Datainspektionen

Datum
2013-05-08

Diarienr
643-2012

Socialnämnden
Järfälla kommun
177 80 Järfälla

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

Datainspektionens beslut

Datainspektionen förutsätter att Socialnämnden i Järfälla kommun, om nämnden ska behandla känsliga eller integritetskänsliga personuppgifter i mobila enheter;

- tar fram skriftliga instruktioner till användarna,
- säkerställer att inloggning till administrationsgränssnittet sker med hjälp av stark autentisering,
- tar fram rutiner för regelbunden logguppföljning,
- tar fram rutiner för att förhindra åtkomst till personuppgifter som inte längre behöver vara åtkomliga via mobila enheter, samt
- tecknar personuppgiftsbiträdesavtal med tjänsteleverantören (Netpublicator).

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.

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

Socialnämnden i Järfälla kommun (nämnden) har besvarat en skriftlig enkät. Datainspektionen har också genomfört en inspektion på plats där nämnden mer utförligt fått möjlighet att beskriva de säkerhetsåtgärder nämnden har vidtagit för att skydda personuppgifterna i de mobila enheterna.

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 erbjuder mobila enheter (iPad) till bland annat nämndledamöter för att de ska kunna ta del av elektroniska handlingar inför och under möten. Än så länge hanteras inte handlingar som innehåller integritetskänsliga personuppgifter i enheterna. Nämnden har dock för avsikt att behandla även sådana personuppgifter så fort de vet att säkerhetsåtgärderna de vidtagit är tillräckliga i förhållande till de krav som ställs i PuL.

För att göra handlingar åtkomliga i de mobila enheterna använder sig nämnden av en app som tillhandahålls av företaget Netpublicator. När dokumenten har publicerats är de också åtkomliga för användarna. Offentliga handlingar publiceras i en katalog för offentliga ärenden och sekretessbelagda handlingar publiceras i en annan katalog.

2. *Riskanalys*

Datainspektionen konstaterar att nämnden inte 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.

3. *Instruktioner till användarna*

Datainspektionen konstaterar att nämnden inte tagit fram instruktioner till användarna om hur det är tillåtet att använda de mobila enheterna. Datainspektionen förutsätter att nämnden tar fram skriftliga instruktioner till användarna.

Varje användare får en kort utbildning i hur surfplattan ska hanteras. I övrigt har nämnden inte några instruktioner eller rutiner för hur det är tillåtet att använda enheterna.

Avsaknaden av instruktioner kan innebära, eller i vart fall signalera, att det inte finns några begränsningar för hur de mobila enheterna får användas. Även om det helt saknas instruktioner för användningen är det ändå alltid nämnden, dvs. den personuppgiftsansvarige, som ansvarar för att skydda personuppgifterna som behandlas. Så är fallet även om en enskild användare hanterat sin mobila enhet på ett sätt som nämnden inte kunnat förutse.

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 inloggning till administrationsgränssnittet sker med hjälp av användarnamn och lösenord. Datainspektionen förutsätter att nämnden inför stark autentisering för åtkomst till integritetskänsliga personuppgifter i administrationsgränssnittet.

Nämndsekreteraren loggar in i administrationsgränssnittet med hjälp av användarnamn och lösenord på en https-krypterad webbsida. Via administrationsgränssnittet kommer åtkomst ges till handlingar som innehåller integritetskänsliga personuppgifter.

För att användaren ska få åtkomst till handlingarna i sekretesskatalogen måste denne logga in med ett engångslösenord som skickas via flash-SMS. Handlingarna strömmas sedan till den mobila enheten, tre sidor i taget. Så fort användaren stänger ner appen krävs en förnyad inloggning till sekretesskatalogen. I appen finns också ett inaktivitetslås som är förinställt på att stänga ner efter 15 minuters inaktivitet. Användaren kan dock justera tidsintervallet upp till maximala 30 minuter.

När en mobil enhet delas ut är den förinställd med ett yttre skärmlås i form av en PIN-kod. Användaren kan dock välja att inaktivera detta skärmlås eller justera tidsintervallet för när plattan ska släckas ned vid inaktivitet.

Åtkomst till integritetskänsliga personuppgifter över öppet nät förutsätter, enligt 31 § PuL, att inloggning sker med någon form av stark autentisering t.ex. engångslösenord, e-legitimation eller liknande.

5. *Logguppföljning och behörighetsstyrning*

Datainspektionen konstaterar att nämnden saknar rutiner för regelbunden logguppföljning. Datainspektionen förutsätter att nämnden inför regelbundna loggkontroller och informerar användarna om detta.

All aktivitet i den mobila enheten och i appen loggas. Nämnden har inga fastställda rutiner för uppföljning av loggarna men kontroller görs på förekommen anledning.

Det är nämndsekreteraren som administrerar behörighetstilldelningen till appen. För att få behörighet till sekretesskatalogen krävs att användaren har behov av uppgifterna i katalogen.

Krav på logguppföljning och behörighetsstyrning är sådana säkerhetsåtgärder som omfattas av 31 § PuL.

6. *Förhindra åtkomst till personuppgifter som inte längre är nödvändiga*

Datainspektionen konstaterar att nämnden saknar rutiner för förhindra åtkomst till personuppgifter som inte längre är nödvändiga att hålla tillgängliga via surfplattan. Datainspektionen förutsätter att nämnden inför rutiner för att förhindra åtkomst till sådana personuppgifter.

En grundläggande princip i personuppgiftslagen (9 § i)) är att personuppgifter inte ska bevaras längre än nödvändigt. När integritetskänsliga personuppgifter är åtkomliga via mobila enheter är det extra viktigt att det finns rutiner och funktioner för att förhindra åtkomst till sådana uppgifter som inte längre behöver vara tillgängliga via mobila enheterna. För att minimera risken för spridning av uppgifterna bör man begränsa den information som hålls tillgänglig via surfplattan så mycket som det är faktiskt och praktiskt möjligt. Även när det gäller personuppgifter som förekommer i offentliga handlingar måste nämnden ta ställning till hur länge dessa ska vara åtkomliga i de mobila enheterna.

7. *Personuppgiftsbiträdesavtal*

Datainspektionen konstaterar att nämnden inte tecknat personuppgiftsbiträdesavtal med Netpublicator. Datainspektionen förutsätter att nämnden snarast upprättar ett biträdesavtal med Netpublicator.

Överföring av handlingar sker med stöd av en app som utvecklats och underhålls av företaget Netpublicator som också behandlar personuppgifter åt nämnden. Biträdesavtal saknas mellan parterna. Personuppgiftslagen innehåller krav på att sådant ska finnas (30 § andra stycket).

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.

Detta beslut har fattats av tf generaldirektören Hans-Olof Lindblom i närvaro av tillsynschefen Erik Janzon, IT-säkerhetsspecialisten Mikael Ejner och juristen Ingela Alverfors (föredragande).

Hans-Olof Lindblom Ingela Alverfors

Kopia till:
Personuppgiftsombudet