Socialnämnden

§80 Dnr SN 2024-50

Revidering av socialnämndens riktlinjer för personuppgiftsbehandling Beslut

Socialnämnden antar förslag till revidering av riktlinjer för personuppgiftsbehandling.

Sammanfattning av ärendet

Socialnämnden antog riktlinjer för personuppgiftsbehandling 2021-09-30, § 97, SN 21-630 002. Dessa har sedan reviderats vid ett tillfälle 2022. Riktlinjerna har setts över utifrån nya bestämmelser i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten som trädde i kraft 2024-03-01 och det föreslås att riktlinjerna revideras för att tydliggöra ansvaret som den nya regleringen medför. Vidare föreslås att riktlinjerna revideras avseende vilket digitalt mötesverktyg som ska användas i klientmöten till att det av kommunen fastställda mötesverktyget ska användas i dessa situationer.

Beslutsunderlag

§171 SNAU Revidering av socialnämndens riktlinjer för personuppgiftsbehandling
Tjänsteutlåtande revidering av socialnämndens riktlinjer för personuppgiftsbehandling
Bilaga 1 Riktlinjer för personuppgiftsbehandling inom Socialnämnden i Norrtälje kommun

Beslutande sammanträde

Beslutsgång

Ordföranden frågar om socialnämnden kan besluta i enlighet med socialnämndens arbetsutskotts förslag, och finner att socialnämnden beslutar i enlighet med förslaget.

Beslutet ska skickas till

Förvaltningsdirektör

Enhetschef säkerhet, beredskap och systemförvaltning

Förvaltningsjurist

Paragrafen är justerad

Socialnämndens arbetsutskott

§171 Dnr SN 2024-50

Revidering av socialnämndens riktlinjer för personuppgiftsbehandling Beslut

Socialnämndens arbetsutskott föreslår

Socialnämnden antar förslag till revidering av riktlinjer för personuppgiftsbehandling.

Sammanfattning av ärendet

Socialnämnden antog riktlinjer för personuppgiftsbehandling 2021-09-30, § 97, SN 21-630 002. Dessa har sedan reviderats vid ett tillfälle 2022. Riktlinjerna har setts över utifrån nya bestämmelser i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten som trädde i kraft 2024-03-01 och det föreslås att riktlinjerna revideras för att tydliggöra ansvaret som den nya regleringen medför. Vidare föreslås att riktlinjerna revideras avseende vilket digitalt mötesverktyg som ska användas i klientmöten till att det av kommunen fastställda mötesverktyget ska användas i dessa situationer.

Beslutsunderlag

Tjänsteutlåtande revidering av socialnämndens riktlinjer för personuppgiftsbehandling
Bilaga 1 Riktlinjer för personuppgiftsbehandling inom Socialnämnden i Norrtälje kommun

Beslutande sammanträde

Beslutsgång

Ordföranden frågar om socialnämndens arbetsutskott kan besluta i enlighet med socialkontorets tjänsteutlåtandes förslag, och finner att socialnämndens arbetsutskott beslutar i enlighet med förslaget.

Beslutet ska skickas till

Förvaltningsdirektör

Enhetschef säkerhet, beredskap och systemförvaltning

Förvaltningsjurist

Paragrafen är justerad

NORRTÄLJE KOMMUN

TJÄNSTEUTLÅTANDE

Datum: 2024-03-25
Diarienummer: SN 2024-50

Förvaltning och avdelning

Handläggare: Therese Lantz
Titel: Förvaltningsjurist
E-post: Therese.lantz@norrtalje.se

Till: Socialnämndens arbetsutskott

Revidering av socialnämndens riktlinjer för personuppgiftsbehandling

Förslag till beslut

Socialnämnden antar förslag till revidering av riktlinjer för personuppgiftsbehandling.

Sammanfattning av tjänsteutlåtandet

Socialnämnden antog riktlinjer för personuppgiftsbehandling 2021-09-30, § 97, SN 21-630 002. Dessa har sedan reviderats vid ett tillfälle 2022. Riktlinjerna har setts över utifrån nya bestämmelser i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten som trädde i kraft 2024-03-01 och det föreslås att riktlinjerna revideras för att tydliggöra ansvaret som den nya regleringen medför. Vidare föreslås att riktlinjerna revideras avseende vilket digitalt mötesverktyg som ska användas i klientmöten till att det av kommunen fastställda mötesverktyget ska användas i dessa situationer.

