

*Datainspektionen
informerar*



Personuppgifter i arbetslivet

7

Ändringar i PuL

Observera att innehållet i den här skriften inte är anpassat till de ändringar i PuL som trädde i kraft den 1 januari 2007. Ändringar förs in i nästa upplaga. Här följer en kortfattad beskrivning av vad förändringarna i PuL innebär.

PuL innehåller numera två olika regelsystem. Som tidigare innehåller lagen ett antal detaljerade hanteringsregler (närmare 50 paragrafer), till exempel grundläggande krav som ska vara uppfyllda då personuppgifter behandlas, bestämmelser om vad som är tillåten behandling och om skyldighet att informera de registrerade. Dessa regler gäller för behandling av personuppgifter i strukturerat material som traditionella dataregister, databaser och ärende- och dokumenthanteringssystem. För behandling av personuppgifter i ostrukturerat material som löpande text och ljud och bild gäller en helt ny och förenklad reglering.

Den 1 januari 2007 infördes dessa lättnader i PuL. De innebär att många av hanteringsreglerna inte längre behöver tillämpas på viss hantering av personuppgifter i ett ostrukturerat material. Syftet är att underlätta vardaglig hantering av personuppgifter som inte medför integritetsrisker. Lättnaderna gäller för vardaglig ostrukturerad behandling av personuppgifter som löpande text i ordbehandlingsystem, löpande text på Internet, ljud- och bildupptagningar och korrespondens per e-post. Undantaget kan också omfatta enkla strukturer som klasslistor och listor över anställda – om inte materialet ingår i eller ska infogas i en databas med en personuppgiftsanknuten struktur, till exempel ett ärendehanteringssystem.

Den förenklade regleringen innebär att vardaglig ostrukturerad behandling i princip får utföras fritt så länge man inte kränker den uppgifterna avser. Kränkande behandling är således fortfarande otillåten. För att avgöra om en behandling är kränkande måste man göra en samlad bedömning av hur känsliga uppgifterna är, i vilket samman-

hang de förekommer, för vilket syfte de behandlas, vilken spridning de har fått eller riskerar att få, samt vad behandlingen kan leda till. Man får således göra en avvägning i det enskilda fallet där den registrerades intresse av en fredad, privat sfär vägs mot andra motstående intressen.

Vid behandling av personuppgifter i regelrätta register eller andra samlingar av personuppgifter som är ordnade så att det ska bli enklare att söka efter eller sammanställa personuppgifter, till exempel databaser eller stora dokument- och ärendehanteringssystem gäller fortfarande hanteringsreglerna för alla personuppgifter i systemet.

Frågor och svar om vad ändringarna i PuL innebär finns på www.datainspektionen.se.



Datainspektionen

Besöksadress: Fleminggatan 14, Plan 9
Postadress: Box 8114, 104 20 Stockholm
Tfn: 08-657 61 00 Fax: 08-652 86 52
E-post: datainspektionen@datainspektionen.se
Webbplats: www.datainspektionen.se

Innehåll

Definitioner	4
Inledning	5
När tillämpas PuL?	6
Vem är personuppgiftsansvarig?	7
Vad innebär ansvaret?	8
<i>Sanktioner</i>	8
<i>Skadestånd</i>	9
Grundläggande bestämmelser	9
Informationsskyldigheten	11
När får en arbetsgivare behandla personuppgifter?	11
<i>På grund av avtal</i>	12
<i>På grund av en rättslig skyldighet</i>	12
<i>För att skydda vitala intressen</i>	13
<i>Efter en intresseavvägning</i>	13
Känsliga uppgifter	13
<i>På grund av skyldighet eller rättighet inom arbetsrätten</i> ...	13
<i>För att hävda rättsliga anspråk</i>	14
Med arbetstagarens samtycke	15
<i>Giltigt samtycke?</i>	15
<i>Om samtycket återkallats</i>	16
Känsliga uppgifter	16
Brottsuppgifter	17
Personnummer	18
Kontroll och övervakning m.m	18
<i>Arbetstagares prestationer</i>	18
<i>Rekryteringssystem och kompetensdatabaser</i>	19
<i>Regler för användningen av IT-systemet</i>	19
<i>Loggning</i>	20
<i>Kameraövervakning</i>	21
Utlämnande av personuppgifter till utlandet	22
<i>Internet</i>	23
Arbetsgivare i offentlig verksamhet	24
Säkerhet	25
Anmälan till Datainspektionen	25
Personuppgiftsombud	26
Datainspektionens tillsyn	26

Den här skriften innehåller information om hur personuppgifter i arbetslivet får behandlas enligt personuppgiftslagen (1998:204), PuL. Skriften omfattar behandling av personuppgifter inom både privat och offentlig sektor. I vissa fall kan särskilda regler gälla för arbetsgivare i offentlig verksamhet. Dessa behandlas i ett särskilt avsnitt.

När det talas om arbetstagare avses i vissa fall även arbetssökande.

Datainspektionens allmänna råd ”Personuppgifter i arbetslivet” (1992) upphörde att gälla den 1 oktober 2001. De synsätt som kommer till uttryck i de allmänna råden kan ofta utgöra en utgångspunkt också vid en integritetsbedömning enligt PuL.

Den s.k. Integritetsutredningen (Dir.1999:73) arbetar med en översyn av behovet av lagstiftning eller andra åtgärder för att stärka skyddet av den enskildes personliga integritet i arbetslivet. Uppdraget beräknas vara slutfört den 31 december 2001.

Stockholm den 1 oktober 2001

De skrifter och informationsblad som texten hänvisar till kan hämtas på www.datainspektionen.se. Tryckta utgåvor kan beställas per telefon 08-657 61 42 eller via webbplatsen.

Definitioner

Personuppgifter är all slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Även bild- och ljuduppgifter om en fysisk person räknas som personuppgifter, även om inga namn nämns. Krypterade uppgifter och olika slag av elektroniska identiteter omfattas också av PuL om uppgifterna direkt eller indirekt kan kopplas till fysiska personer.

