



Vägledning för bolag

Ansvar för personuppgifter som hanteras i system för whistleblowing

FAKTA

Personuppgiftslagen

Personuppgiftslagen (PuL, 1998:204) trädde i kraft 1998 och har till syfte att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas. Personuppgiftslagen bygger på gemensamma regler som har beslutats inom EU, det så kallade dataskyddsdirektivet. Övriga EU-länder har alltså liknande skyddslagar.

Personuppgiftsansvarig

Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Det är alltså *inte* chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig.

Personuppgiftsombud

Den som behandlar personuppgifter kan utse ett personuppgiftsombud som ska se till att personuppgifter behandlas korrekt och lagligt inom verksamheten. Ombudet ska föra en förteckning över vilka behandlingar som utförs och hjälpa registrerade att få felaktiga uppgifter korrigerade. Mer än 6 100 verksamheter har anmält ombud (januari 2009).

Vägledning för bolag

Ansvaret för personuppgifter som hanteras i system för whistleblowing

Oktober 2010

Pris 53 kr, inklusive moms.

Tryckt hos Intellecta infolog i Solna, på Arctic Volume White papper



Miljömärkt trycksak 341077.

Innehåll

Sammanfattning	4
Bakgrund till föreskriften	5
Det här innebär föreskriften	6
Bolaget är ansvarigt	7
Krav i både personuppgiftslagen och föreskriften måste uppfyllas	7
Personuppgiftslagens krav på whistleblowingsystem.	8
Grundläggande krav måste uppfyllas	8
Intresseavvägning ger stöd	8
Känsliga personuppgifter kräver särskilt stöd	9
De som registreras måste informeras	9
Säkerhetsåtgärder ska skydda personuppgifterna	10
Om personuppgifter skickas utanför EU	10
Föreskriftens krav på whistleblowingsystem.	11
Tillstånd krävs om föreskriften inte följs	12
Om reglerna inte följs.	12

Sammanfattning

Genom en ny bestämmelse i **Datainspektionens föreskrift DIFS 2010:1** är det nu möjligt för bolag att behandla uppgifter i whistleblowingsystem utan att ansöka om särskilt tillstånd från Datainspektionen.

I sak gäller dock samma villkor som tidigare för sådana system. Bolag som vill inrätta så kallade whistleblowingsystem, där uppgifter om lagöverträdelser kan förekomma, måste följa bestämmelserna i personuppgiftslagen (PuL) och de särskilda förutsättningar som beskrivs i den nya föreskriften.

Personuppgiftslagens krav innebär bland annat att bolaget måste uppfylla de grundläggande kraven i personuppgiftslagen, ha en laglig grund för behandlingen och lämna tillräcklig information till registrerade.

Villkoren i föreskriften innebär bland annat att rapporteringen endast får omfatta allvarliga oegentligheter som begåtts av personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen.

FAKTA

Vad är ett whistleblowingsystem?

Det finns ingen generell definition av begreppet whistleblowing. Datainspektionen har ansett att begreppet omfattar särskilda rapporteringskanaler som inrättas i syfte att underlätta för anställda att anmäla misstänkta brott mot såväl bolagets egen uppförandekod som mot nationell lag. Sådana rapporteringskanaler kan vara en särskild e-postadress, telefontjänst eller webbplats genom vilka uppgifter om brottsmisstankar avseende enskilda personer samlas in och behandlas. I bolagskoncerner stannar uppgifterna inte alltid hos det bolag där den anmälda personen är anställd utan förs vidare inom koncernen.

Bakgrund till föreskriften

Många bolag tillhandahåller särskilda rapporteringskanaler som anställda kan använda för att rapportera om allvarliga oegentligheter inom bolagen, som exempelvis bokföringsbrott eller mutbrott. Kraven på att bolag ska ha en sådan rapporteringskanal kommer i första hand från USA och från de amerikanska börserna där den typen av system kallas för whistleblowingsystem.

Enligt 21 § personuppgiftslagen (1998:204) är det förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelse. Datainspektionen kan dock meddela undantag från detta förbud, antingen genom särskilda beslut eller i generella föreskrifter.

Sedan 2008 har ett stort antal bolag ansökt om, och beviljats undantag, från 21 § personuppgiftslagen för att behandla personuppgifter om lagöverträdelse i whistleblowingsystem. För att förenkla hanteringen hos bolagen och samtidigt upprätthålla de krav som ställs till skydd för den personliga integriteten har Datainspektionen nu meddelat en generell föreskrift (DIFS 2010:1) som under vissa förutsättningar gör det möjligt att behandla sådana uppgifter utan särskilt beslut från Datainspektionen.

Denna vägledning beskriver vilka regler som gäller för sådan personuppgiftsbehandling.