Ärendet

Beskrivning

Socialnämnden antog riktlinjer för personuppgiftsbehandling 2021-09-30, § 97, SN 21-630 002. Dessa har sedan reviderats vid ett tillfälle 2022. Riktlinjerna har setts över utifrån nya bestämmelser i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten som trädde i kraft 2024-03-01 och reglerar hur tilldelning av behörigheter och kontroll av åtkomst till personuppgifter ska göras. Enligt den nya bestämmelsen (10 §) ska socialnämnden:

1. bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter,
2. se till att åtkomst till sådana uppgifter dokumenteras och kan kontrolleras, och
3. göra systematiska och återkommande kontroller av om någon obehörigen kommer åt sådana uppgifter.

Behörigheten enligt första stycket 1 ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter inom socialtjänsten.

Det föreslås att stycke 7.3 i riktlinjerna revideras för att tydliggöra detta ansvar.

I riktlinjerna anges vidare att ett visst mötesverktyg ska användas för digitala samtal med klienter och vid tjänstemöten där klienter diskuteras. Det föreslås att stycket 7.7.2 och 7.7.3 i riktlinjerna revideras till att i stället ange att det av kommunen fastställda mötesverktyget ska användas i dessa situationer.

Lagkrav

Ej tillämpligt.

Koppling till gällande styrdokument

Ej tillämpligt.

Ekonomiska konsekvenser och riskanalys

Ej tillämpligt.

Förvaltningens analys och slutsatser

Socialförvaltningen bedömer att revideringen behövs för att tydliggöra ansvaret som åligger socialnämnden gällande tilldelning av behörigheter och kontroll av åtkomst till personuppgifter.

Tidplaner

Ärendet tas upp i socialnämndens arbetsutskott 2024-04-18 och i socialnämnden 2024-04-25.

Nicklas Söderblom Gräns
Enhetschef enheten för Säkerhet, beredskap och systemförvaltning
Socialförvaltningen

Bilagor

Bilaga 1 Socialnämndens riktlinjer för personuppgiftsbehandling.

Beslut skickas till

Förvaltningsdirektör
Enhetschef säkerhet, beredskap och systemförvaltning
Förvaltningsjurist

NORRTÄLJE KOMMUN

Riktlinjer för personuppgiftsbehandling inom Socialnämnden i Norrtälje kommun

NORRTÄLJE KOMMUN

1 Styrande dokument om dataskydd och informationssäkerhet i kommunen

Kommunens policy och riktlinjer för säkerhetsarbete med tillhörande anvisningar och instruktioner styr hur samtliga medarbetare i Norrtälje kommun får hantera kommunens information. Nedanstående riktlinje reglerar hur socialnämndens medarbetare får behandla personuppgifter.

2 Behandling av personuppgifter inom socialnämnden

Dataskyddsförordningen (EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG, gäller för behandling av personuppgifter och det finns kompletterande bestämmelser i lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning – dataskyddslagen. Dataskyddsreglerna omfattar all behandling av personuppgifter som är helt eller delvis automatiserad. Den gäller även för manuell behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier, dvs. i ett register.

För verksamhet som bedrivs enligt SoL, LVU, LVM och LSS finns även kompletterande bestämmelser i lagen (2001:454) och förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten – SoLPuL och SoLPuLF. Här anges de preciseringar i förhållande till dataskyddsförordningen som är nödvändiga i socialtjänstens verksamhet. Om en fråga inte regleras i SoLPuL eller i den tillhörande förordningen får man gå till dataskyddsförordningen för att få reda på vad som gäller, exempelvis när det gäller de grundläggande kraven på behandling av personuppgifter, information till den registrerade, de registrerades rättigheter eller krav på säkerhet vid behandling av personuppgifter.