Känsliga personuppgifter är personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt sådana personuppgifter som rör hälsa eller sexualliv.

Behandling av personuppgifter är varje åtgärd eller serie av åtgärder som utförs med personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex.

- insamling
- registrering
- lagring
- bearbetning eller ändring
- utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter
- sammanställning eller samkörning.

(Se också avsnittet *När tillämpas PuL?* s. 6).

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen, dvs. syftet med, och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

(Se också avsnittet *Vem är personuppgiftsansvarig?* s. 7).

Den registrerade är den som en personuppgift avser.

Samtycke är varje slag av otvetydig viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom eller henne. Samtycket ska vara

- frivilligt
- särskilt
- informerat, dvs. lämnat efter det att information om behandlingen har lämnats (informerat samtycke).

Inledning

I arbetslivet används personuppgifter i många olika sammanhang. När uppgifterna ADB-behandlas måste integritetsfrågorna beaktas. Vissa typer av personuppgifter anser de flesta av oss vara integritetskänsliga, t.ex. uppgifter om hälsa och sexualliv. Ibland kan en person uppleva behandling av personuppgifter som ett integritetsintrång, t.ex. om information som behandlas om honom eller henne är mycket detaljerad. Målsättningen är att finna en rimlig balans mellan en arbetsgivares behov av att behandla personuppgifter och den enskildes anspråk på integritet. När man bedömer om en behandling av personuppgifter i arbetslivet är tillåten bör man tänka på att en arbetstagare i allmänhet befinner sig i en beroendeställning i förhållande till arbetsgivaren. Ett samtycke till en viss behandling kan kanske därför inte alltid ges samma betydelse som i andra sammanhang.

Någon lagstiftning som direkt avser behandling av personuppgifter inom arbetslivet finns inte. Arbetstagares integritet i arbetslivet regleras genom arbetsrättslig lagstiftning och genom bestämmelser i kollektivavtal. Preciseringar finns t.ex. i Arbetsmiljöverkets föreskrifter och allmänna råd, i domstolsavgöranden (praxis) och i riktlinjer som skapas på arbetsmarknaden och anses uttrycka god sed i arbetslivet. Det grundläggande skyddet för den enskildes personliga integritet vid registrering finns i 2 kap. 3 § andra stycket regeringsför-

men. Där sägs att varje medborgare ska – i den utsträckning som närmare anges i lag – skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av ADB. De bestämmelser som äsyftas är i första hand personuppgiftslagen, PuL.

De licenser, tillstånd och föreskrifter som Datainspektionen har meddelat enligt datalagen upphörde att gälla den 1 oktober 2001. PuL ställer inte något krav på licens eller tillstånd från Datainspektionen för att få behandla personuppgifter. I stället ansvarar den *personuppgiftsansvarige* självständigt för att behandling av personuppgifter görs enligt lagen. Det är alltså arbetsgivaren som beslutar om vem eller vilka som har rätt att behandla personuppgifter och som ansvarar för att behandlingen är laglig. Detta gäller även om någon annan har fått till uppgift att utföra själva registreringen, t.ex. en servicebyrå. Datainspektionen är *tillsynsmyndighet* och övervakar tillämpningen av bestämmelserna.

När tillämpas PuL?

PuL tillämpas på all behandling av personuppgifter som utförs helt eller delvis med hjälp av datorer. Uppgifterna behöver inte finnas i ett register utan även behandling av personuppgifter i löpande text omfattas.

Även manuell behandling av personuppgifter (manuellt register) omfattas av lagen om uppgifterna är sorterade enligt något slags system som gör det möjligt att söka bland uppgifterna.

Bestämmelserna gäller inte för privat behandling av personuppgifter, t.ex. när man för en elektronisk dagbok eller ett adressregister av privat natur. Enskilda personers privata ord- och textbehandling och kommunikation med elektronisk post faller som regel också utanför lagen. Däremot kan publicering på Internet av andras personuppgifter inte betraktas som en privat behandling eftersom uppgifterna kan bli tillgängliga över hela världen.

Utgångspunkten är att PuL ska tillämpas på all behandling av personuppgifter som utförs i Sverige. Det gäller även om den personuppgiftsansvarige kommer från en stat som inte ingår i Europeiska unionen eller är ansluten till Europeiska ekonomiska samarbetsområdet.

Om det finns bestämmelser i en annan lag eller förordning om behandling av personuppgifter som avviker från PuL, s.k. *registerförfattning*, ska de bestämmelserna tillämpas i stället.

Vem är personuppgiftsansvarig?

Personuppgiftsansvarig är normalt den juridiska person (t.ex. aktiebolag, stiftelse, förening) eller den myndighet som bestämmer *vilka* personuppgifter som ska behandlas i verksamheten och *vad* uppgifterna ska användas till. Det är alltså inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig. Även en fysisk person kan vara personuppgiftsansvarig, t.ex. en enskild företagare.

Om flera juridiska personer i en organisation, t.ex. en koncern, behöver behandla samma personuppgifter kan organisationen vara sådan att moderbolaget ensamt är personuppgiftsansvarig för behandlingen. En annan möjlighet är att varje bolag inom koncernen är personuppgiftsansvarig för behandlingen av uppgifter om anställda i bolaget. Man kan även tänka sig att alla bolag inom koncernen är gemensamt personuppgiftsansvariga för ett gemensamt register.

Den personuppgiftsansvarige kan låta någon annan utföra den faktiska behandlingen av personuppgifter genom att anlita ett *personuppgiftsbiträde*, t.ex. en servicebyrå. Personuppgiftsansvaret kan däremot aldrig överlätas. Ett personuppgiftsbiträde finns alltid utanför den egna organisationen. En anställd som behandlar personuppgifter för arbetsgivarens räkning är alltså *inte* personuppgiftsbiträde.

