mellan parterna. Personuppgiftsansvaret ligger hela tiden kvar hos den personuppgiftsansvarige. Troligen är företagshälsovårdens behandling självständig och det går inte att reglera i ett personuppgiftsbiträdesavtal hur företagshälsovården ska hantera personuppgifter. Detta beror dels på att det är annan lagstiftning som tar över och dels att företagshälsovården har en friare roll än vad som avses för att det ska föreligga en situation där företagshälsovården är att betrakta som ett personuppgiftsbiträde.

15.3. Hur ska ett personuppgiftsbiträdesavtal hanteras i förhållande till ett externt bolag som sköter till exempel löner?

Det externa bolaget som får uppdraget att sköta löner för den personuppgiftsansvariges räkning är troligen att se som personuppgiftsbiträde. Det innebär att mellan parterna ska upprättas ett personuppgiftsbiträdesavtal som reglerar hur personuppgiftsbiträdet får hantera personuppgifter. Avtalet bör kompletteras med instruktioner.

15.4. Vad måste ett personuppgiftsbiträdesavtal innehålla?

Om den personuppgiftsansvarige anlitar ett personuppgiftsbiträde ska det upprättas ett personuppgiftsbiträdesavtal mellan parterna som anger hur biträdet får behandla personuppgifter för den personuppgiftsansvariges räkning. Dataskyddsförordningen anger vad ett personuppgiftsbiträdesavtal ska innehålla (se artikel 28).

Enligt Datainspektionen ska biträdet, i avtalet, åta sig att:

- Bara behandla personuppgifter enligt dokumenterade instruktioner från den personuppgiftsansvarige.
- Se till att personer som har behörighet att behandla personuppgifter hos biträdet har åtagit sig att iaktta tystnadsplikt eller omfattas av lagstadgad sådan.
- Vidta alla tekniska och organisatoriska åtgärder som är nödvändiga för att säkerställa en lämplig säkerhetsnivå i förhållande till riskerna med behandlingen.
- Respektera kraven på förhandstillstånd och avtal vid anlitande av ett annat biträde (ett underbiträde).
- Vidta lämpliga tekniska och organisatoriska åtgärder så att den personuppgiftsansvarige kan svara på en enskilds begäran om att få utöva sina rättigheter, såsom rätten till information och registerutdrag, rättelse, radering m.m.
- Bistå den personuppgiftsansvarige med att se till att skyldigheterna fullgörs ifråga om säkerhetsåtgärder, anmälan av personuppgiftsincidenter och information om sådana incidenter till de registrerade samt konsekvensbedömning och förhandssamråd.
- Radera eller återlämna alla personuppgifter till den personuppgiftsansvarige (beroende på vad den personuppgiftsansvarige väljer) när uppdraget avslutas och även radera alla kopior.
- Ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att man fullgör alla skyldigheter som man har som biträde samt att möjliggöra och bidra till inspektioner och andra granskningar som den personuppgiftsansvarige vill genomföra.

Se vidare på Datainspektionens hemsida www.datainspektionen.se

15.5. Vilka räknas som personuppgiftsbiträde?

En annan fysisk eller juridisk person som utför personuppgiftsbehandling för den personuppgiftsansvariges räkning. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen, se artikel 4.8.

15.6. Behöver vi ett personuppgiftsbiträdesavtal med vår rekryteringsfirma?

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Det innebär att frågan ifall ett personuppgiftsavtal behövs är beroende av hur uppdraget mellan arbetsgivaren och rekryteringsfirman har utformats. Om rekryteringsfirman i uppdraget behandlar personuppgifter å en personuppgiftsansvarigs vägnar och inte självständigt kan bestämma hur personuppgifter ska hanteras krävs ett personuppgiftsbiträdesavtal som anger hur personuppgiftsbiträdet får behandla personuppgifterna. Personuppgiftsansvaret kvarstår hos arbetsgivaren.

Kan rekryteringsfirman däremot hantera personuppgifterna självständigt och till exempel endast välja ut tre kandidater till arbetsgivaren (kunden) och matcha övriga kandidater mot andra tjänster och uppdrag för andra arbetsgivare (kunder) har rekryteringsfirman sannolikt ett personuppgiftsansvar och ett personuppgiftsbiträdesavtal ska inte träffas.

