

## 1.4 Grundläggande krav på behandling av personuppgifter

Den personuppgiftsansvarige skall bl.a. se till att personuppgifter:

- behandlas bara om det är lagligt.
- behandlas på ett korrekt sätt.
- endast samlas in om de är relevanta och om ändamålen är berättigade.
- bara behandlas om det är nödvändigt med hänsyn till ändamålet.
- endast behandlas om uppgifterna är riktiga.
- rättas eller tas bort om de är felaktiga.
- inte sparas längre än nödvändigt.

Behandling av personuppgifter får endast ske om den registrerade lämnat sitt samtycke eller om behandlingen är nödvändig av andra skäl, t.ex. om den ansvarige arbetar på en myndighet och skall utföra en arbetsuppgift.

En registrerad kan när som helst ta tillbaka sitt samtycke.

Det är förbjudet att behandla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religionstillhörighet samt medlemskap i fackförening.

Det är också förbjudet att behandla personuppgifter som rör hälsa och sexualliv. Det finns undantag då förbudet inte gäller, t.ex. om den registrerade ger sitt samtycke. Personnummer får inte behandlas utan samtycke om det inte är absolut nödvändigt, t.ex. då säker identifiering krävs.

## 1.5 Personuppgiftsansvarig

Den person eller de personer som bestämmer varför och hur personuppgifterna ska behandlas, kallas för personuppgiftsansvarig. Det kan vara en juridisk person, förening, företag eller myndighet. Den som behandlar uppgifterna åt den ansvarige kallas personuppgiftsbiträde.

## 1.6 Personuppgiftsombud

Den person som kan utses av den personuppgiftsansvarige för att se till att personuppgifterna behandlas på ett lagligt och korrekt sätt kallas personuppgiftsombud.

- Ombudet ska påpeka eventuella brister för den ansvarige. Bryter den ansvarige mot bestämmelserna och ombudet påpekar detta utan att den ansvarige rättar till felet, ska ombudet anmäla detta till Datainspektionen.
- Ombudet ska även hjälpa registrerade att få rättelse om deras personuppgifter är felaktiga eller ofullständiga.

Det ska finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att personuppgiftsbitrådet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbitrådet är skyldigt att vidta de åtgärder som avses i 31§ första stycket.

*Hämtat ur Personuppgiftslagen 30§.*

## 1.7 Anmälan om behandling av personuppgifter

Det tidigare licens- och tillståndssystemet har tagits bort. Enligt PUL finns det en principiell skyldighet att anmäla all databehandling till datainspektionen, som ska föra ett register över anmälningarna.

Om den personuppgiftsansvarige utsett ett ombud och meddelat detta till datainspektionen behöver man inte göra en anmälan. Allmänheten har rätt att få reda på om det finns databehandlingar som inte anmälts. Dessa uppgifter har man rätt att få direkt från den personuppgiftsansvarige.

## 1.8 Datainspektionen

Datainspektionen är den myndighet som ska se till att lagarna efterföljs. Om datainspektionen upptäcker att personuppgifter behandlas på ett olagligt sätt kan de förbjuda den ansvarige att använda uppgifterna. Datainspektionen får då ansöka hos länsrätten om att uppgifterna ska tas bort. För att detta ska ske måste det först vara helt säkert att det inte finns något sätt att göra databehandlingen laglig.

Ett beslut av Datainspektionen överklagas i första hand hos länsrätten. Datainspektionen får bestämma att beslutet ska gälla även om det överklagas.

Datainspektionen:

- ger tillstånd till de som skriftligen begär det.
- ger kostnadsfritt råd och hjälp till enskilda personer som har problem med personuppgiftsansvariga.
- inspekterar användningen av personregister.
- övervakar kreditupplysningsföretagens verksamhet.

### Datainspektionen

Box 8114

104 20 Stockholm

Telefon: 08-657 61 00

Fax: 08-652 86 52,

E-post: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

## 1.9 Straff

- Brott*: Brott mot PUL kan leda till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år. Ex: Om ett register inrättas utan att en skriftlig anmälan gjorts till datainspektionen.
- Skadestånd*: Den personuppgiftsansvarige ska ersätta den person som lidit skada av olagliga, felaktiga eller missvisande personuppgifter.
- Dataintrång*: Den som olovligt tar sig in i ett datorsystem och tar del av, förstör, ändrar eller lägger till någonting till registret, kan dömas till böter eller fängelse i högst två år.

## 1.10 Offentlighetsprincipen

I Sverige har vi tillgång till alla dokument som tas fram av stat, landsting eller kommun. Dock kan vissa dokument sekretessbeläggas. Detta innebär att du har rätt att läsa offentliga handlingar. Du behöver inte uppge namn eller varför du vill studera handlingarna.

Offentliga handlingar har du rätt att ta del av, oavsett om de finns i tryck, är handskrivna, eller finns lagrade i en dator. Finns informationen lagrad i en dator har du rätt att få hjälp att använda datorn.

Om du ej får lov att använda datorn av sekretesskäl så har du rätt att kostnadsfritt få en pappersutskrift av den begärda informationen.

## 1.11 Sammanfattning

Om du är ansvarig för personregister i någon form är du skyldig att anmäla ditt registerinnehav till datainspektionen. Som ansvarig för register måste du ha en aktuell förteckning över vad registret innehåller och hur det används.

Du behöver tillstånd när du ska registrera känsliga uppgifter, uppgifter om personer du inte har någon direkt anknytning till, och om du vill samköra två olika personregister. Personnummer ska bara användas om det är absolut nödvändigt. Datainspektionen förordar att man t.ex. använder kund- eller medlemsnummer istället.