(Se även Datainspektionens informationsblad *Personuppgiftsansvar*).

Vad innebär ansvaret?

Den personuppgiftsansvarige, dvs. arbetsgivaren, ansvarar för att inga otillåtna behandlingar av personuppgifter utförs på arbetsplatsen och kan bli ansvarig för skador som de anställda orsakar genom lagstridig behandling av personuppgifter. Arbetsgivaren måste därför se till att all behandling av personuppgifter på arbetsplatsen uppfyller de krav som föreskrivs i lagar, förordningar och föreskrifter, t.ex. vad gäller ändamål med behandlingen, gallring och bevarande samt säkerhet. En del av detta ansvar kan vara att utforma interna regler som beskriver de personuppgiftsbehandlingar som arbetsgivaren har bestämt för verksamheten och att utforma behörighetsregler för de anställda. Reglernas innehåll kan dokumenteras i personalhandböcker eller liknande. Information eller utbildning om reglerna behövs som regel också.

Sanktioner

PuL innehåller regler om straff – böter eller fängelse i högst sex månader – för den som bryter mot bestämmelser i lagen. Det straffrättsliga ansvaret utkrävs av den fysiska person hos den personuppgiftsansvarige som har gjort sig skyldig till överträdelsen. Vem detta är får avgöras mot bakgrund av omständigheterna i det enskilda fallet och av allmänna straffrättsliga regler. Till straff döms den som

- Lämnar osann uppgift i information till registrerade eller i anmälan och information till Datainspektionen.
- Behandlar känsliga personuppgifter eller uppgifter om brott m.m. i strid med bestämmelserna i lagen.
- För över personuppgifter till tredje land i strid med bestämmelserna i lagen.
- Låter bli att göra en anmälan om behandling till Datainspektionen när sådan krävs.

Är brottet grovt är straffet fängelse i högst två år. I ringa fall döms inte till straff.

Skadestånd

En arbetsgivare som behandlar personuppgifter i strid med PuL ska ersätta arbetstagaren för skada och kränkning av den personliga integriteten som behandlingen har orsakat. Dessutom kan ideell ersättning utgå för själva kränkningen. Om arbetsgivaren visar att felet inte berodde på denne, kan ersättningsskyldigheten sättas ned eller helt falla bort i den omfattning det är skäligt.

Även om arbetsgivaren har överlåtit den faktiska behandlingen av personuppgifter till t.ex. ett personuppgiftsbiträde, kan personuppgiftsansvaret aldrig överlåtas. Det är alltid arbetsgivaren som ytterst ansvarar för att PuL följs och som kan bli skadeståndsskyldig.

Grundläggande bestämmelser

All behandling av personuppgifter måste vara *laglig* och ska dessutom utföras på ett *korrekt sätt* och i enlighet med *god sed* på arbetsmarknaden. Man bör sträva efter att i första hand samla in personuppgifter från arbetstagaren själv.

Personuppgifter får bara behandlas för *särskilda, uttryckligt angivna och berättigade ändamål eller syften*. Arbetsgivaren måste därför bestämma ett ändamål för varje typ av behandling, t.ex. personaladministration, behörighetskontroll, utbildning, säkerhets-, beredskaps- och katastrofplanering. Uppgifter som har samlats in för ett visst syfte, t.ex. personaladministration, får sedan inte behandlas för något syfte som är *oförenligt* med det man samlade in uppgifterna för, t.ex. prestationsmätning.

Ändamålet bör beskrivas så noggrant som möjligt eftersom det bestämmer ramen för vilka personuppgifter som får behandlas. Detta ska göras innan man börjar att samla in personuppgifter. Man kan ange flera ändamål samtidigt. Det ställs inte krav på att ändamålen ska skrivas ned. För att undvika tvister och förenkla arbetet med att lämna information

till de registrerade kan det ändå vara en fördel att skriftligt dokumentera ändamålet eller ändamålen.

Om personuppgifterna ska lämnas vidare till någon annan krävs att även utlämnandet är förenligt med de ursprungliga ändamålen. T.ex. innebär sambearbetning av två eller flera register med olika ändamål i allmänhet att ett eller flera nya register med nya ändamål skapas.

Man får bara behandla uppgifter som är *adekvata och relevanta* i förhållande till ändamålet med behandlingen. Det betyder att uppgifterna måste ha någon faktisk betydelse för det ändamål som har bestämts för behandlingen. T.ex. får en arbetsgivare bara behandla de personuppgifter om en arbetssökande som behövs för att bedöma lämpligheten för den sökta anställningen.

Personuppgifter ska hålla så *hög kvalitet* som möjligt. Arbetsgivaren måste därför se till att det finns tydliga *rutiner för uppdatering och gallring* av uppgifter om arbetstagare. Uppgifter får inte bevaras längre än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Ändamålet är alltså utgångspunkten för bedömningen av när uppgifter ska bevaras eller gallras. Vissa typer av uppgifter bör gallras så snart som möjligt. Ibland krävs det att uppgifterna bevaras under en längre tid, t.ex. på grund av bestämmelser i lag eller för att de behövs för utbetalning av t.ex. pension från arbetsgivaren.

Personuppgifter som lämnas vid en ansökan om anställning bör normalt gallras när anställningsförfarandet har avslutats. Vill arbetsgivaren använda uppgifterna längre måste den arbetssökande informeras och samtycka till fortsatt registrering.

En offentlig arbetsgivare måste under vissa förhållanden behålla uppgifter om en arbetssökande, t.ex. vid ett överklagande av ett beslut att inte anställa sökanden. Arbetsgivaren kan behöva uppgifterna för att styrka att ansökan har behandlats på rätt sätt.