15.7. När ett externt företag hanterar våra uppgifter – när vet man om de är ett personuppgiftsbiträde och vad ska man tänka på då?

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Det innebär att frågan ifall ett personuppgiftsavtal behövs är beroende av hur uppdraget mellan arbetsgivaren och det externa företaget har utformats. Om det externa företaget i uppdraget behandlar personuppgifter å en personuppgiftsansvarigs vägnar och inte självständigt kan bestämma hur personuppgifter ska hanteras krävs ett personuppgiftsbiträdesavtal som anger hur personuppgiftsbiträdet får behandla personuppgifterna. Personuppgiftsansvaret kvarstår hos arbetsgivaren.

15.8. Krävs personuppgiftsbiträdesavtal med Fora/Collectum? Måste arbetsgivaren informera arbetstagarna om att personuppgifter överförs till Fora/ Collectum

Collectum uppger själva:

2018-01-30

Information till arbetsgivare om hur Collectum behandlar personuppgifter enligt GDPR.

Collectum har redan ett personuppgiftsansvar för de personuppgifter som ni har lämnat till Collectum enligt kollektivavtalet. Därför är ett separat personuppgiftsbiträdesavtal med Collectum inte aktuellt. Alla arbetsgivare som har tecknat ett kollektivavtal är också skyldiga att teckna ett pensioneringsavtal med Collectum om tjänstepensionen ITP och en tjänstegrupplivförsäkring (TGL) för sina privatanställda tjänstemän.

16. Samtycke

Allmänt

Ett samtycke till att behandla personuppgifter ska enligt dataskyddsförordningen vara frivilligt, särskilt, informerat och en otvetydig viljeyttring. Samtycket ska också vara individuellt. Det kan lämnas muntligt eller skriftligt. Eftersom det är arbetsgivaren som har bevisbördan för att arbetstagaren verkligen givit sitt samtycke kan det vara lämpligt att på något sätt dokumentera det, till exempel på ett formulär som samtidigt innehåller den information som ska lämnas till den registrerade. Skriver man in sina personuppgifter i en databas efter att ha fått information om vad uppgifterna ska användas till anses man ha samtyckt. Däremot är det inte tillräckligt att arbetsgivaren antar att arbetstagaren samtycker till en behandling av personuppgifter.

Det kan ofta vara svårt för arbetsgivare att stödja en behandling av personuppgifter på samtycken från arbetstagarna. Det beror på att arbetstagare ofta befinner sig i en beroendeställning gentemot sina arbetsgivare och därför inte kan lämna sådana frivilliga samtycken som personuppgiftslagen kräver. Behandling av personuppgifter i arbetslivet med stöd av samtycke begränsas därför till sådana situationer där arbetstagaren har ett verkligt fritt val och senare kan ta tillbaka sitt samtycke utan att det medför några nackdelar. Om de anställda erbjuds rimliga alternativ och inte utsätts för någon direkt eller indirekt påtryckning att samtycka kan det vara tillåtet för arbetsgivaren att behandla personuppgifter med stöd av samtycken från de anställda.

Man kan inte samtycka generellt till behandling av personuppgifter, till exempel eventuella behandlingar i framtiden, utan att känna till vilka dessa är. Arbetsgivaren måste informera om en eller flera planerade behandlingar och samtycket avser då dessa. Det avgörande är att arbetstagaren vet vilka behandlingar han eller hon samtycker till.

Att samtycket ska vara individuellt innebär att det ska vara den registrerade som genom viljeyttringen godtar behandlingen av personuppgifter. Med det hindrar inte att en facklig organisation samlar in samtycken från varje medlem och lämnar dessa vidare till arbetsgivaren.

Ett samtycke kan återkallas

Arbetstagaren har rätt att när som helst ta tillbaka sitt samtycke. Det kan göras skriftligt eller muntligt. Det är arbetstagaren som har bevisbördan för att en återkallelse har gjorts och när det gjordes. Därefter får bara redan insamlade personuppgifter behandlas. Eftersom uppgifterna inte får uppdateras eller kompletteras utan samtycke kan de därför bli inaktuella eller ofullständiga och behöva avidentifieras eller raderas. De grundläggande kraven innebär nämligen att personuppgifter måste vara riktiga och aktuella.