3 Begrepp

3.1 Personuppgifter

Personuppgifter är varje upplysning som avser en identifierad eller identifierbar fysisk person (en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

3.2 Känsliga personuppgifter och ömtåliga personuppgifter

Känsliga personuppgifter är personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Inom socialtjänsten förekommer uttrycket ömtåliga personuppgifter. Begreppet ”uppgifter om ömtåliga personliga förhållanden” omfattar, förutom vad som räknas som känsliga personuppgifter, även andra uppgifter om personliga förhållanden som kan förekomma inom socialtjänsten och vilkas behandling kan anses vara kränkande för den personliga integriteten. Det kan t.ex. vara uppgifter om försörjningsförmåga och familjeförhållanden. Personnummer och personuppgifter om lagöverträdelser som innefattar brott och domar i brottmål klassificeras inte som känsliga uppgifter enligt dataskyddsförordningen men bör ändå jämställas med känsliga personuppgifter.

3.3 Behandling av personuppgifter

Med behandling av personuppgifter avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.

4 Personuppgiftsansvar och organisation för arbetet med dataskydd inom socialnämnden

4.1 Personuppgiftsansvarig

Enligt reglemente för samtliga nämnder i Norrtälje kommun är varje nämnd ansvarig för att behandling av personuppgifter som sker i dess verksamhet, är förenlig med EU:s dataskyddsförordning (EU) 2016/679 och Lag (2018:218) om kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). När det i dessa riktlinjer hänvisas till personuppgiftsansvarig menas socialnämnden.

Den som är ansvarig för personuppgiftsbehandlingen är också ansvarig för säkerheten för personuppgifterna. Personuppgiftsansvarig ska se till att all behandling av personuppgifter i verksamheten uppfyller de krav som finns i lagar, förordningar och föreskrifter. Ansvaret gäller för så väl uppgifter om anställda och förtroendevalda som uppgifter om medborgare, klienter och affärskontakter. Ansvaret kvarstår även vid sådan personuppgiftsbehandling som sker för den personuppgiftsansvariges räkning via ett personuppgiftsbiträde (PuB), oftast en leverantör. Den personuppgiftsansvarige är skyldig att ersätta den registrerade för

sådan skada och kränkning av den personliga integriteten som en behandling i strid med dataskyddsförordningen har orsakat.

Personuppgiftsansvaret är omfattande och följande lista tjänar som vägledning för vad som ingår. Listan är ej uttömmande. Den personuppgiftsansvarige ansvarar för att:

- rådande lagstiftning som omfattar personuppgiftsbehandling följs, bl.a. se till att;
  - personuppgifter behandlas lagligt, på ett korrekt sätt och i enlighet med god sed,
  - personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifter samlades in,
  - de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen samt riktiga och, om det är nödvändigt, aktuella,
  - alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och
  - personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.
  - upprätthålla förteckning över samtliga processer/behandlingar av personuppgifter inklusive de system och kataloger/lagringsytor där personuppgifter lagras och behandlas,
  - utse och anmäla dataskyddsombud, stödja ombudet i utförandet av de uppgifter som dataskyddsförordningen föreskriver och se till att ombudet har tillräcklig kompetens,
  - försäkra sig om att förvaltningen och verksamheten har en ändamålsenlig organisation med tillräckliga resurser och dokumenterad ansvarsfördelning,
  - säkerställa att medarbetarna har nödvändig kompetens för att kunna följa personuppgiftslagstiftningen,
  - säkerställa att det tecknas personuppgiftsbiträdesavtal med de leverantörer och motsvarande som behandlar personuppgifter för verksamhetens räkning.

4.2 Organisation för dataskydd inom socialnämnden

4.2.1 Verksamhetsansvariga

Verksamhetsansvariga inom socialkontoret bestämmer ändamål och medel med personuppgiftsbehandlingarna. Verksamhetsansvariga är också i egenskap av informationsägare ansvariga för att i enlighet med socialnämndens hanteringsanvisningar bestämma hur och när information ska gallras samt se till att det blir gjort.

4.2.2 Dataskyddsombud

Dataskyddsombudets arbetsuppgifter och ställning styrs av lagstiftning. Ombudet har i uppdrag att bland annat granska efterlevnaden av dataskyddslagstiftningen och vara rådgivande. I uppdraget ingår bland annat följande;

- Utöva tillsyn över behandlingar och registerförteckning.
- Granska socialnämndens rutiner och riktlinjer inom området och ge förslag på förändringar.
- Ge råd om och granska konsekvensbedömningar.