Informationsskyldigheten

PuL ställer stora krav på att de registrerade informeras om *vilka* personuppgifter som samlas in och *vad* uppgifterna ska användas till. Detta gäller vid all behandling av personuppgifter, oavsett på vilken grund uppgifterna behandlas. För att ett samtycke till behandling ska vara giltigt måste arbetstagaren ha fått sådan information att han eller hon kan bedöma för- och nackdelarna med att de aktuella personuppgifterna behandlas. Informationen och samtycket måste gälla en *viss behandling* som rör arbetstagaren och som utförs av en viss arbetsgivare för bestämda syften.

Arbetsgivaren bör i första hand samla in personuppgifter direkt från arbetstagaren. Om uppgifter samlas in från något annat håll ska arbetsgivaren normalt informera arbetstagaren om vilka uppgifter som samlas in och varför. I vissa fall, t.ex. om uppgifterna är känsliga, måste uttryckligt samtycke inhämtas.

Se även Datainspektionens allmänna råd "*Information till registrerade enligt PuL*".

När får en arbetsgivare behandla personuppgifter?

För att en arbetsgivare ska få behandla personuppgifter krävs att behandlingen är *nödvändig för att uppfylla vissa syften* som nämns i PuL. En förutsättning är att de grundläggande krav som ställs på all behandling av personuppgifter är uppfyllda, t.ex. att ändamålet med behandlingen är tydligt beskrivet i förväg och sakligt grundat i verksamheten och att de personuppgifter som behandlas har betydelse för arbetsförhållandet (se avsnittet *Grundläggande bestämmelser* s. 9).

För *känsliga* personuppgifter, uppgifter om *brott* m.m. och *personnummer* finns det ytterligare bestämmelser om när

behandling är tillåten. Det finns också särskilda regler för hur personuppgifter får överföras till utlandet (se avsnittet *Utlämnande av personuppgifter till utlandet* s. 22).

På grund av avtal

Personuppgifter får behandlas om det är *nödvändigt* för att *anställningsavtalet eller något annat avtal* mellan arbetsgivaren och arbetstagaren ska kunna uppfyllas. Detsamma gäller för att åtgärder som den registrerade har begärt ska kunna vidtas innan ett avtal träffas. Avtalet måste ha ingåtts med arbetstagaren själv. Ett avtal mellan arbetsgivaren och en juridisk person, t.ex. ett bemanningsföretag, innebär alltså inte att uppgifter får behandlas om personer som är anställda hos bemanningsföretaget. Personuppgifter som behövs för att administrera ett anställningsavtal kan t.ex. vara

- personaladministrativa system, dvs. system för löneberäkning, registrering av sjukfrånvaro,
- in- och utpasseringssystem,
- flextidssystem,
- behörighetskontrollsystem, eller
- företagshälsövård.

Uppgifter om betyg, omdömen eller andra värderande upplysningar, t.ex. från utvecklingssamtal med den anställde, får registreras om det behövs för anställningsförhållandet. Samma gäller uppgifter om prestationer, t.ex. om uppgifterna behövs för att uppfylla skyldigheter enligt ett ackordslöneavtal eller något annat avtalat prestationsbaserat lönesystem (se avsnittet *Arbetstagares prestationer* s. 18).

På grund av en rättslig skyldighet

En arbetsgivare får behandla personuppgifter om det är *nödväntigt* för att fullgöra *en rättslig skyldighet*. Arbetsgivare är enligt ett flertal lagar och förordningar skyldiga att lämna ut uppgifter om anställda till bl.a. statliga och kommunala myn-

digheter. En sådan skyldighet ger arbetsgivaren rätt att samla in och registrera *nödvändiga* personuppgifter. Som exempel kan nämnas uppgifter som behövs för att

- redovisa skatter och avgifter beträffande arbetstagarna,
- erlægga gruppliv- och pensionsavgifter till försäkringsbolag,
- upprätta listor över anställda p.g.a. de civilrättsliga turordningsbestämmelserna.

Det kan också finnas krav på personuppgiftsbehandling i arbetarskyddslagstiftningen. T.ex. kan hälsoundersökningar av arbetstagare krävas för anställningen.

För att skydda vitala intressen

En arbetsgivare får behandla personuppgifter om det är *nöd-vändigt* för att skydda arbetstagaren, dvs. i situationer som innebär fara för liv och hälsa.

Efter en intresseavvägning

En arbetsgivare får behandla personuppgifter om det är *nöd-vändigt* och intresset av att behandla uppgifterna är större än den anställdes intresse av att uppgifterna inte behandlas. Hur en sådan intresseavvägning utfaller beror bl.a. på förhållandena på den aktuella arbetsplatsen. Vägledande bör vara att arbetsledningsrätten inte får utövas godtyckligt eller kränkande eller på ett sätt som strider mot lag eller god sed på arbetsmarknaden.

Känsliga uppgifter

En arbetsgivare får bara behandla känsliga personuppgifter i vissa undantagsfall. Sådana uppgifter får aldrig behandlas efter en intresseavvägning.

På grund av skyldighet eller rättighet inom arbetsrätten

En arbetsgivare får behandla känsliga personuppgifter om

det krävs för att fullgöra skyldigheter eller utöva rättigheter inom *arbetsrätten*. Härmed avses i stort sett alla skyldigheter och rättigheter som en arbetsgivare har gentemot sina arbetstagare och deras fackliga organisationer. Som *exempel* kan nämnas när uppgifter om anställdas sjukdom behandlas för att beräkna sjuklön, utreda frånvarorätt eller inleda en rehabiliteringsutredning enligt arbetsmiljölagen. Ytterligare exempel är när uppgifter om fackligt medlemskap registreras på grund av att arbetsgivaren har åtagit sig att göra avdrag på lön för fackföreningsavgift. Arbetsgivarens s.k. primära förhandlingsskyldighet enligt 11 § MBL kan också ge rätt att behandla känsliga personuppgifter.

