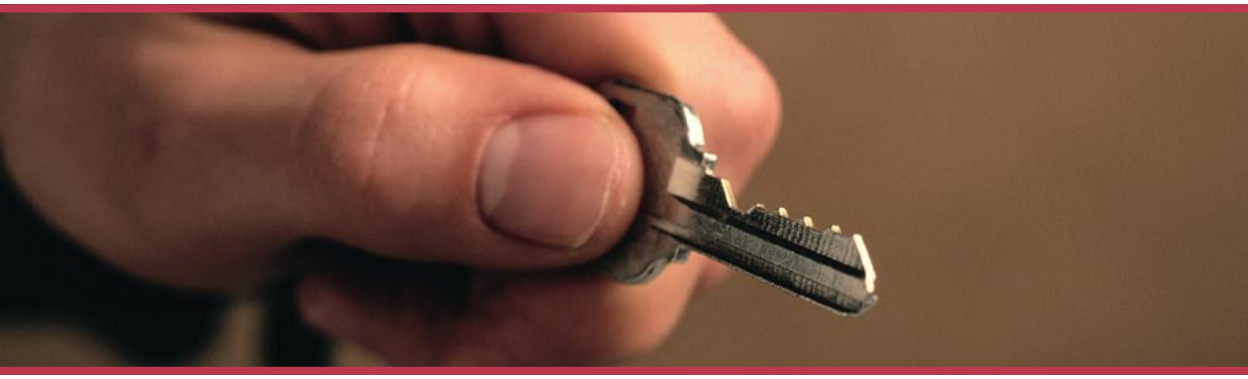
# Säkerhet för person-uppgifter



## Datainspektionens allmänna råd

Reviderad november 2008

Datainspektionen

## Datainspektionens allmänna råd

Vid sidan av lagar och förordningar samt de föreskrifter som Datainspektionen utarbetat, ger vi även ut allmänna råd med rekommendationer i olika frågor. De allmänna råden är inte bindande men de är rekommendationer om hur de bindande kraven i lagarna kan uppnås. Råden ligger också till grund för de föreskrifter som Datainspektionen ger exempelvis i samband med tillsyn och när tillstånd för inkassoverksamhet utfärdas.
De allmänna råden är inte uttömmande och får inte uppfattas så att allt som inte behandlas i råden är tillåtet.

**Av Datainspektionen utgivna Allmänna råd**
Säkerhet för personuppgifter
Information till registrerade
Tillämpning av inkassolagen

De allmänna råden går att beställa eller hämta på Datainspektionens webbplats www.datainspektionen.se

Datainspektionens allmänna råd. Säkerhet för personuppgifter.
Pris 53 kr inklusive moms.
Reviderad i november 2008.
Tryckt hos Lenanders Grafiska (32387), november 2008 på Munken Lynx FSC-certifierat papper. Miljömärkt trycksak 341 145. IISSN 1100-3308.
Har du frågor om innehållet kontakta Datainspektionen, telefon 08-657 61 00,
e-post datainspektionen@datainspektionen.se, eller besök www.datainspektionen.se

# Innehåll

# Förord

Den här skriften innehåller allmänna råd som preciserar personuppgiftslagens (1998:204) krav på säkerhet vid behandling av personuppgifter.

Säkerhetskraven innebär enligt 31 § personuppgiftslagen att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna, och
- hur pass känsliga de behandlade personuppgifterna är.

Råden riktar sig alltså till den som behandlar personuppgifter enligt personuppgiftslagen.

*Stockholm november 2008*

# Inledning

**Säkerhet**

I personuppgiftslagen finns bestämmelser om säkerhet vid behandling av personuppgifter. Syftet med personuppgiftslagen är att skydda människor mot att deras personliga integritet kränks vid behandling av personuppgifter.

Säkerhet är en viktig del av skyddet för den personliga integriteten. Den som behandlar personuppgifter med hjälp av informationsteknik måste därför skydda uppgifterna. En tillfredsställande säkerhet är ett krav enligt personuppgiftslagen.

Många har redan en god säkerhet för att skydda uppgifter, till exempel för att skydda sig mot ekonomiska förluster. Detta är dock inte alltid detsamma som att ha en god säkerhet för att skydda de registrerades integritet.