- Utbilda och ge råd om behandlingar, juridik, rutiner och riktlinjer.
- Granska pub-avtal.
- Hantera incidenter i samverkan med dataskyddsansvarig.
- Vara kontaktpunkt mot Integritetsskyddsmyndigheten och de registrerade.
- Samverka med kommunstyrelsen i frågor om dataskydd och informationssäkerhet.

4.2.3 Dataskyddsansvarig

Dataskyddsansvarig har det operativa ansvaret för arbetet med dataskydd, IT-säkerhet och informationssäkerhet. Bland annat ska dataskyddsansvarig;

- Vara förvaltningens säkerhets- och beredskapssamordnare.
- Ta fram och revidera rutiner och riktlinjer inom området i samråd med dataskyddsombud.
- Utarbeta information till registrerade och göra den tillgänglig för de registrerade.
- Genomföra riskbedömningar och konsekvensbedömningar med verksamheten i samråd med dataskyddsombudet.
- Säkerställa att frågor om dataskydd, IT-säkerhet och informationssäkerhet implementeras i arbetet med utvecklingen av verksamhet och arbetsprocesser. Det gäller såväl vid införande av nya arbetsuppgifter eller processer som när nya verksamheter startas upp. Det gäller även vid utvecklande och införande av digitala tjänster, appar eller andra IT-system.
- Säkerställa att frågor om dataskydd, IT-säkerhet och informationssäkerhet beaktas vid upphandlingar.
- Upprätta pub-avtal i samråd med dataskyddsombud.
- Uppdatera registerförteckningen tillsammans med verksamheten.
- Hantera incidenter i samverkan med dataskyddsombud.
- I övrigt samverka och samråda med dataskyddsombud och digitaliseringsansvarig vid socialkontoret, IT-avdelningen, dataskyddsombud och informationssäkerhetsansvarig vid kommunstyrelsen i dessa frågor.

4.2.4 Kontaktperson för dataskydd

Inom varje avdelning ska en kontaktperson för dataskydd utses. Kontaktpersonen samverkar med dataskyddsansvarig och dataskyddsombud i dessa frågor och deltar i dataskyddsarbetet.

4.2.5 Medarbetare

Samtliga medarbetare har ett ansvar för att behandlingen av personuppgifter utförs på ett korrekt och lagligt sätt och i enlighet med socialnämndens riktlinjer.

5 Villkor för behandling av personuppgifter inom socialtjänsten

Bestämmelserna i dataskyddsförordningen, SoLPuL och SoLPuLF anger när det är tillåtet att inom socialtjänsten behandla personuppgifter helt eller delvis automatiserat (datoriserat) och i vissa manuella register. Om och vilka personuppgifter som ska samlas in eller lämnas ut i det enskilda fallet avgörs av annan lagstiftning, t.ex. TF, OSL, SoL och LSS. Bestämmelserna i dataskyddsförordningen, SoLPuL och SoLPuLF tillåter således att uppgifter som behövs i det enskilda fallet får behandlas inom socialtjänsten.

5.1 Behandling av personuppgifter kräver inte den enskildes samtycke

Syftet med bestämmelserna är att se till att socialtjänsten har möjlighet att utnyttja IT för att höja effektiviteten och kvaliteten i sitt arbete samtidigt som ett fullgott integritetsskydd garanteras. Det finns ett allmänintresse av att socialtjänstens verksamhet bedrivs effektivt och säkert. Även med beaktande av den enskildes krav på integritet bör därför personuppgifter få behandlas i verksamheten utan att den som uppgiften avser har gett sitt samtycke. En registrerad person har alltså inte rätt att motsätta sig att personuppgifter behandlas helt eller delvis automatiserat eller manuellt i ett register när behandlingen är tillåten enligt SoLPuL (6 § tredje stycket SoLPuL). Att samtycke inte behövs ger socialtjänsten möjlighet att utnyttja IT men utvidgar inte socialtjänstens möjlighet att registrera uppgifter om medborgarna.

5.2 Nödvändig behandling av personuppgifter

Enligt 6 § SoLPuL får personuppgifter behandlas endast om behandlingen är nödvändig för att arbetsuppgifter inom socialtjänsten ska kunna utföras samt för uppgiftslämnande som föreskrivs i lag eller förordning.

5.3 Personuppgifter som får behandlas

Socialtjänsten får enligt 7 § SoLPuL behandla samtliga kategorier av personuppgifter helt eller delvis automatiserat eller manuellt i ett register. Detta gäller även

- person- och samordningsnummer,
- känsliga personuppgifter som avses i art 9.1 dataskyddsförordningen, samt
- uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden.

