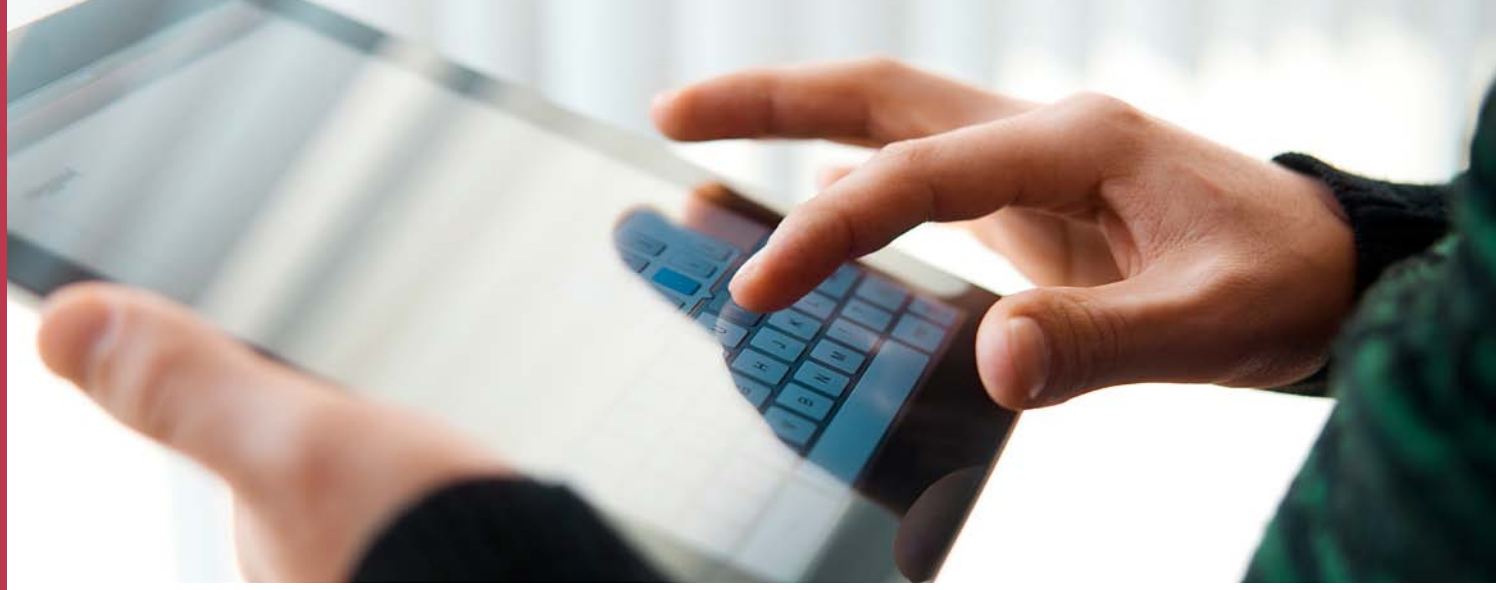

Mobila enheter

Checklista för behandling av personuppgifter

Den som vill behandla personuppgifter i mobila enheter (till exempel surfplattor och smarta mobiltelefoner) måste vara medveten om att det kan innebära vissa särskilda risker. Risker som kan få svåra konsekvenser för en enskild vars personuppgifter riskerar att spridas. En mobil enhet kan kommunicera över öppna nätverk och används ofta utanför arbetsgivarens lokaler. Det finns möjlighet att ladda ned appar och utnyttja ett stort antal olika tjänster på en mobil enhet. Appar kan dock påverka säkerheten i den mobila enheten och medföra oavsiktlig spridning av personuppgifter.

Mobila enheter är som regel stöldbegärlig egendom. Om personuppgifterna i enheten inte är tillräckligt skyddade kan det vara svårt att avgöra om det är den behörige användaren som tar del av uppgifterna. Den personuppgiftsansvarige måste, så långt det är möjligt, vidta säkerhetsåtgärder för att bara en behörig användare ska få åtkomst till personuppgifterna i fråga.

Den här checklistan ska underlätta för den som planerar att använda sig av mobila enheter för överföring av integritetskänsliga personuppgifter. Det handlar både om sådana uppgifter som definieras som känsliga i personuppgiftslagen och andra uppgifter som rör den enskildes privatliv. Den personuppgiftsansvariges skyldigheter är samma även för anställda som tillåts använda sina egna mobila enheter.