Råden är inte bindande. De är rekommendationer om hur de bindande kraven i personuppgiftslagen om säkerhet kan uppnås. Enligt personuppgiftslagen får Datainspektionen i enskilda fall besluta om vilka säkerhetsåtgärder som ska vidtas. Bindande föreskrifter om säkerhet kan meddelas till exempel vid behandling av personuppgifter som innebär särskilda risker för otillbörligt intrång i den personliga integriteten eller om inspektionen vid till exempel tillsyn finner brister vid behandling av personuppgifter.

Bedömningen av vilka säkerhetsåtgärder som behövs är beroende bland annat av vilka personuppgifter som behandlas.

Ytterligare åtgärder, som inte nämns i dessa allmänna råd, kan vara nödvändiga för att skydda de personuppgifter som behandlas.

**FAKTA**

**Personuppgifter**
All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

**Behandling av personuppgifter**
Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter till exempel insamling, registrering, organisering, lagring, bearbetning, ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

**Personuppgiftsansvarig**
Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

**Personuppgiftsbiträde**
Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

**Personuppgiftsombud**
Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Utöver Datainspektionens allmänna råd om säkerhet finns Ledningssystem för informationssäkerhet med krav och råd om säkerhet i svensk standard för informationssäkerhet, SS-ISO/IEC 27001 och SS-ISO/IEC 27002 som ingår i ISO 27000-serien.

Datainspektionens allmänna råd om säkerhet innehåller både råd och allmän information. De allmänna råden anges med **fetstil**.

# Ansvaret för säkerheten

**Person-uppgifts-ansvarig**

*Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter*

(3 § personuppgiftslagen)

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 är inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig. Undantagsvis kan en fysisk person vara personuppgiftsansvarig, till exempel en enskild företagare.

Det är de faktiska omständigheterna i det enskilda fallet som avgör vem som är personuppgiftsansvarig, det vill säga vem som faktiskt bestämmer över behandlingen. Avtal där ansvaret preciseras kan ge vägledning vid bedömningen. Om två eller flera gemensamt bestämmer över en viss behandling är de personuppgiftsansvariga tillsammans.

Vem som är personuppgiftsansvarig för en viss behandling kan också särskilt anges i lag eller förordning, till exempel i särskilda registerlagar.

En användare som enbart har rätt att komma åt person-uppgifter genom att läsa dem och söka bland dem, men som inte självständigt får ändra, komplettera eller radera uppgifterna är inte personuppgiftsansvarig.

En juridisk person eller en myndighet är personuppgifts-ansvarig även om verksamheten bedrivs i filialer eller andra organisatoriska enheter.

Om flera juridiska personer i en organisation behöver behandla samma personuppgifter (till exempel föra ett register över alla anställda i en koncern), kan ansvarsfördelningen se ut på olika sätt.

Om moderbolaget ensamt bestämmer över behandlingen blir moderbolaget personuppgiftsansvarig.

För det fall 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.

I en kommun är normalt både kommunstyrelsen och de kommunala nämnderna om de är så självständiga att de är förvaltningsmyndigheter personuppgiftsansvariga, var och en i sin verksamhet. Vilket organ i kommunen som är personuppgiftsansvarig kan inte anges generellt; de faktiska omständigheterna i det enskilda fallet måste beaktas, till exempel om nämnden och dess förvaltning självständigt förfogar över de personuppgifter som behandlas.

Den personuppgiftsansvarige ska enligt 31 § personuppgiftslagen vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av:

- de tekniska möjligheter som finns,
- vad det skulle kosta att genomföra åtgärderna,
- de särskilda risker som finns med behandlingen av personuppgifterna, och
- hur känsliga de behandlade personuppgifterna är.

*Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.*

(3 § personuppgiftslagen)

**Personuppgiftsbiträde**

Med benämningen personuppgiftsbiträde avses alltid någon utanför den egna organisationen. En anställd eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde.

Ett personuppgiftsbiträde kan vara antingen en fysisk eller en juridisk person. Om en personuppgiftsansvarig anlitar till exempel en servicebyrå, blir denna ett personuppgiftsbiträde som får behandla personuppgifter enligt den personuppgiftsansvariges instruktioner.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, ska den personuppgiftsansvarige enligt 31 § personuppgiftslagen förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

Ett personuppgiftsbiträde får behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige och är skyldig att vidta de säkerhetsåtgärder som den personuppgiftsansvarige kräver/instruerar om.