De känsliga personuppgifterna får bara *lämnas vidare* till någon annan om arbetstagaren uttryckligen har samtyckt till det eller när det finns en sådan skyldighet inom arbetsrätten. Det kan t.ex. röra sig om uppgifter för gruppliv- och pensionsavgifter som lämnas till försäkringsbolag eller uppgifter som krävs för att uppfylla förhandlingsskyldigheten i 11 § MBL. Det innebär bl.a att en arbetsgivare inte utan vidare får lämna ut uppgifter om en tidigare arbetstagares sjukfrånvaro till en annan arbetsgivare.

Behandling av uppgifter som har kommit fram vid undersökning, behandling och vård inom *företagshälsövården* regleras särskilt genom patientjournallagen och vårdregisterlagen. Arbetsgivaren får inte registrera uppgifter om provsvar, diagnoser etc. i sina personaladministrativa system. Uppgifter om t.ex. vaccinering som krävs i tjänsten får däremot registreras.

För att hävda rättsliga anspråk

En arbetsgivare får behandla känsliga personuppgifter när det behövs för att utreda, göra gällande eller försvara ett *rättsligt anspråk*. Exempel på sådana behandlingar är

- uppgift om medlemskap i fackförening för att fastställa var en talan i domstol ska väckas eller föras,

- rätt till skatteavdrag för fackföreningsavgift, eller
- rätt till socialbidrag för fackföreningsavgift.

Med arbetstagarens samtycke

Är inget av villkoren ovan för att få behandla personuppgifter uppfyllt kan en arbetsgivare ha rätt att utföra behandlingen med samtycke av arbetstagaren. En förutsättning är att de *grundläggande krav* som ställs på all behandling av personuppgifter (se s. 9) har iakttagits när uppgifterna samlades in, t.ex. att de är relevanta för registrets ändamål, och att kraven uppfylls under den fortsatta behandlingen av uppgifterna.

Om samtycke har lämnats kan känsliga personuppgifter (se nedan) och personnummer få behandlas. Uppgifter kan också få lämnas ut till tredje land. Brottsuppgifter får däremot inte behandlas ens med samtycke, se avsnittet *Brottsuppgifter*, s. 17.

Giltigt samtycke?

Ett samtycke till att behandla personuppgifter ska vara frivilligt, uttryckligt och informerat (se avsnittet *Definitioner*, s. 4). Det kan lämnas muntligt eller skriftligt. Skriver man in sina personuppgifter i ett datasystem efter att ha fått information om vad uppgifterna ska användas till anses man också ha samtyckt. Däremot är det inte tillräckligt att arbetsgivaren *antar* att arbetstagaren samtycker till en behandling av personuppgifter.

När man bedömer om kravet på frivilligt samtycke är uppfyllt måste man särskilt tänka på den beroende ställning som en arbetstagare ofta befinner sig i förhållande till arbetsgivaren. Behandling av personuppgifter i arbetslivet med stöd av samtycke begränsas till sådana situationer där arbetstagaren har ett verkligt fritt val och senare kan ta tillbaka sitt samtycke utan att det medför några nackdelar för honom eller henne.

För att undvika eventuella tvister om samtycket kan det vara bra om det ges skriftligt, t.ex. på ett formulär som samtidigt

innehåller den information som ska lämnas till den registrerade.

Man kan inte samtycka generellt till behandling av personuppgifter, t.ex. till 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.

Ett ombud som har fått fullmakt att företräda en arbetstagare kan lämna dennes samtycke. Arbetstagaren behöver i så fall inte ha fått någon egen information om behandlingen. En facklig organisation kan t.ex. samla in samtycke från varje medlem och lämna dessa vidare till arbetsgivaren. Däremot kan organisationen inte samtycka för medlemmarnas räkning.

Om samtycket återkallats

Ett samtycke kan när som helst tas tillbaka. Detta kan göras skriftligt eller muntligt. Därefter får bara redan insamlade personuppgifter behandlas. Eftersom uppgifterna inte får uppdateras eller kompletteras utan samtycke kan de dock bli för gamla för att få användas (jfr. de grundläggande kraven på att uppgifterna ska vara aktuella).

Känsliga uppgifter

Känsliga personuppgifter (se avsnittet *Definitioner* s. 4), t.ex. uppgifter om sjukdom, kan få behandlas med ett *klart uttalat samtycke*. Samma gäller om känsliga personuppgifter ska lämnas vidare till någon annan utan att det finns en arbetsrättslig skyldighet att lämna ut uppgifterna. Är uppgifterna känsliga är det naturligtvis särskilt viktigt att tänka på att kraven på ett giltigt samtycke är uppfyllda.

Personuppgifter som är känsliga får också behandlas om arbetstagaren själv har *offentliggjort* den känsliga uppgiften på ett tydligt sätt, t.ex. medlemskap i fackförening genom att aktivt verka för föreningen på arbetsplatsen.

Brottsuppgifter

Det är förbjudet för arbetsgivare som inte är myndigheter att behandla personuppgifter om lagöverträdelser, dvs. uppgifter om brott, domar i brottmål, straffprocessuella tvångsmedel (t.ex. häktning) eller administrativa frihetsberövanden (olika former av tvångsingripande med stöd av lag). En uppgift om att någon har eller misstänks ha begått ett *visst brott* är en sådan uppgift om lagöverträdelse som omfattas av förbudet. Någon dom eller liknande beträffande brottet krävs inte. Ett samtycke från arbetstagaren ger inte arbetsgivaren rätt att frångå förbudet. Däremot kan det finnas särskilda bestämmelser i lag eller annan författning eller ett myndighetstillstånd i enskilt fall som tillåter behandling av detta slags uppgifter. Uppgifter om brott, brottmålsdomar och liknande får behandlas om behandlingen avser en enstaka personuppgift som är nödvändig för att kunna fastställa, göra gällande eller försvara ett rättsligt anspråk i ett särskilt fall, t.ex. ett skadeståndsanspråk. Brottsuppgifter får också behandlas om det krävs för att kunna fullgöra en anmälningsskyldighet enligt lag, t.ex. att göra en polisanmälan.

