Datainspektionen

Datum
2013-05-08

Diarienr
646-2012

Socialnämnden i
Halmstad kommun
Box 230
301 06 Halmstad

Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av känsliga personuppgifter i mobila enheter

Datainspektionens beslut

Datainspektionen förelägger Socialnämnden i Halmstad kommun att

- ta fram funktioner för säker överföring av känsliga och integritetskänsliga personuppgifter över öppet nät,
- att kryptera känsliga och integritetskänsliga personuppgifter som lagras på mobila enheter,
- att införa någon form av stark autentisering för att medge användarna åtkomst till känsliga och integritetskänsliga personuppgifter.

Datainspektionen förutsätter att nämnden kompletterar sina instruktioner till användarna i enlighet med vad som framgår av Datainspektionens checklista.

Datainspektionen vill också påminna nämnden om vikten av att löpande göra riskidentifieringar och säkerhetsutvärderingar i en riskanalys.

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har granskat ett antal socialnämnders behandling av känsliga personuppgifter vid användning av mobila enheter. Syftet har varit att undersöka om nämnderna vidtagit tillräckliga säkerhetsåtgärder för att skydda personuppgifterna som behandlas. Socialnämnden i Halmstads kommun (nämnden) har beskrivit sin behandling av personuppgifter i mobila enheter genom att besvara en skriftlig enkät. Nämnden har till sitt yttrande

bifogat ”Anvisningar för läsplattor för socialnämnden” och en skriftlig ansvarsförbindelse.

Gällande regelverk
Säkerhet för personuppgifter som behandlas i socialtjänstens verksamhet regleras i 31 § personuppgiftslagen (PuL). Enligt denna bestämmelse är den personuppgiftsansvarige skyldig att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda uppgifterna som behandlas. Den ansvarige ska vara medveten om vilka risker en behandling medför och se till att vidta lämpliga säkerhetsåtgärder för att skydda uppgifterna. Känsligheten hos de personuppgifter som behandlas är en viktig faktor för skyddsnivån. Grundläggande vid överföring av känsliga personuppgifter via öppet nät är att uppgifterna ska skyddas genom exempelvis kryptering och att mottagarens, dvs. den som tar del av uppgifterna, identitet kan säkerställas. Mottagarens identitet ska säkerställas genom någon form av stark autentisering exempelvis e-legitimation, engångslösenord eller liknande.

Känsliga personuppgifter är uppgifter som avslöjar

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening, samt
- uppgifter som rör hälsa eller sexualliv (13 § PuL).

Uppgifter som inte klassificeras som känsliga enligt 13 § PuL kan ändå vara så pass integritetskänsliga att de, när det gäller kraven på säkerhetsåtgärder, ska jämställas med känsliga personuppgifter. Sådana uppgifter kan exempelvis vara uppgifter om lagöverträdelser, uppgifter om ömtåliga förhållanden eller annan information som rör den enskildes privata sfär.

Kravet på att teckna personuppgiftsbiträdesavtal finns i 30 § och bestämmelser om bevarande av personuppgifter regleras i 9 § i) PuL.

Allmänt om behandling av känsliga personuppgifter i mobila enheter
En organisation som vill hantera känsliga eller integritetskänsliga personuppgifter (härefter används enbart benämningen integritetskänsliga personuppgifter) i mobila enheter måste vara medveten om att detta kan innebära vissa särskilda risker. Risker som kan få svåra konsekvenser för en enskild vars personuppgifter riskerar att spridas. En mobil enhet, t.ex. en surfplatta eller en smart telefon, kommunicerar över öppna nätverk och används ofta utanför arbetsgivarens (den personuppgiftsansvarige) lokaler. Det går att utnyttja ett stort antal olika tjänster och ladda ner appar. 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 eller någon annan som tar del av uppgifterna. Den ansvarige måste, så långt det är möjligt, vidta säkerhetsåtgärder för att bara en behörig användare ska få åtkomst till personuppgifterna ifråga.

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 och utvärdering av utvecklingen på marknaden. Datainspektionen har tagit fram en checklista för att underlätta för den som planerar att använda sig av mobila enheter för överföring av integritetskänsliga personuppgifter. Den personuppgiftsansvariges skyldigheter är samma även för anställda som tillåts använda sina egna mobila enheter.