## 2 Datasäkerhet

Datasäkerheten blir allt mer viktig i dagens IT-miljö. Som användare bör du tänka på vad som kan göras för att skydda din information och din utrustning mot otilbörligt användande.



1.4

Du bör tänka på dessa saker för att maximera säkerheten:

- Har du skydd mot stöld av dator, hårddisk, och disketter, m.m?
- Är dina enheter skyddade med lösenord och användarnamn?
- Är du skyddad från yttre intrång via Internet genom brandvägg och virussydd?
- Utför du säkerhetskopiering och förvaras kopiorna på ett säkert ställe?
- Är dina data som överförs via Internet skyddade för avlyssning?

Enligt undersökningar är den mänskliga faktorn den överlägset största orsaken till störningar i datorstödd verksamhet. Med mänskliga faktorn menas störningar som kan uppstå på grund av omedvetna/medvetna misstag. Det kan t.ex. vara slarv med säkerhetskopieringen eller att virusmittade program/filer har kopierats/laddats ner.

### 2.1 Brandvägg

En brandvägg är ett system, som med hjälp av en programvara eller en hårdvara, skyddar t.ex. ett företags lokala nätverk mot attacker från ett externt nät. För att en brandvägg skall kunna fungera förutsätts det att all nättrafik mellan det interna och externa nätet passerar igenom brandväggen och att brandväggen enbart släpper igenom viss, tillåten nättrafik. Brandväggen själv måste naturligtvis vara skyddad för attack eller övertagande.

Brandväggen hindrar obehöriga användare att passera utifrån in till det skyddade interna nätverket och ser till att sårbara funktioner inom det interna nätverket inte kan användas utifrån. Trafiken från det interna nätverket till det externa nätverket kan också begränsas. Brandväggar kan även användas för att öka säkerheten inom det lokala nätverket genom att bilda "vattentäta skott" mellan olika avdelningar, t.ex. där vissa funktioner inte kan genomföras över avdelningsgränserna. Förutom attacker mot funktioner kan brandväggen också hindra flera olika typer av attacker som syftar till att förfälska routing- eller källadressen (spoofing).

Brandväggarnas loggar ger information om hur trafiken sett ut och de kan ge larm vid intrångsförsök. Brandväggen är också en bra grund för andra tjänster, t.ex. NAT (*Network Address Translation*), VPN (*Virtual Private Network*) och IDS (*Intrusion Detection System*).

En brandvägg skyddar dock inte mot alla attacker. Angriparen kan bl.a. utnyttja informationssäkerhetshål som finns i en tjänst som brandväggen tillåter (t.ex. i webbservern). Brandväggen skyddar inte heller mot sådana attacker där den passerar eller kringgås. Den kan inte heller hindra skadliga programvaror (t.ex. virus) från att passera utifrån till det interna nätverket och tvärtom.

## 2.2 Säkerhetskopiering

Det primära när det gäller säkerheten för den information som är lagrad i datorn är säkerhetskopiering. Det innebär att du tar en exakt kopia av den lagrade informationen. Skulle någonting gå fel på hårddisken kan du återställa informationen med hjälp av säkerhetskopian. Lyckas inte det kan du alltid ta den till en annan PC och återskapa den där. Förtjänsten är att du slipper göra om kanske månaders arbete.



*Säkerhetskopiering av den information som finns i persondatorn till en bandstation.*

Har du under dagen ändrat, lagt till, eller tagit bort information från hårddisken, bör du göra en säkerhetskopiering. Samma sak gäller för disketter.

Backup kan bl.a. göras på vanliga disketter, CD-skivor eller backupband som är särskilt avsedda för backup och kan lagra flera Giga-byte. För att skapa eller återställa backuper använder du ett särskilt program. Många operativsystem har sådan programvara installerat, annars kan du använda separata program, som t.ex. Norton Ghost eller BackBones NetVault.

Eftersom man inte alltid upptäcker ett fel eller förlust av data omedelbart, så bör du förvara flera olika backup-generationer. Du kan t.ex. spara en backup för varje vecka eller månad för att, när du upptäckt att olyckan varit framme, kunna återställa en backup som togs innan felet inträffade.

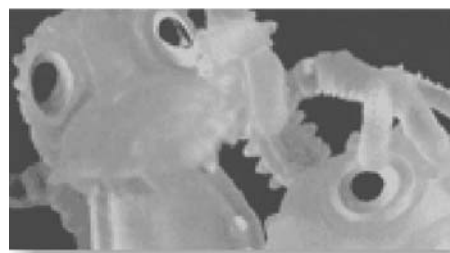
Ju oftare säkerhetskopiering sker, desto större säkerhet.

## 3 Hot

Alla system utsätts för någon form av hot. Det kan vara ett problem med hårdvaran, ett fel i mjukvaran, eller hot utifrån. Virus, trojaner, och maskar, är olika program som på något sätt förändrar, förstör, eller bryter sig in i datasystem. Dessutom kan system avlyssnas. Dessa hot måste på något sätt stängas ute. Man kan använda antivirusprogram för att slippa virus, trojaner, och maskar. Nätverks-trafiken kan krypteras så att avlyssningen inte är ett överhängande problem, o.s.v.

### 3.1 Virus

Datavirus är program som "infekterar" filer på användarens dator. Namnet "virus" kommer av att dataviruset kopierar sig själv.



Det finns mängder av olika virus, varav en del är ganska harmlösa. De kan t.ex. visa ett meddelande vid ett visst datum, eller vända upp och ner på bilden på skärmen. Huvuddelen är konstruerade för att på något sätt skada de filer som finns på användarens dator.