Det förekommer att arbetsgivare vid en anställningsintervju ställer frågor om brottslighet eller kräver att den arbetsökande visar upp ett intyg ur polisens belastningsregister. Registrering av sådana uppgifter som inte har stöd i lag eller annan författning (se t.ex. lagen (2000:873) om registerkontroll av personal inom förskoleverksamhet, skola och barnomsorg) står i strid med PuL.

Personnummer

Uppgift om personnummer får behandlas med arbetstagarens samtycke eller när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller av något annat beaktansvärt skäl. En arbetsgivare får t.ex. registrera personnummer för att *administrera sina anställda* eller för att *fullgöra uppgiftsskyldighet* till olika myndigheter, t.ex. skattemyndigheten. Däremot finns det sällan anledning att behandla personnummer genom utskrift på tjänstgöringslistor och adressetiketter.

Kontroll och övervakning m.m

Arbetstagares prestationer

Uppgifter om *betyg, omdömen eller andra värderande upplysningar*, t.ex. från utvecklingssamtal med arbetstagaren, får registreras om det är *nödväntigt* för att administrera anställningsavtalet eller för att uppfylla rättsliga skyldigheter.

Behandling av personuppgifter för ändamål som innebär *individuell prestationsmätning* är tillåten om den är *nödväntig* och utförs för att uppfylla anställningsavtalet, t. ex. för beräkning och utbetalning av lön. Uppgifter av detta slag kan också få behandlas efter en intresseavvägning. Hur denna utfaller är beroende av omständigheterna på den aktuella arbetsplatsen, t.ex. för vilket ändamål mätningen utförs, hur den genomförs, hur resultatet används och vilka eventuella överenskommelser som kan finnas på arbetsplatsen. Vägledande vid bedömningen är också om behandlingen följer vad som kan anses vara normalt tillämpligt förfarande och i enlighet med god sed på arbetsmarknaden. Behandlingen kan också vara tillåten om arbetstagaren har lämnat ett giltigt samtycke till den.

I samtliga fall måste de grundläggande kraven på all behandling av personuppgifter vara uppfyllda. För att behandlingen

ska vara laglig krävs också att arbetsgivaren *har informerat arbetstagaren* om den behandling som ska utföras.

Sammanställningar av uppgifter om de anställda som lagras för att användas för t.ex. fakturering eller bemanningsplanering får inte användas för något annat syfte, t.ex. individuell värdering vid lönesättning.

Uppgifter om resultat från *personlighetstester, profiler* och liknande får bara behandlas med arbetstagarens samtycke. Undantag från denna regel kan finnas i lag eller annan författning.

Rekryteringssystem och kompetensdatabaser

Intern och extern rekrytering av arbetstagare utförs ofta med hjälp av datoriserade rekryteringssystem. Bara sådana uppgifter som är *nödvändiga* för registrets ändamål får behandlas, t.ex. för att bedöma den arbetsökandes lämplighet och karriärmöjligheter.

Om det i lag eller annan författning finns särskilda kompetenskrav för en viss anställning kan det vara nödvändigt för en arbetsgivare att behandla sådana uppgifter. I övrigt får sådana personuppgifter behandlas med arbetstagarens samtycke. För att kravet på informerat samtycke ska vara uppfyllt krävs *information* om hur uppgifterna kommer att behandlas, t.ex. vem som har möjlighet att använda dem och hur länge de kommer att lagras. Detta gäller oavsett på vilket sätt den arbetsökande lämnar sina uppgifter.

Regler för användningen av IT-systemet

Datorer som arbetsgivaren ställer till de anställdas förfogande är arbetsredskap. Med stöd av arbetsledningsrätten har arbetsgivaren rätt att bestämma hur utrustningen på arbetsplatsen får användas. Utgångspunkten är att sådan utrustning i första hand ska användas i arbetet. Detta gäller även e-post och internetabonnemang. Många arbetstagare ges också möjlighet att skicka e-post och använda Internet och andra funktioner av IT-systemet för privat bruk.

Arbetsgivaren ansvarar för organisationens informations-säkerhet och för att inga otillåtna behandlingar av personuppgifter utförs på arbetsplatsen. Denne bör därför utarbeta *regler och riktlinjer* som tydligt talar om vad som gäller för användningen av datorer och datanät. Av reglerna bör det framgå om de anställda har rätt att använda t.ex. e-post och Internet för privata ändamål.

Arbetsgivaren har rätt att *kontrollera* om reglerna följs. All kontroll av anställda måste ha ett i förväg *uttryckligt 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.

Loggning

Logguppgifter registreras ofta av tekniska skäl men förekommer även i en mängd olika situationer, t.ex. vid elektroniska inpasseringskontroller, i telefonväxlar och butikskassor. Genom loggfiler i program kan man t.ex. kontrollera arbetstagares användning av e-post och vilka adresser på Internet denne har besökt. Arbetsgivares möjligheter att genom uppgifter från loggning samla detaljerad information om arbetstagares beteende uppfattas ofta som mycket integritetskänsligt. En behandlingshistorik bör inte utformas eller utnyttjas så att den medför risk för intrång i de anställdas integritet. Ibland är det kanske tillräckligt att övervaka ett systems tekniska funktion eller kontrollera dess användning utan att den enskilde användaren registreras. En behandlingshistorik har också en förebyggande funktion. En förutsättning för detta är dock att de anställda informeras om att det finns en behandlingshistorik och att den kontrolleras.

Om uppgifter som registreras i en loggfil går att knyta till en enskild person är de *personuppgifter*. Samma gäller när särskilda programvaror används för att övervaka enskilda arbetstagares arbetsinsatser eller för att sammanställa arbetstagarnas användning av IT-systemet. Det betyder att bestämmelserna i PuL sätter gränser för vilka personuppgifter som

kan behandlas, på vilken grund de får behandlas, vad de får användas till och vem som ska ha tillgång till dem.