- **Riskanalys**
  När personuppgifter behandlas finns det alltid en risk att uppgifterna förstörs, ändras, går förlorade eller att någon obehörig får tillgång till dem. Detta kan bero på olyckshändelse eller att uppgifterna har hanterats på ett otillåtet sätt. För att så långt som möjligt skydda de uppgifter som behandlas måste den personuppgiftsansvarige, innan behandlingen påbörjas, genomföra en riskanalys. I riskanalysen 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.
- **Utbildning och instruktioner till användarna**
  Ta fram skriftliga instruktioner om hur det är tillåtet att använda mobila enheter. Instruktionerna bör exempelvis omfatta information om
  - hur integritetskänsliga personuppgifter får hanteras,
  - vilka säkerhetsinställningar som ska användas,
  - eventuella begränsningar för privat användning,
  - vilka appar som är tillåtna att ladda ned, samt
  - vilka konsekvenser otillåten användning kan medföra.

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

- **Behörighetsstyrning**
  För att minimera risken för spridning av integritetskänsliga personuppgifter är det viktigt att begränsa åtkomsten till uppgifterna i fråga. Enbart den som har behov av uppgifterna för att fullgöra sitt uppdrag eller sina arbetsuppgifter ska få åtkomst till uppgifterna.
- **Autentisering och kryptering**
  Om integritetskänsliga personuppgifter är eller kan göras åtkomliga över öppet nät krävs att inloggning sker med stark autentisering såsom e-legitimation, engångslösenord eller liknande. Även inloggning till administrationsgränssnitt kräver stark autentisering. När man använder öppna nät för att hantera integritetskänsliga personuppgifter, ska uppgifterna 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 molnet. 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.
- **Specifika säkerhetsåtgärder för mobila enheter**
  Användning av mobila enheter är förenad med särskilda säkerhetsrisker. För att hantera dessa behöver specifika säkerhetsåtgärder övervägas. Sådana åtgärder kan exempelvis vara att införa
    - 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.
- **Loggning och 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. För att få en förebyggande effekt ska användarna informeras om att loggar kontrolleras regelbundet.
- **Begränsa åtkomsten till personuppgifter**
  När det inte längre finns behov av att hålla personuppgifter tillgängliga via en mobil enhet ska den ansvarige se till att användarna inte längre får åtkomst till uppgifterna i fråga.

- **Personuppgiftsbiträdesavtal**
  Den som använder sig av en tredje part, ett s.k. personuppgiftsbiträde, för behandling av personuppgifter ska teckna ett personuppgifts-biträdesavtal med denna part. Avtalet ska bland annat innehålla instruktioner för biträdets personuppgiftsbehandling och vilka säkerhetsåtgärder biträdet ska vidta.

Datainspektionens bedömning och skäl för beslutet

1. *Allmänt*

Nämnden tillhandahåller mobila enheter (iPads) till samtliga nämnd-ledamöter för att kunna distribuera elektroniska handlingar inför möten. För att ta del av de elektroniska dokumenten måste applikationen Goodreader installeras på enheten.

Alla handlingar som är offentliga läggs på en särskild kommunal server. För att hämta handlingarna från servern måste ett lösenord i Goodreader kopplas till servern. För att användaren ska få åtkomst till handlingarna måste först enheten låsas upp med en fyrsiffrig PIN-kod. Därefter loggar användaren in i Goodreader med hjälp av användarnamn och lösenord. För överföring av handlingar med känsliga personuppgifter använder nämnden särskilda e-postadresser som skapats för ändamålet.

2. *Riskanalys*

Datainspektionen konstaterar att nämnden inte har genomfört en riskanalys. Datainspektionen rekommenderar att nämnden fortlöpande arbetar med riskidentifiering och säkerhetsutvärdering. Detta för att möta riskerna med hanteringen av integritetskänsliga personuppgifter i mobila enheter.

Nämnden har i samarbete med bland annat kommunjurist och IT-service utarbetat rutiner för användningen av de mobila enheterna. Det saknas dock en skriftlig riskanalys med identifiering av risker och analys av vilka säkerhets-åtgärder som är nödvändiga för att behandlingen av integritetskänsliga personuppgifter i mobila enheter ska vara förenlig med PuL.

