



Informationssäkerhet

Informationssäkerhet är en viktig del av skyddet för den personliga integriteten. Enligt personuppgiftslagen (PuL) ska den personuppgiftsansvarige* se till att personuppgifter som behandlas i verksamheten skyddas genom tekniska och organisatoriska åtgärder. Nivån på säkerheten ska anpassas till:

- vilka integritetsrisker behandlingen medför,
- hur känsliga de behandlade personuppgifterna är,
- vilka tekniska möjligheter som finns, och
- vad det kostar att genomföra åtgärderna.

Datainspektionen har givit ut allmänna råd, *Säkerhet för personuppgifter*. Där finns exempel på administrativa och tekniska säkerhetsåtgärder som man kan vidta för att uppfylla de krav som personuppgiftslagen ställer på informationssäkerhet när man behandlar personuppgifter. Det här faktabladet är en sammanställning av de viktigaste säkerhetsåtgärderna som nämns i de allmänna råden.

Ytterligare åtgärder som inte nämns här kan vara nödvändiga för att skydda personuppgifterna som behandlas. I enskilda fall får Datainspektionen besluta om vilka säkerhetsåtgärder som ska vidtas.

Organisation

Säkerhetspolicy. En verksamhet bör ha en säkerhetspolicy – i vart fall om man hanterar känsliga personuppgifter eller behandlar personuppgifter i stor skala. I en sådan policy redovisas organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten. Policyn ska vara tydlig, lätt att förstå och enkel att tillämpa i praktiken. Om det finns anställda i verksamheten bör policyn vara skriftlig

* Personuppgiftsansvarig är normalt en juridisk person (företag, stiftelse, myndighet etc.) som behandlar personuppgifter och bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till. Det är alltså inte chefen eller någon anställd som är personuppgiftsansvarig.

och allmänt tillgänglig inom organisationen. Ompröva säkerhetspolicyn fortlöpande och anpassa den till det aktuella behovet av skydd.

Kontroll/avstämning. Genomför kontroller för att säkerställa att riktlinjerna och reglerna i säkerhetspolicyn efterföljs. Det bör också finnas rutiner för att rapportera och följa upp incidenter.

Personalen. Utforma arbetsrutiner och arbetsuppgifter så att det blir möjligt för personalen att arbeta och tänka säkerhetsmedvetet. Undvik personberoende, till exempel bör mer än en person känna till hur IT-utrustningen fungerar. Se till att alla som har tillgång till personuppgifter får lämplig utbildning och informera personalen om vikten av att följa gällande säkerhetsrutiner.

Hotbild

Som en utgångspunkt för arbetet med informationssäkerhet är det lämpligt att göra risk- och sårbarhetsanalyser för att klargöra vilken säkerhetsnivå som ska gälla för skyddet av organisationens information och informationssystem.

Som underlag för hur säkerhetsåtgärderna ska utformas bör man också göra en bedömning av hur sannolikt det är att olika typer av störningar ska inträffa och vilka konsekvenser det i så fall skulle få.

Säkerhetsnivå

Känsliga uppgifter definieras i personuppgiftslagen som uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och även uppgifter som rör hälsa eller sexualliv. Uppgifter om brott får normalt bara behandlas av myndigheter; de klassificeras inte som känsliga i personuppgiftslagen men bör ändå jämföras med känsliga uppgifter när det gäller säkerhet.

Säkerhetsåtgärder

Fysisk säkerhet. Se till att IT-utrustning som används för att behandla personuppgifter har ett gott skydd mot stöld och händelser som kan förstöra utrustningen. Inför rutiner för hur portabel IT-utrustning ska användas och hur utrustningen och personuppgifterna i den ska skyddas. Nivån på skyddet bestäms av hur känsliga uppgifterna är.

Tillträdeskontroll. För att säkerställa att enbart behörig personal får tillträde till utrymmen där det finns IT-utrustning, bör det finnas rutiner för tillträdeskontroll. Behovet av att kunna utföra en arbetsuppgift kan göras till utgångspunkt för hur en tillträdeskontroll utformas. I vissa organisationer kan det vara lämpligt att skapa områden med olika typer av tillträdeskontroll.

Behörighetskontroll. Ett system för behörighetskontroll hindrar obehöriga från att använda IT-utrustningen och bereda sig tillgång till personuppgifter. Systemet bör kunna identifiera användare och bekräfta användarens identitet, exempelvis med personliga lösenord.