Loggregister får föras av *tekniska eller säkerhetsmässiga skäl*. Det kan också uppställas särskilda krav på loggning på grund av *författningsbestämmelser*, t.ex. för att kontrollera att arbetstagare har *behörighet* till register med känsliga uppgifter och *vilka åtgärder* som har vidtagits. En del registrering och kontroll utförs som en följd av *anställningsavtalet*, t.ex. för beräkning av lön och andra förmåner. I vilken utsträckning insamling av personuppgifter genom loggning kan anses nödvändig för att i övrigt kontrollera att anställningsavtalet fullgörs får avgöras från fall till fall. Uppgifter av detta slag kan också få behandlas efter en intresseavvägning (se avsnittet *Arbetstagares prestationer* s. 18).

Om arbetsgivaren vill logga t.ex. internetanvändningen för att tekniskt övervaka systemet av säkerhetsskäl, får loggen inte senare användas för andra syften, t.ex. kontroll av hur enskilda arbetstagare använder systemet eller deras arbetsprestationer. Om kontroll utförs för andra syften än det ursprungligen bestämda, krävs som huvudregel information och samtycke.

Man måste skilja mellan sådana *filförteckningar* som arbetsgivaren normalt har tillgång till och innehållet i *en enskild fil*. Rätten att kontrollera att uppsatta regler följs innebär som regel inte någon rätt för arbetsgivaren att utan samtycke ta del av innehållet i en enskild fil, t.ex. att läsa privat e-post.

Av intresse är också Arbetarskyddsstyrelsens särskilda föreskrifter om arbete vid bildskärm, AFS 1998:5, 10 §. Av bestämmelsen framgår bl.a. att kvantitativ eller kvalitativ kontroll av arbetstagares arbetsinsats via datasystemet inte får göras utan dennes vetskap.

Kameraövervakning

Användning av kamera för bevakning eller övervakning regleras av *lagen (1998:150) om allmän kameraövervakning*. Om

kameran sitter på en plats dit allmänheten har tillträde krävs som regel tillstånd av länsstyrelsen. På en arbetsplats dit allmänheten inte har tillträde får arbetsgivaren sätta upp såväl kamera som utrustning för ljudupptagning utan tillstånd. De anställda måste alltid informeras om sådan övervakning. Lagen innehåller vissa bestämmelser som syftar till att skydda de övervakades personliga integritet.

Om bilder från en övervakningskamera av en identifierbar person lagras på ett datamedium är det behandling av personuppgifter. Det innebär att bestämmelserna i PuL om när behandling är tillåten kan bli tillämpliga.

Utlämnande av personuppgifter till utlandet

Det är förbjudet att föra över personuppgifter som är under behandling till en stat som inte ingår i Europeiska Unionen eller är ansluten till Europeiska samarbetsområdet. Förbudet omfattar också överföring av personuppgifter för behandling i ett sådant land. Förbudet gäller inte om landet har en adekvat nivå för skyddet av personuppgifterna. Det innebär bl.a. att man vid överföring av personuppgifter inom en koncern måste kontrollera om överföringen är tillåten.

Från överföringsförbudet finns det undantag i PuL och personuppgiftsförordningen (1998:1191). Bl.a. får personuppgifter föras över till tredje land om och i den utsträckning Europeiska gemenskapernas kommission har konstaterat att landet har en adekvat nivå för skyddet av personuppgifter. Kommissionen har meddelat beslut om adekvat skydd av personuppgifter i Schweiz och Ungern samt om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat.

Internet

När personuppgifter publiceras öppet på en webbplats på Internet blir de tillgängliga över hela världen, även i länder som saknar integritetsskydd för personuppgifter. PuL tillåter ändå i vissa fall att personuppgifter läggs ut på webben. En förutsättning för att man ska få föra över personuppgifter till tredje land är att det enligt övriga regler i PuL är tillåtet att över huvud taget behandla uppgifterna.

Det är bara tillåtet att överföra personuppgifter till länder som har ett tillräckligt skydd för informationen (s.k. adekvat skyddsnivå), men harmlös information får publiceras på Internet utan den registrerades samtycke eftersom sådana uppgifter inte kräver något skydd. Vad som i praktiken kan bedömas vara harmlös information måste avgöras från fall till fall. Utgångspunkten bör vara om den enskilde kan uppleva publiceringen som kränkande. Exempel på uppgifter på en arbetsplats som normalt kan publiceras på en webbplats utan arbetstagarens samtycke är namn, befattning, e-postadress och liknande arbetsplatsrelaterade personuppgifter. Vill man däremot lägga ut t.ex. hemadress, hemtelefonnummer eller foton bör man fråga personen först. Observera att namn- och adressuppgifter kan vara skyddade i folkbokföringen genom sekretessbestämmelser.

Om man är osäker på vad arbetstagaren kommer att tycka om publiceringen är det en god regel att inhämta hans eller hennes samtycke (se avsnittet *Giltigt samtycke?* s. 15). Det är viktigt att lämna sådan information att arbetstagaren kan bedöma för- och nackdelar med publiceringen. En arbetsgivare bör bara förlita sig på samtycke i situationer där det inte förorsakar några problem om samtycket senare återkallas. Invänder någon mot att uppgifter om honom eller henne publiceras på Internet, bör uppgifterna inte publiceras även om de för utomstående kan verka harmlösa.

Arbetsgivare i offentlig verksamhet

Särskilda regler gäller för arbetsgivare i offentlig verksamhet. Hos en myndighet är verksamheten reglerad i lagar och andra författningar och ska uppfylla särskilda krav, exempelvis i offentlighetslagstiftningen.

Regeringsformen (2 kap.) ger ett skydd mot att det allmänna, dvs. stat, kommun eller annat offentligt organ, kränker enskildas personliga integritet. Tryckfrihetsförordningen och yttrandefrihetsgrundlagen garanterar vidare offentliganställda s.k. *meddelarfrihet*, dvs. rätt att utan hinder av PuL lämna personuppgifter för offentliggörande i ett skyddat medium.