Ett skriftligt avtal som reglerar förhållandet mellan personuppgiftsbiträdet och den personuppgiftsansvarige ska enligt 30 § personuppgiftslagen upprättas. I avtalet ska säkerhetsåtgärderna vid behandlingen av personuppgifter regleras.

Kravet på skriftlighet innebär att avtalet måste vara uttryckt i text, men texten kan finnas på papper eller i elektronisk form. Något krav på att avtalshandlingen ska

vara undertecknad finns inte, men kan ur bevishänseende rekommenderas.

Den personuppgiftsansvarige kan överlåta den faktiska behandlingen av personuppgifter, men personuppgiftsansvaret kan aldrig överlåtas. Det är alltid den personuppgiftsansvarige som ytterst svarar för att personuppgiftslagen följs och att de registrerade behandlas korrekt.

**Personuppgiftsombud**

*Personuppgiftsombud är den fysiska person som den personuppgiftsansvarige har utsett att självständigt se till att personuppgifter behandlas på ett korrekt och lagligt sätt.*

(3 § personuppgiftslagen)

Har personuppgiftsombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, ska personuppgiftsombudet enligt 38 § andra stycket personuppgiftslagen anmäla förhållandet till Datainspektionen.

Även om det finns ett personuppgiftsombud svarar den personuppgiftsansvarige för att det vidtas lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Mer information om ombudets roll och arbetsuppgifter finns på Datainspektionens webbplats www.datainspektionen.se/personuppgiftsombud.

**Övriga personer**

Den eller de personer som arbetar under ledning av den personuppgiftsansvarige eller personuppgiftsbiträdet får behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige eller personuppgiftsbiträdet.

Skada och kränkning av den personliga integriteten som uppkommer till följd av till exempel bristande säkerhet kan leda till skadestånd enligt 48 § personuppgiftslagen.

**Skade-stånd**

# Organisation

**Inledning**

Personalen är den viktigaste resursen i säkerhetsarbetet. Man kan ha bra och dyr teknisk utrustning för säkerhet, men om utrustningen inte används rätt är investeringen bortkastad. Fungerande administrativa rutiner är väl så viktiga som tekniska lösningar.

**Säkerhetspolicy**

**En personuppgiftsansvarig bör, i vart fall om en omfattande behandling av personuppgifter utförs eller om känsliga personuppgifter behandlas, ha en fastställd säkerhetspolicy.**

**I en säkerhetspolicy bör man lämpligen redovisa organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten. En säkerhetspolicy bör vara tydlig samt lätt att förstå och tillämpa i praktiken.**

**Om det finns anställda i verksamheten bör policyn vara skriftlig och allmänt tillgänglig inom organisationen.**

**Säkerhetspolicyn bör fortlöpande omprövas och anpassas till det aktuella behovet av skydd.**

En säkerhetspolicy bildar grunden för säkerhetsarbetet och ligger till grund för organisationens riktlinjer och regler för hantering av personuppgifter.

En otydlig och svårtillämpad säkerhetspolicy kan uppfattas som en formalitet som måste finnas men som inte berör de anställda.

**Kontroll/avstämning**

**För att säkerställa att riktlinjer och regler följs bör kontroller genomföras. Inom en organisation bör det även finnas rutiner för rapportering och uppföljning av säkerhetsincidenter.**

## Personalen

Rätt kompetens är en viktig faktor för en fungerande säkerhetsorganisation.

**Den personuppgiftsansvarige bör utforma arbetsrutiner och arbetsuppgifter på ett sådant sätt att det blir möjligt för personalen att arbeta och tänka säkerhetsmedvetet.**

En effektiv stödfunktion för praktiska IT-frågor eliminerar många misstag som orsakas av okunnighet.

**I en organisation bör man undvika ett personberoende. Mer än en person bör till exempel känna till hur IT-utrustningen fungerar.**

**Den personuppgiftsansvarige bör se till att alla som har tillgång till personuppgifter får relevant utbildning.**

Intrång kan förorsakas av den egna personalen. Intrången kan både vara avsiktliga och oavsiktliga. Genom att ge de anställda en klar uppfattning om:

- vad som är tillåtet,
- vilka konsekvenserna blir om man bryter mot en regel, och
- hur efterlevnaden av reglerna följs upp kan man minska risken för intrång inom verksamheten.