Den så kallade 29-gruppen (en arbetsgrupp bestående av företrädare för samtliga EU-länders dataskyddsmyndigheter) har också yttrat sig ifråga om vad som bör gälla för whistleblowingsystem mot bakgrund av reglerna i EU:s dataskyddsdirektiv. Yttrandet (WP 117) finns på EU-kommissionens webbplats om dataskydd.

Det här innebär föreskriften

Användning av whistleblowingsystem innebär behandling av personuppgifter i den mening som avses i personuppgiftslagen. Datainspektionen har bedömt att det är fråga om en sådan strukturerad behandling av personuppgifter som omfattas av personuppgiftslagens regler. Det betyder att den personuppgiftsansvarige inte har möjlighet att tillämpa 5 a § personuppgiftslagen.

En uppgift om att någon har eller kan ha begått brott utgör en uppgift om lagöverträdelse även om det inte finns någon dom eller motsvarande beträffande brottet. Enligt 21 § personuppgiftslagen är det förbjudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Förbudet gäller även om den registrerade skulle samtycka till behandlingen.

Trots förbudet i 21 § personuppgiftslagen kan det finnas särskilda situationer när det är berättigat för bolag att behandla sådana personuppgifter. Enligt 9 § personuppgiftsförordningen (1998:1191) får Datainspektionen meddela föreskrifter om undantag från förbudet. Datainspektionen får också besluta om undantag i enskilda fall. De undantag som inspektionen meddelat tidigare i föreskriften DIFS 1998:3 har inte ansetts gälla whistleblowingsystem. Datainspektionen har därför istället, efter ansökan, meddelat särskilda beslut om undantag i enskilda fall. Föreskriften har nu ändrats. Det har införts en ny bestämmelse i punkt f) som rör behandling av brottsuppgifter i whistleblowingsystem. Den nya bestämmelsen gäller från den 1 november 2010. Ändringen framgår av DIFS 2010:1.

Den nya föreskriften innebär att de bolag som vill behandla personuppgifter i whistleblowingsystem inte längre behöver ansöka hos Datainspektionen om ett särskilt undantag från 21 § personuppgiftslagen. Den innebär inte någon ändring i sak beträffande hanteringen av uppgifter i whistleblowingsystem. Föreskriften innehåller samma krav som Datainspektionen tidigare ställde i de enskilda besluten om undantag från förbudet och personuppgiftslagens samtliga bestämmelser måste beaktas vid behandlingen.

För bolag som redan fått beslut om undantag innebär föreskriften ingen ändring. De får fortsätta att behandla uppgifter på samma sätt som tidigare i enlighet med de meddelade besluten.

Bolaget är ansvarigt

Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter är personuppgiftsansvarig i personuppgiftslagens mening (3 § personuppgiftslagen).

Datainspektionen anser att varje bolag är personuppgiftsansvarigt för den insamling och utlämnande av personuppgifter som kan förekomma genom att bolaget ger sina anställda och andra möjlighet att använda ett system för whistleblowing. Genom att bolaget tillhandahåller och anvisar de angivna rapporteringskanalerna för sina anställda anses bolaget bestämma ändamålen och medlen för insamlingen av personuppgifter. Detta personuppgiftsansvar gäller även om uppgifterna slutligen skulle hamna hos något annat bolag i koncernen, som exempelvis moderbolaget. Bolaget är också personuppgiftsansvarigt för den fortsatta behandling av personuppgifter som bolaget kan komma att utföra avseende de lämnade uppgifterna. Detta utesluter inte att även andra bolag i koncernen kan ha ett personuppgiftsansvar för samma uppgifter.

Ofta anlitas en extern part för att ta emot anmälningarna i ett första skede. En sådan extern part är att anse som ett personuppgiftsbiträde och får bara hantera uppgifterna i enlighet med den personuppgiftsansvariges instruktioner (30 § personuppgiftslagen). Det finns också krav på ett skriftligt biträdesavtal, se vidare nedan under rubriken *Säkerhetsåtgärder ska skydda personuppgifterna*.

Krav i både personuppgiftslagen och föreskriften måste uppfyllas

Vid behandling av personuppgifter i whistleblowingsystem måste den personuppgiftsansvarige se till att följa:

- relevanta bestämmelser i personuppgiftslagen samt
- kraven i den generella föreskriften.