Andra tekniker för identifiering kan också komma i fråga: engångslösenord, aktiva behörighetskort eller biometriska metoder.

Systemet bör också kunna kontrollera åtkomstskyddade personuppgifter så att bara de som behöver uppgifterna för sitt arbete får tillgång till dem. Inför rutiner för tilldelning och kontroll av behörigheter.

Behandlingshistorik (logg). För att kunna kontrollera vilka som har haft tillgång till personuppgifterna bör det finnas en behandlingshistorik (logg) som sparas en viss tid. Hur loggen ska utformas beror på hur känsliga personuppgifterna är. En logg ska följas upp och skyddas mot otillåtna ändringar. Normalt ska den vara så detaljerad att den kan användas för att utreda om personuppgifter har använts felaktigt eller obehörigt.

Om personuppgifterna är känsliga ska loggen visa användaridentitet, tidpunkt och vilka personuppgifter användaren har haft tillgång till – även om han bara har läst informationen.

Loggen ger också ett förebyggande skydd. En förutsättning är dock att användarna informeras om att all användning loggas och att loggen följs upp.



Kommunikation. Förhindra att personuppgifter förstörs, ändras eller förvanskas då de överförs via nät och skydda anslutna tjänster mot obehörig åtkomst. Skyddet ska anpassas till hur känsliga uppgifterna är. När utrustningen ansluts till Internet eller annat öppet nät ska anslutningen skyddas så att obehörig trafik förhindras. Man bör också skydda sin utrustning och sina lokala nät så att inga obehöriga kan komma in via det öppna nätet. Om uppgifter enbart får lämnas ut till identifierade användare ska mottagarens identitet säkerställas.

Känsliga personuppgifter får endast lämnas ut via öppna nät till **identifierade användare** vars identitet är säkerställd med en teknisk funktion som asymmetrisk kryptering (till exempel e-legitimation), engångslösenord eller motsvarande. Dessutom ska känsliga personuppgifter vara krypterade vid överföring.

Överväg också vilka åtgärder (och eventuell policy) som behövs för säker användning av Internet och e-post.

Åtgärder mot förlust av information. För att förhindra förlust av personuppgifter ska det finnas rutiner för säkerhetskopiering. För att säkerhetskopieringen ska fungera bör man:

- Ta säkerhetskopior tillräckligt ofta
- Prova regelbundet att det går att återskapa säkerhetskopieringen
- Förvara kopian skyddad

Skydd mot skadliga program. Se över vilka åtgärder som behövs för att upptäcka och skydda systemet mot skadliga program.

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

Reparation och service bör utföras på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga. Skriv ett avtal med serviceföretaget om utomstående ska reparera eller serva IT-utrustningen. Anpassa avtalet till hur känsliga personuppgifter som finns i systemet. Avtalet kan också innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas i samband med servicen.

Om service utförs på distans ska servicepersonalen identifieras på ett säkert sätt och endast ha tillgång till utrustningen under själva servicetillfället.

Personuppgiftsbiträde

Det är inte ovanligt att den personuppgiftsansvarige får hjälp med databearbetningen av någon annan, datadriften sköts i praktiken av någon som inte är anställd i organisationen, vanligen en servicebyrå. I sådana fall blir servicebyrån personuppgiftsbiträde. Biträdet kan vara en fysisk eller juridisk person (företag, stiftelse, myndighet, etcetera). En anställd i den personuppgiftsansvariges organisation eller någon annan som behandlar personuppgifter under den personuppgiftsansvariges direkta ansvar är inte personuppgiftsbiträde.

Enligt personuppgiftslagen får biträdet bara behandla personuppgifter enligt instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal som reglerar hur biträdet ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas.

Mer att läsa om informationssäkerhet

Datainspektionens allmänna råd, *Säkerhet för personuppgifter*.
www.datainspektionen.se

Krisberedskapsmyndighetens rekommendationer *Basnivå för informationssäkerhet* (BITS). www.krisberedskapsmyndigheten.se

Svensk standard. *Ledningssystem för informationssäkerhet – Riktlinjer för styrning av informationssäkerhet* (SS-ISO/IEC 17799:2005) och *Krav* (SS-ISO/IEC 27001:2006). www.sis.se

Kontakta Datainspektionen

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