Det är viktigt att skapa medvetenhet inom hela organisationen om vilka riskerna är samt att:

- lära personalen att uppmärksamma tecken på eventuella intrång,
- göra klart vem personalen ska vända sig till när den misstänker intrång.

**Mänskliga misstag**

**Den personuppgiftsansvarige bör se till att personalen informeras om vikten av att följa gällande säkerhetsrutiner. Den personuppgiftsansvarige bör göra klart för personalen att det är viktigt att:**

- **inte skriva upp lösenord,**
- **logga ut när man lämnar arbetsstationen,**
- **inte använda gemensam användaridentitet,**
- **inte ha bildskärmen vänd så att obehöriga**
- **kan läsa informationen,**
- **inte dela med sig information till någon annan utan att vara säker på att den personen är behörig att få ta del av informationen,**
- **inte skriva ut känslig information på en skrivare som obehöriga har eller lätt kan skaffa sig tillgång till.**

# Hotbild

**Störningar**

Störningar kan medföra att personuppgifter förstörs, att de förändras så de blir felaktiga eller missvisande eller sprids till obehöriga. Detta kan medföra att människors personliga integritet kränks.

Störningarna kan till exempel bestå i felaktigt handhavande, driftstörningar, olyckshändelser, sabotage, stöld av utrustning eller obehörig åtkomst till personuppgifter.

**Hotbilden**

Utgångspunkten för säkerhetsarbetet är medvetenhet om vilka risker som finns i den egna IT-miljön. Först när man vet vad man vill skydda sig mot och vad man vill skydda kan man bygga upp en god och kostnadseffektiv säkerhet. Genom att kartlägga riskerna kan man undvika att resurser koncentreras till områden där de inte gör någon nytta, medan områden där de verkliga hoten finns förblir oskyddade.

**En bedömning av sannolikheten för olika typer av störningar och konsekvenserna av dessa bör göras som underlag för utformningen av säkerhetsåtgärder.**

**Den personuppgiftsansvarige bör därför göra klart för sig:**

- **vilken hotbild som finns, det vill säga vilka händelser som skulle kunna drabba den egna IT-miljön,**
- **hur stor risken är för att ett hot blir verklighet,**
- **vilka konsekvenserna kan bli om ett hot blir verklighet,**
- **vilka resurser en obehörig behöver för att realisera ett hot, det vill säga vilken kunskap, utrustning, eller omständighet som krävs för att hotet ska kunna inträffa.**

### Sårbarhets- och risk-analyser

Det finns flera etablerade metoder för sårbarhets- och riskanalyser. När man använder dessa metoder, särskilt de som baseras på checklistor, är det viktigt att komma ihåg att det ofta är fråga om generella riktlinjer. Styrkan med metoderna är att någon redan har tänkt igenom olika situationer som kan uppstå. Man får stöd så att inte något viktigt glöms bort. Dessutom går man systematiskt till väga när man arbetar efter en redan fastlagd metod. Nackdelen med att använda en checklista är att det finns en risk för att man arbetar mekaniskt efter listan och därmed låter bli att tänka själv samt att verkligen analysera resultaten.

# Säkerhetsnivå

**Lämplig säkerhets-nivå**

Personuppgiftslagen kräver att den personuppgifts-ansvarige vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska ställas i relation till:

- de tekniska möjligheter som finns,
- kostnader för åtgärderna,
- de risker som finns, samt
- de behandlade uppgifternas känslighet.

Bedömningen av de tekniska möjligheter som finns kan till exempel avse vilka fysiska och logiska säkerhetshjälpmedel som finns tillgängliga på marknaden.

Vidare kan vägas in vad det skulle kosta att genomföra åtgärderna. Den personuppgiftsansvarige behöver alltså inte använda den allra bästa tekniken om det skulle kosta för mycket. Det räcker således i huvudsak att använda utrustning som normalt används och finns att tillgå på marknaden.

En särskild riskfaktor är antalet personer som de behandlande uppgifterna avser. Skador av till exempel ett angrepp kan bli mer omfattande när uppgifter om många personer behandlas. En angripare kan antas vara beredd att lägga ned större resurser på ett intrång om han samtidigt kan skaffa sig tillgång till uppgifter om många personer.

Känsligheten hos de personuppgifter som behandlas beror på flera faktorer och måste alltid bedömas särskilt. Arten av de uppgifter som behandlas har stor betydelse men även mängden av uppgifter om varje person måste beaktas eftersom den bestämmer hur detaljerad bild som kan erhållas.