16.1. Måste man ha samtycke för att spara anteckningar om anställda i en personalakt?

Arbetsgivare har oftast andra mer lämpliga rättsliga grunder än samtycke. Samtycke bör undvikas. Om det till exempel är nödvändigt för att uppfylla avtal med den registrerade, för att uppfylla en rättslig förpliktelse som åvilar den personuppgifts-ansvarige eller efter en intresseavvägning.

För att ett samtycke ska vara giltigt krävs att det är frivilligt, informerat, särskilt och en entydig viljeyttring. Inom arbetslivet kan samtycke endast användas om det finns ett alternativ till att lämna samtycke.

16.2. Finns det några hinder för att återkalla sitt samtycke?

Sker en personuppgiftsbehandling med stöd av samtycke som rättslig grund ska samtycket alltid kunna återkallas av den registrerade.

16.3. Gäller tidigare samtycken enligt Personuppgiftslagen efter övergång till dataskyddsförordningen?

Reglerna kring samtycke är mycket lika i Personuppgiftslagen och dataskydds-förordningen. Dock finns några nyheter i dataskyddsförordningen. Ett samtycke ska kunna klart särskiljas från andra frågor, det ska också alltid finnas information om att samtycke kan återkallas m.m. Den Personuppgiftsansvarige måste kontrollera att tidigare lämnade samtycken uppfyller kraven i dataskyddsförordningen. Gör de inte det, måste nya samtycken tas in.

16.4. Kan facket lämna samtycke kollektivt för sina medlemmar?

Nej, om de inte har fullmakt från var och en. Ett samtycke ska lämnas av den registrerade själv.

17. Sanktioner

17.1. Kan det bli sanktioner eller skadestånd vid en enskild händelse? Exempelvis om inte arbetsgivaren informerar den anställda innan han läser dennes privata mail. Kan den anställda då kontakta datainspektionen?

Ja, en enskild kan lämna in klagomål till Datainspektionen. Den som anser att någon behandlar uppgifter om honom eller henne i strid med dataskyddsförordningen kan lämna in ett klagomål till Datainspektionen. Datainspektionen tar del av alla klagomål och bedömer om tillsyn ska inledas och lämnar därefter besked till den som fört fram klagomålet. Datainspektionen måste meddela om tillsyn ska inledas eller inte inom tre månader efter att ha tagit emot klagomålet. Om den klagande inte får besked inom den tiden, kan han eller hon vända sig till domstol för att begära besked.

18. Säkerhet

18.1. Hur ska vi skydda känsliga uppgifter, exempelvis läkarintyg?

Den som behandlar personuppgifter måste se till att ha en lämplig säkerhetsnivå för uppgifterna, både tekniskt och organisatoriskt. Vad som är en lämplig säkerhetsnivå beror på bland annat riskerna med behandlingen, vilken typ av uppgifter som behandlas, på de tekniska möjligheter som finns och på kostnaderna.

Vid riskbedömningen ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet risken för 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.

Pseudonymisering och kryptering av personuppgifter är exempel på åtgärder som minskar risken med behandlingen. Pseudonymiserade personuppgifter kan inte kopplas till en specifik individ utan att man använder kompletterande information. Den kompletterande informationen måste förvaras tekniskt och organisatoriskt avskild så att personuppgifterna inte kan hänföras till en person.

19. Tvister

19.1. Om bolaget är i arbetsrättslig tvist med facket eller en anställd så hanteras ju personuppgifter med stöd av den lagliga grunden ”rättslig förpliktelse”. Inbegriper denna lagliga grund all personuppgiftshantering som har med tvisten att göra, även intern administration som visserligen inte utgör en rättslig förpliktelse, men som ofta är nödvändig del av rutinerna vid tvist? Eller ska behandlingen delas upp och olika lagliga grunder tillämpas på olika behandlingar?

All personuppgiftsbehandling som är nödvändig för att uppfylla ändamålet faller in under samma rättsliga grund.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

Arkitektkopia AB, Bromma, 2018