3. *Instruktioner till användarna*

Datainspektionen ser positivt på att nämnden tagit fram skriftliga anvisningar och att användarna får skriva på en ansvarsförbindelse. Datainspektionen förutsätter att nämnden kompletterar sina anvisningar i enlighet med vad som framgår av Datainspektionens checklista.

Nämnden har tagit fram grundläggande instruktioner (anvisningar) till sina användare. Instruktionerna saknar dock bestämmelser om hur integritetskänsliga personuppgifter får hanteras, vilka säkerhetsinställningar som ska användas, eventuella begränsningar för privat användning, konsekvenser av otillåten användning m.m. För att underlätta för användarna och sätta ramar för vad som är tillåten användning måste nämnden komplettera sina instruktioner. Som ledning i detta arbete är det lämpligt att nämnden utgår ifrån vad som anges i Datainspektionens checklista.

Den personuppgiftsansvarige ska vidta lämpliga organisatoriska säkerhetsåtgärder (31 § PuL). Att utfärda instruktioner till användarna om exempelvis tillåten behandling av personuppgifter är en sådan säkerhetsåtgärd (se även 30 § PuL).

4. Autentisering och kryptering

Datainspektionen konstaterar att nämnden överför integritetskänsliga personuppgifter över öppet nät utan tillräcklig säkerhet.
Datainspektionen konstaterar att nämnden lagrar integritetskänsliga personuppgifter på mobila enheter utan tillräckligt krypteringsskydd.
Datainspektionen konstaterar också att åtkomst till integritetskänsliga personuppgifter medges efter att användarna identifierat sig med hjälp av användarnamn och lösenord.

Datainspektionen förelägger nämnden att ta fram funktioner för säker överföring av integritetskänsliga personuppgifter över öppet nät.
Datainspektionen förelägger nämnden att kryptera integritetskänsliga personuppgifter som lagras på mobila enheter.
Datainspektionen förelägger nämnden att införa någon form av stark autentisering för att medge användarna åtkomst till uppgifterna.

Handlingar som innehåller integritetskänsliga personuppgifter skickas till användarna via särskilda e-postadresser. Varje mottagare har ett e-postkonto som skapats för det specifika ändamålet att ta emot handlingar som innehåller integritetskänsliga personuppgifter. Handlingarna skickas som PDF-filer och för att kunna öppna filerna måste användarna ange ett lösenord. Lösenordet ändras av nämndsekreteraren inför varje sammanträde och måste anges varje gång användaren vill öppna dokumentet.

När man använder portabel IT-utrustning såsom mobila enheter är risken att utomstående kan komma åt uppgifterna särskilt stor. Integritetskänsliga

uppgifter måste därför skyddas med kryptering både vid överföring och vid lagring. Åtkomst till integritetskänsliga personuppgifter över öppet nät förutsätter också att mottagaren kan identifiera sig med någon form av stark autentisering exempelvis engångslösenord, e-legitimation eller liknande (31 § PuL).

5. *Radering av integritetskänsliga personuppgifter*

Datainspektionen ser positivt på att nämnden har tagit fram rutiner för radering av integritetskänsliga personuppgifter i de mobila enheterna.

Nämnden har som rutin att samtliga ledamöter vid ett sammanträdes slut raderar alla dokument som innehåller integritetskänsliga personuppgifter. Detta innebär att personuppgifterna lagras på mobila enheter högst sex dagar.

En grundläggande princip i personuppgiftslagen är att personuppgifter inte ska bevaras längre än vad som är nödvändigt i förhållande till ändamålen med behandlingen. När känsliga personuppgifter behandlas i mobila enheter är det extra viktigt att det finns rutiner för att ta bort uppgifterna när de inte längre är nödvändiga. För att minimera risken för spridning av uppgifterna bör man begränsa den information som hålls tillgänglig via mobila enheter så mycket som det är faktiskt och praktiskt möjligt.

Hur man överklagar
Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet skall ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Ingela Alverfors

Kopia till:
Personuppgiftsombudet