Anledningen till behandlingen av personuppgifterna kan vara känslig liksom förekomsten av en personuppgift (till exempel ett register över personer som utgör en utsatt grupp).

Som exempel på personuppgifter som normalt inte är att anse som känsliga är personuppgifter som följer av:

- medlemskap,
- anställningsförhållande,
- kundförhållande, eller
- något därmed jämförligt förhållande.

Som exempel på personuppgifter som normalt är att anse som känsliga kan nämnas uppgifter angående:

- ekonomisk hjälp eller vård inom socialtjänsten,
- enskilds personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet,
- uppgifter inom kreditupplysning eller inkasso-verksamhet.

Ett uttryck för att det är fråga om känsliga uppgifter kan vara att uppgifterna omfattas av sekretess enligt sekretesslagen (1980:100).

**Känsliga uppgifter**

Som känsliga personuppgifter enligt personuppgiftslagen betecknas uppgifter som avslöjar:

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening, eller
- personuppgifter som rör hälsa eller sexualliv.

**Personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden**

**klassificeras inte som känsliga enligt person-uppgiftslagen men bör ändå när det gäller säkerhet jämställas med känsliga uppgifter.**

Uppgifternas art är alltså av stor betydelse för vilken säkerhet som bör iakttas. Om känsliga uppgifter behandlas ställs högre krav på säkerheten.

## Säkerhetsåtgärder

### Fysisk säkerhet

**IT-utrustning som används för behandling av personuppgifter bör ha ett tillfredsställande skydd mot stöld och händelser som kan förstöra utrustningen. Den personuppgiftsansvarige bör därför se över behovet av till exempel**

- **låsutrustning,**
- **inpasseringskontroll,**
- **galler för fönster,**
- **en fungerande larmutrustning för till exempel rök, brand, vatten och inbrott,**
- **utrustning som skyddar vid strömavbrott och strömstörningar,**
- **kylanläggning,**
- **skydd mot rök- och vattenskada,**
- **brandsläckningsutrustning,**
- **speciell placering av utrustning,**
- **säkerhetsskåp,**
- **märkning av utrustning.**

Det kan ibland bli konflikt mellan olika skyddsåtgärder. Till exempel kan brandskyddskrav på olåsta dörrar komma i konflikt med krav på inpasseringskontroll. Kravet på att begränsa antalet personer som har åtkomst till systemet kan strida mot kravet på personoberoende när det gäller IT-utrustning och system. I sådana situationer måste man vara extra vaksam när man väljer lämpliga skyddsåtgärder.

Särskilda krav på säkerhet behövs när portabel IT-utrustning som mobila enheter och flyttbara lagringsmedia används. När man använder sådan utrustning är risken särskilt stor för att utomstående kan komma åt personuppgifterna. Känsliga personuppgifter kan därför behöva krypteras.

**Rutiner för användning av portabel IT-utrustning och hur utrustningen och personuppgifterna i den ska skyddas bör, beroende på känsligheten hos personuppgifterna, upprättas.**

Tillträdeskontroll

**För att säkerställa att endast behörig personal får tillträde till utrymmen där IT-utrustning finns bör rutiner för en tillträdeskontroll upprättas.**

**Behovet av att kunna utföra en arbetsuppgift bör vara utgångspunkten för en tillträdeskontroll. I en organisation bör övervägas att skapa områden med olika typer av tillträdeskontroll.**

Behörighetskontroll

**För att förhindra obehörig användning eller åtkomst bör ett system för behörighetskontroll upprättas. Ett sådant system bör omfatta möjligheter att identifiera användare och bekräfta användarens identitet, exempelvis genom användning av personliga lösenord. Andra tekniker för identifiering, till exempel engångslösenord, aktiva behörighetskort eller biometriska metoder, till exempel fingeravtryck bör övervägas.**

**Systemet bör kunna kontrollera användningen så att endast de som behöver uppgifterna för sitt arbete får tillgång till åtkomstskyddade personuppgifter. Det bör finnas rutiner för tilldelning och kontroll av behörigheter.**

Kryptering, där krypteringsnycklarna är tillräckligt kraftfulla och där nycklarna handhas på ett säkert sätt, kan användas som skydd även när man vill försäkra sig om att personal som behöver fullständiga rättigheter till systemet inte ska kunna läsa viss information.