☐ Gör en riskanalys

För att så långt som möjligt skydda de uppgifter som behandlas måste den personuppgiftsansvarige, innan behandlingen påbörjas, genomföra en riskanalys. I analysen ska man identifiera vilka allmänna och särskilda risker som finns med behandlingen av integritetskänsliga personuppgifter i mobila enheter. Därefter gör man en analys av vilka tekniska och organisatoriska säkerhetsåtgärder som måste vidtas för att hantera dessa risker. Målet är att den personuppgiftsansvarige ska vara medveten om riskerna och ha kontroll över personuppgiftsbehandlingen.

Maj 2013

Datainspektionen

☐ Utbilda och instruera användarna

Ta fram skriftliga instruktioner om hur det är tillåtet att använda mobila enheter. Instruktionerna bör exempelvis omfatta information om

- hur personuppgifter får hanteras
- vilka säkerhetsinställningar som ska användas
- eventuella begränsningar för privat användning
- vilka appar som är tillåtna att ladda ned
- vilka konsekvenser otillåten användning kan medföra.

Den ansvarige behöver också se till att anställda och uppdragstagare som använder sig av mobila enheter får löpande information om och utbildning i hur det är tillåtet att hantera enheterna.

☐ Tänk på behörighetsstyrningen

För att minimera risken för spridning av integritetskänsliga personuppgifter är det viktigt att begränsa åtkomsten. Enbart den som har behov av uppgifterna för att fullgöra sitt uppdrag eller sina arbetsuppgifter ska få åtkomst.

☐ Inför autentisering och kryptering

Om integritetskänsliga personuppgifter är eller kan göras åtkomliga över öppet nät krävs att inloggning sker med stark autentisering som till exempel e-legitimation, engångslösenord eller liknande. Även inloggning till administrationsgränssnitt kräver stark autentisering. Integritetskänsliga personuppgifter som överförs eller kan göras åtkomliga i öppna nät ska skyddas genom exempelvis kryptering.

☐ Lagring på en mobil enhet

Integritetskänsliga personuppgifter som lagras i en mobil enhet ska vara krypterade. Den ansvarige behöver även kontrollera att informationen som lagras i den mobila enheten inte oavsiktligt kopieras och lagras i så kallade molntjänster. När det inte längre är nödvändigt att lagra uppgifterna i de mobila enheterna ska de raderas. I den mån detta inte görs automatiskt ska det finnas skriftliga rutiner som stöd för den manuella hanteringen.

☐ Inför specifika säkerhetsåtgärder

För att hantera säkerhetsriskerna behöver specifika säkerhetsåtgärder övervägas, till exempel

- lösenordslås
- automatisk låsning av enheten efter viss tids inaktivitet
- centrala spärrfunktioner eller distansradering vid händelse av att den mobila enheten tappas bort eller blir stulen
- central styrning av säkerhetsinställningar och begränsning för vilka appar som kan laddas ned.

☐ Genomför logguppföljning

Som vid all behandling av personuppgifter måste den personuppgiftsansvarige kunna kontrollera vem eller vilka som har haft åtkomst till personuppgifter via en mobil enhet. IT-systemen ska därför kunna generera loggar som regelbundet ska kontrolleras. Den personuppgiftsansvarige ska informera användarna om att loggar kontrolleras regelbundet.

☐ Begränsa åtkomsten till personuppgifter

Personuppgifter ska bara vara tillgängliga mobilt när det verkligen behövs.

☐ Teckna ett personuppgiftsbiträdesavtal

Den som använder sig av en tredje part, ett så kallat personuppgiftsbiträde, för behandling av personuppgifter ska teckna ett personuppgiftsbiträdesavtal med denna part. Avtalet ska bland annat innehålla instruktioner för biträdets personuppgiftsbehandling och vilka säkerhetsåtgärder biträdet ska vidta.

☐ Håll koll på tekniken

För att den personuppgiftsansvarige ska ha möjlighet att vidta nödvändiga säkerhetsåtgärder vid användning av nya program och tjänster är det viktigt att ha kontinuerlig bevakning av utvecklingen på marknaden för mobila enheter och tjänster.

Vill du veta mer?

På www.datainspektionen.se/sakerhet kan du läsa mer om hur man kan skydda personuppgifter. På webbplatsen kan du också läsa mer om molntjänster och hur länge personuppgifter får bevaras.

Kontakta Datainspektionen

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

Datainspektionen