För personuppgifter hos offentliga arbetsgivare gäller 2 kap. tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet, den s.k. *offentlighetsprincipen*. Principen garanterar var och en att fritt få ta del av allmänna handlingar som är offentliga och som finns hos en myndighet. På grund av offentlighetsprincipen ska personuppgifter i t.ex. ett personregister hos en offentlig arbetsgivare lämnas ut till allmänheten i samma omfattning som traditionella handlingar. Det innebär att många uppgifter om arbetstagare kan bli tillgängliga för vem som helst. Utlämnandet kan dock vara förbjudet på grund av bestämmelser i sekretesslagen som begränsar tillgängligheten till personuppgifter, t.ex. i myndigheternas personalsociala och personaladministrativa verksamhet.

När uppgifter lämnas ut med stöd av offentlighetsprincipen kan arbetsgivaren inte informera arbetstagaren om för vilket ändamål uppgiften lämnas ut eller till vem den lämnas.

Bestämmelser om bevarande och gallring hos statliga och kommunala myndigheter finns i arkivlagen (1990:782). Bestämmelser om arkivvård kan innebära undantag från PuL:s huvudregel om gallring.

Offentlighetsprincipen medför att det i offentlig verksamhet finns särskilda krav på rutiner för att behandla inkommande e-postmeddelanden. Alla e-postmeddelanden hos myndigheter är dock inte allmänna handlingar, t.ex. privata meddelanden och meddelanden inom en facklig organisation. Sådana meddelanden bör gallras bort från databasen. Om en arbetstagare vill spara meddelandet kan det t.ex. placeras i en särskilt markerad ”privat” mapp i databasen.

En arbetsgivare som är myndighet berörs inte av förbudet att behandla brottsuppgifter. Det krävs dock att de grundläggande kraven för att få behandla personuppgifter är uppfyllda.

Säkerhet

Personuppgifter som rör ett anställningsförhållande är ofta integritetskänsliga och ska därför skyddas från insyn av obehöriga. Datainspektionen har utfärdat *allmänna råd om säkerhet för personuppgifter*. Dessa beskriver närmare vilka krav PuL ställer på säkerhet vid behandlingen av personuppgifter.

Anmälan till Datainspektionen

Den personuppgiftsansvarige är skyldig att anmäla sina handlingar av personuppgifter till Datainspektionen. Från anmälningsskyldigheten finns det omfattande undantag enligt PuL, personuppgiftsförordningen och föreskrifter från Datainspektionen. Se Datainspektionens informationsblad *”Anmälan och förhandskontroll”*.

Personuppgiftsombud

PuL innehåller en rad regler som den som är personuppgiftsansvarig måste iaktta för att åstadkomma ett gott skydd för personuppgifter. Den personuppgiftsansvarige bör därför överväga att utse ett *personuppgiftsombud*, som ska anmälas till Datainspektionen. Personuppgiftsombudet ska hjälpa den personuppgiftsansvarige att uppfylla lagens krav och bidra till att skapa ordning och reda. Den som har anmält ett personuppgiftsombud behöver inte anmäla sina behandlingar till Datainspektionen. Se även Datainspektionens informationsblad "*Personuppgiftsombudet*".

Datainspektionens tillsyn

Datainspektionen är tillsynsmyndighet enligt PuL.

Datainspektionen kan genom tillsyn kontrollera om en behandling av personuppgifter är laglig, dvs. att samtliga bestämmelser i PuL följs. Finns annan lagstiftning som reglerar behandlingen, t.ex. patientjournallagen och vårdregisterlagen som reglerar journalföringen inom företagshälsovården, omfattar tillsynen även dessa regler.

Tillsynen kan inledas genom ett klagomål från en arbetstagare eller en facklig organisation, genom uppgifter i massmedia, genom en anmälan om behandling eller genom uppgifter från ett personuppgiftsombud. Tillsynen utförs genom inspektioner på företag eller myndigheter, ofta i form av stickprovskontroller. Datainspektionen kan också begära in en skriftlig redogörelse från den personuppgiftsansvarige. Detta är en vanlig form av tillsyn efter klagomål.

Datainspektionen har rätt att få tillgång till de personuppgifter som behandlas och tillträde till lokaler med anknytning till behandlingen. Upplysningar om och dokumentation av behandlingen, liksom om säkerhetsåtgärder, ska lämnas på inspektionens begäran. Om den personuppgiftsansvarige

inte tillmötesgår begäran kan Datainspektionen besluta om vite.

I första hand ska Datainspektionen åstadkomma rättelse genom påpekanden till den personuppgiftsansvarige om att olaglig personuppgiftsbehandling ska upphöra. Är detta inte möjligt kan inspektionen besluta om vite. Även när den personuppgiftsansvarige inte frivilligt följer ett beslut om säkerhetsåtgärder kan vite föreläggas.

Datainspektionen kan ansöka om utplåning av personuppgifter. Åtgärden är tänkt att användas när det inte genom andra åtgärder är möjligt att förena behandlingen med de regler som gäller. Har t.ex. känsliga personuppgifter behandlats utan att det finns en rätt till behandlingen kan regeln komma till användning (se avsnitten *Känsliga uppgifter*, s. 13 och 14).

Brott mot PuL handläggs av polis och åklagare.

Datainspektionen kan i sin tillsynsverksamhet uppmärksamma polisen på förfaranden som kan misstänkas vara brott mot PuL.

Talan om skadestånd enligt PuL förs hos allmän domstol.



Datainspektionen

Postadress: Box 8114, 104 20 Stockholm

Besöksadress: Fleminggatan 14, Plan 9

Tel: 08-657 61 00 Beställningar: 08-657 61 42 (telefonsvarare)

Fax: 08-652 86 52 e-post: datainspektionen@datainspektionen.se

Webbplats: www.datainspektionen.se