### Behandlings-historik (logg)

**För att åtkomsten ska kunna kontrolleras bör det, beroende på känsligheten hos personuppgifterna, finnas en behandlingshistorik som sparas en viss tid.**

En behandlingshistorik behövs normalt inte om endast en person använder utrustningen.

**En behandlingshistorik bör följas upp och skyddas mot otillåtna ändringar.**

**En behandlingshistorik bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av person-uppgifter. Behandlingshistoriken bör, beroende på känsligheten hos personuppgifterna, ange till exempel läsning, ändring, utplåning eller kopiering av personuppgifter.**

**En behandlingshistorik bör inte utformas eller utnyttjas så att den medför risk för intrång i personalens integritet.**

En behandlingshistorik har också en förebyggande funktion. Förutsättningen för det är att användarna informeras om att det förs en behandlingshistorik och att den kontrolleras.

### Inloggning och lösenord

**I fråga om inloggning och lösenord bör följande iakttas:**

- **Användaridentitet och lösenord bör inte antecknas där andra kan komma åt uppgifterna.**
- **Lösenordet bör regelbundet bytas.**
- **Personlig inloggningsidentitet bör aldrig överlåtas till någon annan.**
- **En skärmsläckare med lösenord bör användas om inte utloggning alltid sker när en arbets-station lämnas obemannad, även för en kort tid.**

- **Lösenord bör vara långa och det är bra att blanda små och stora bokstäver med siffror.**

Ett lösenord bör vara lätt att komma ihåg och svårt att gissa och bör inte kunna hänföras till användaren. Dessa krav är motsägelsefulla, men om man tänker på en hel mening, till exempel 5 Fula elefanter flög till de 7 månarna och använder de första bokstäverna i varje ord och siffrorna blir lösenordet 5Feftd7m . Lösenordet blir då svårt att gissa för en utomstående, men lätt för innehavaren att komma ihåg. Lösenord bör inte lagras i klartext i behörighetskontrollsystem.

Kommunikation

**För att förhindra att personuppgifter förstörs, ändras eller förvanskas vid överföring via nät och för att skydda anslutna tjänster mot obehörig åtkomst bör den personuppgiftsansvarige införa lämpliga åtgärder för att åstadkomma en tillfredsställande säkerhet. Personuppgifter som överförs via nät bör, beroende på känsligheten hos personuppgifterna, skyddas, till exempel genom kryptering.**

**När utrustningen ansluts till Internet eller annat öppet nät bör anslutningen skyddas för att förhindra obehörig trafik. I samma syfte bör åtkomst förhindras från det öppna nätet till annan utrustning eller lokala nät hos den personuppgiftsansvarige. Om uppgifterna endast får lämnas ut till identifierade användare bör mottagarens identitet säkerställas.**

Mottagarens identitet kan säkerställas genom e-legitimation, engångslösenord, aktiva behörighetskort eller motsvarande.

**Behovet av åtgärder och policy för att minska säkerhetsrisker vid användning av elektronisk post bör övervägas.**

Genom exempelvis kryptering förhindrar man att uppgifterna kan läsas eller förvanskas i samband med överföringen. För att kryptering ska ge det skydd som krävs måste krypteringsnycklarna vara tillräckligt kraftfulla och nycklarna måste handhas på ett säkert sätt.

Om extern datakommunikation upprättas via en anslutning kan obehöriga få åtkomst till datorsystemet om inte en säker identifiering av användaren utförs.

## Åtgärder mot förlust av information

Information kan försvinna och förstöras på olika sätt. Det viktigaste skyddet mot förlust är säkerhetskopiering.

**För att förhindra förlust av personuppgifter bör rutiner för säkerhetskopiering finnas. För att säkerhetskopieringen ska fungera bör den personuppgiftsansvarige se till att:**

- **Säkerhetskopior tas tillräckligt ofta.**
- **Kopieringen automatiseras för att eliminera risken för mänskliga misstag.**
- **Flera generationer av säkerhetskopior sparas.**
- **Prova regelbundet att det går att återskapa säkerhetskopian. Prova om möjligt också på annan dator än den där kopian gjordes.**
- **Förvara kopian skyddad och gärna i flera exemplar på olika skyddade platser.**
- **Skapa rutiner för att logga kopieringen och att loggen läses efter varje kopiering för att se att inga fel har uppstått under kopieringen.**