Personuppgiftslagens krav på whistleblowingsystem

Grundläggande krav måste uppfyllas

I personuppgiftslagen finns grundläggande krav som alltid måste följas för att personuppgifter ska få behandlas (9 § personuppgiftslagen). För whistleblowingsystem innebär dessa krav bland annat följande:

- Behandlingen får inte vara i strid med svensk arbetsrättslig lagstiftning eller gällande kollektivavtal.
- Behandlingen måste vara i enlighet med god sed på svensk arbetsmarknad.
- Systemet måste inrättas på ett sådant sätt att det inte finns risk för att fler personuppgifter än vad som är nödvändigt eller relevant med hänsyn till ändamålet behandlas, eller att känsliga personuppgifter behandlas i strid med personuppgiftslagen. Detta kan ske genom tydliga användarinstruktioner, utbildning, tekniska begränsningar och tillräckliga säkerhetsåtgärder.
- Uppgifter som samlas in och bevaras måste vara riktiga, adekvata och relevanta. Det innebär att bolaget skyndsamt kan behöva göra en första granskning och bedömning av de inkomna uppgifterna.
- Uppgifter får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. En anmälan som befinner sig utan grund bör tas bort omedelbart. Om en anmälan leder till utredning bör uppgifterna tas bort när utredningen är avslutad eller, om utredningen leder till åtgärder mot den registrerade, när uppgifterna inte längre behövs för detta ändamål.

Intresseavvägning ger stöd

En personuppgiftsansvarig får bara behandla personuppgifter om den registrerade har samtyckt till det eller om behandlingen är nödvändig för vissa ändamål (10 § personuppgiftslagen). Ett sådant ändamål kan vara att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet. Med det avses i första hand en skyldighet som grundar sig på svenska regler eller EU-rättsliga bestämmelser.

Personuppgifter kan få behandlas utan samtycke efter en intresseavvägning, det vill säga om den personuppgiftsansvarige har ett berättigat intresse av att behandla personuppgifterna och detta intresse

väger tyngre än den registrerade personens intresse av skydd för sin personliga integritet.

Datainspektionen anser att behandling av personuppgifter i whistleblowingsystem kan vara tillåten med stöd av en sådan intresseavvägning. I denna avvägning har hänsyn tagits till eventuella skyldigheter i utländsk lagstiftning, som Sarbanes-Oxley-reglerna i USA, men ett berättigat intresse kan finnas även hos bolag som inte lyder under sådana regler.

Känsliga personuppgifter kräver särskilt stöd

Personuppgifter som enligt personuppgiftslagen är känsliga, som exempelvis uppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös övertygelse eller rör hälsa eller sexualliv får bara behandlas under vissa förutsättningar (15–19 §§ personuppgiftslagen). Systemet för whistleblowing måste inrättas på ett sådant sätt att risken för att känsliga personuppgifter behandlas i strid med personuppgiftslagen minimeras.

De som registreras måste informeras

Den personuppgiftsansvarige måste på eget initiativ lämna information om behandlingen till de anställda och andra personer vilkas uppgifter kan komma att behandlas (23–25 §§ personuppgiftslagen). Sådan information kan ges som allmän information, till exempel på den webbplats där information om rapporteringskanalerna samlats.

Informationen bör innehålla uppgifter om:

- vem som är personuppgiftsansvarig för behandlingen samt kontaktuppgifter till denne
- syftet med behandlingen
- vilka typer av uppgifter som behandlas
- att det är frivilligt att göra en anmälan via de särskilda rapporteringskanalerna
- till vilka kategorier av mottagare uppgifterna kan komma att lämnas
- att den registrerade har rätt att begära ett registerutdrag för att kunna kontrollera vilken information som finns registrerad om honom eller henne samt
- att den personuppgiftsansvarige är skyldig att på begäran av den registrerade rätta uppgifter som är felaktiga, ofullständiga eller missvisande.

När uppgifter samlats in ska den som uppgifterna avser också få särskild information om detta. Om det inte är möjligt att ge sådan information på en gång, till exempel för att det skulle kunna äventyra den fortsatta utredningen, kan man dröja med att informera den registrerade till dess att någon sådan fara inte längre föreligger. Den registrerade ska dock informeras så snart som möjligt och senast i samband med att uppgifterna används för att vidta åtgärder som rör honom eller henne.

Information måste också ges till den som begär att få reda på om det finns uppgifter registrerade om honom/henne (26 § personuppgiftslagen). Sådan information ska ges inom en månad och allra senast inom fyra månader efter att ansökan gjordes. Denna information får dock inte innehålla uppgift om identiteten hos den som lämnat anmälan.

Ett bolag får vägra att lämna ut uppgifter till den registrerade i motsvarande fall som avses i offentlighets- och sekretesslagen (2009:400) (27 § personuppgiftslagen).