Att systemet kan återskapas från säkerhetskopian testas lämpligen av den som i praktiken är ansvarig för att informationen återskapas. Regelbundna tester gör den systemansvarige rutinerad och säker när han ska utföra kopieringen i praktiken. Tyvärr är det vanligt att informationen går förlorad på grund av att rutiner för säkerhets-

kopiering inte fungerar. Informationen kanske inte har blivit kopierad trots att det såg ut så. Det förekommer också att ingen vet hur man återskapar systemet från säkerhetskopian, liksom att den enda säkerhetskopian som fanns har förvarats i samma rum som datorn och förstörts samtidigt vid en brand.

### Utplåning

**När fasta eller löstagbara lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål bör lagringsmedierna förstöras, eller alternativt raderas på sådant sätt att uppgifterna inte kan återskapas.**

### Reparation och service

**Reparation och service bör ske på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga. När reparation och service av IT-utrustning utförs av annan än den personuppgiftsansvarige bör, beroende på personuppgifternas känslighet, ett avtal om säkerhet träffas med serviceföretaget. Ett sådant avtal bör till exempel innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas i samband med service.**

### Skydd mot skadliga program

Information kan förstöras av skadliga program. Det ökande behovet av datakommunikation ökar risken för spridning av skadliga program.

**Den personuppgiftsansvarige bör se över vilka åtgärder som bör införas för att upptäcka och skydda mot skadliga program.**

Det finns leverantörer som erbjuder stöd vid till exempel en virusattack. Leverantörer har ofta goda kunskaper på området och är experter på hur man gör för att minska skadan.

Genom att upprätta en särskild policy för användande av Internet och portabel IT-utrustning kan man minska risken för att skadliga program kommer in i datorsystemet. En kartläggning av alla ingångar till datorsystemet är en relevant åtgärd när man ser över sin hotbild angående skadliga program.

### Verifiering av säkerheten

Regelbundna tester är viktiga om man ska försäkra sig om att säkerhetsorganisationen och utrustningen fungerar samt för att hitta eventuella brister i säkerheten.

Det finns företag som erbjuder tjänster för detta. Dessa företag har kunskap om var brister kan finnas. De har även den tekniska utrustning som krävs för testerna.

### Andra åtgärder

**När det gäller åtgärder mot otillbörlig åtkomst bör den personuppgiftsansvarige även se över behovet av till exempel:**

- **rutiner vid besök,**
- **rutiner och regler vid distansarbete och Internetanvändning,**
- **rutiner för att ta bort inaktuella användarkonton,**
- **avstängning av modem när det inte används,**
- **installation av aktuella programrättelser från leverantörerna för att motverka säkerhetshål i programvaror,**
- **skyddsåtgärder mot avlyssning och röjande signaler.**

# Sammanfattning

**Den personuppgiftsansvarige bör tänka på att:**

- **Kartlägga hotbilden**
- **Sätta mätbara mål för säkerhet**
- **Fastställa policy för säkerhet**
- **Skapa en fungerande organisation för säkerhet**
- **Skaffa den utrustning som behövs och använda den rätt**
- **Upprätta regler och rutiner**
- **Informera och utbilda kontinuerligt**
- **Följa upp att regler och rutiner efterlevs och respekteras**
- **Testa säkerheten regelbundet**

## Datainspektionen

Datainspektionen är en myndighet som arbetar för att behandlingen av personuppgifter i samhället inte ska medföra otillbörliga intrång i enskilda människors personliga integritet. Ansvarsområdet omfattar framförallt personuppgiftslagen, inkassolagen och kreditupplysningslagen. Datainspektionen gör inspektioner och hanterar klagomål från enskilda medborgare samt tar fram vägledningar och ger synpunkter på utredningar och lagförslag. Datainspektionen har också en omfattande informationsverksamhet, vi utbildar, svarar på frågor och ger stöd till personuppgiftsombud.

**Datainspektionens allmänna råd**

Datainspektionen ger ut allmänna råd med rekommendationer i olika frågor. Råden ligger till grund för de föreskrifter som Datainspektionen ger exempelvis i samband med tillsyn och när tillstånd för inkassoverksamhet utfärdas. Broschyrerna beställer på vår webbplats www.datainspektionen.se.

## Kontakta Datainspektionen

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

Datainspektionen