Säkerhetsåtgärder ska skydda personuppgifterna

Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna (30–31 §§ PuL). Hanteringen av personuppgifterna ska begränsas till endast de personer som hanterar anmälningar och utreder misstänkta oegentligheter. Om ett biträde anlitas för att behandla uppgifterna för den personuppgiftsansvariges räkning ska det finnas ett skriftligt avtal som särskilt föreskriver att biträdet endast får behandla uppgifterna enligt instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de åtgärder som anges i 31 § personuppgiftslagen. För mer information om säkerhet, se Datainspektionens allmänna råd *Säkerhet för personuppgifter* från november 2008 som finns tillgänglig via Datainspektionens webbplats, www.datainspektionen.se.

Om personuppgifter skickas utanför EU

Vid överföring av personuppgifter till tredje land gäller ytterligare krav. Om uppgifter ska skickas till någon annan som är etablerad utanför EU, till exempel ett annat bolag inom koncernen eller ett personuppgiftsbiträde, måste personuppgiftslagens regler om sådan överföring iakttas (33–35 §§ personuppgiftslagen). Det innebär bland annat att det tredje land som mottagaren finns i måste vara godkänt av kommissionen som ett land med adekvat skyddsnivå eller att överföringen regleras av ett avtal som innehåller sådana standardavtalsklausuler som kommissionen godkänt som tillräckliga garantier. För mer information om tredjelandsöverföring se www.datainspektionen.se/tredjeland.

Föreskriftens krav på whistleblowingsystem

I ett whistleblowingsystem behandlas integritetskänslig information. För att en sådan personuppgiftsbehandling ska vara tillåten med stöd av en intresseavvägning måste den personuppgiftsansvarige kunna åberopa starka skäl. Ett whistleblowingsystem bör därför endast användas för sådana oegentligheter som kan få allvarliga konsekvenser för bolaget.

Därför gäller följande begränsningar för whistleblowingsystem:

- Behandling av personuppgifter om lagöverträdelse får endast avse personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen.
- Uppgifter får endast behandlas i systemet om det är sakligt motiverat att behandla uppgifterna för att utreda om personen ifråga varit delaktig i allvarliga oegentligheter.
- Behandlingen får endast avse uppgifter om allvarliga oegentligheter som rör:
 - bokföring, intern bokföringskontroll, revision, bekämpande av mutor, brottslighet inom bank- och finansväsen, eller
 - andra allvarliga oegentligheter som rör bolagets eller koncernens vitala intressen eller enskildas liv och hälsa, som till exempel allvarliga miljöbrott, stora brister i säkerheten på arbetsplatsen och mycket allvarliga former av diskriminering och trakasserier.

Tre av Datainspektionens tidigare beslut i enskilda fall har överklagats ifråga om begränsning under första punkten. Förvaltningsrätten avslag överklagandena. Se till exempel *Förvaltningsrätten i Stockholm dom 2010-03-12 i mål nr 12584-10*.

Vad det innebär att uppgifter endast får behandlas i systemet när det är sakligt motiverat framgår av Datainspektionens tidigare beslut och gäller fortfarande. Systemet får bara användas när det är sakligt motiverat att inte använda bolagets interna informations- och rapporteringskanaler, till exempel om den anmälda ingår i ledningen och de misstänkta oegentligheterna av det skälet annars riskerar att inte tas om hand på vederbörligt sätt. Det innebär också att systemet ska utgöra ett komplement till normal internförvaltning och måste vara frivilligt att använda.

Tillstånd krävs om föreskriften inte följs

Möjligheten att behandla personuppgifter om lagöverträdelser utan att ansöka om tillstånd hos Datainspektionen gäller bara om man följer någon av de generella föreskrifterna i DIFS 2010:1. Om man vill behandla sådana uppgifter på något annat sätt måste man ansöka om ett särskilt undantag från Datainspektionen.

För att behandla andra personuppgifter än brottsuppgifter krävs inget beslut av Datainspektionen, men den personuppgiftsansvarige ansvarar alltid för att se till att personuppgiftslagens regler följs.

Om reglerna inte följs

Att behandla personuppgifter i strid med vissa av personuppgiftslagens regler (inklusive 21 § personuppgiftslagen) är straffbart (49 § personuppgiftslagen). Den registrerade har också rätt till skadestånd för skada och integritetskränkning som orsakats av att personuppgifter har behandlats i strid med personuppgiftslagen (48 § personuppgiftslagen).

Datainspektionen har i uppgift att utöva tillsyn över den personuppgiftsbehandling som sker. Detta kan ske antingen genom inspektioner på plats eller genom skriftliga kontakter. Datainspektionens befogenheter finns angivna i 43-47 §§ personuppgiftslagen.

Kontakta Datainspektionen

E-post: datainspektionen@datainspektionen.se Webb: www.datainspektionen.se
Tfn 08-657 61 00. Postadress: Datainspektionen, Box 8114, 104 20 Stockholm.