Ovan nämnda personuppgifter får dock behandlas endast om de har lämnats i ett ärende eller är nödvändiga för verksamheten. Samtliga kategorier av personuppgifter får dock inte behandlas i alla olika sammanhang. När det gäller sammanställningar, sökbegrepp och samkörning finns det vissa begränsningar i lagen och förordningen.

5.4 Ändamål för behandlingen

I SoLPuLF finns regler som anger för vilka ändamål socialnämnden får behandla personuppgifter. För att behandlingen ska vara laglig krävs således att den faller

inom ramen för något av de ändamål som finns angivna där. Till exempel är behandling tillåten för handläggning av ärenden om bistånd och annat stöd samt för genomförande av beslut om bistånd.

5.5 Sökningar i verksamhetssystem

Vid handläggning av ärenden och vid sammanställningar får medarbetare enbart använda namn och personnummer som sökbegrepp vid sökning i ärendehanteringssystemet. Det är inte tillåtet att använda några andra sökbegrepp.

Undantag från denna regel finns bl.a. för tillsyn, uppföljning och utvärdering. Detta undantag är emellertid enbart tillämpligt för de personer som arbetar med dessa typer av arbetsuppgifter.

5.6 Sammanställningar av personuppgifter

Känsliga personuppgifter eller uppgifter i övrigt om ömtåliga personliga förhållanden får inte tas in i sammanställningar (listor) av personuppgifter. Med uppgifter om ömtåliga personliga förhållanden avses förutom känsliga personuppgifter även andra uppgifter om personliga förhållanden som kan förekomma inom socialtjänsten och vars behandling kan anses vara kränkande för den personliga integriteten. Det kan t.ex. vara uppgifter om försörjningsförmåga och familjeförhållanden.

Undantag finns för sammanställningar som görs bl.a. för uppföljning, utvärdering och kvalitetssäkring. Detta undantag är emellertid endast tillämpligt för personer som arbetar med dessa typer av arbetsuppgifter.

5.7 Uppdatering av personuppgifter

Den personuppgiftsansvarige är skyldig att se till att de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella. Det åligger den personuppgiftsansvarige att inom rimlig tid och både på begäran eller självmant rätta uppgifter som innehåller sakliga fel eller uppgifter som inte får behandlas. I samband med att en rättelse genomförts har socialnämnden en skyldighet att se till att tidigare felaktiga uppgifter tas bort.

Socialnämnden uppdaterar verksamhetssystemet Procapita/Lifecare varje morgon mot Skatteverkets befolkningsregister. De personuppgiftsbehandlingar i form av t ex. listor och sammanställningar som medarbetare själva upprättar ansvarar respektive medarbetare för att se till att personuppgifterna som behandlas är riktiga och aktuella.

5.8 Gallring av personuppgifter

Regler för gallring av handlingar inom socialtjänsten finns i 12 kap. socialtjänstlagen. Socialnämnden har antagit hanteringsanvisningar för de allmänna handlingar som finns i verksamheten. Hanteringsanvisningarna finns i Fyren.

För det fall medarbetare har upprättat egen lista eller sammanställning med personuppgifter ansvarar medarbetaren för att hålla listan korrekt och uppdaterad samt för att ta bort personuppgifter då de inte längre är relevanta för det ändamål som listan eller sammanställningen är avsedd för.

5.9 Skyldighet att föra förteckning

Socialnämnden ska föra en förteckning över alla personuppgiftsbehandlingar som finns i verksamheten. Medarbetare är skyldiga att samråda med dataskyddsansvarig innan ny behandling av personuppgifter påbörjas. Det kan handla om att medarbetare vill upprätta listor/sammanställningar eller att ett nytt IT-verktyg ska köpas in. Medarbetare ska sedan tillsammans med dataskyddsansvarig förteckna behandlingen i det register över personuppgiftsbehandlingar som finns. Medarbetare ska också anmäla till dataskyddsansvarig om befintlig behandling som finns upptagen i förteckningen förändras eller tas bort eller vid byte av kontaktperson för registret.

6 Den registrerades rättigheter

6.1 Information till registrerade

Den personuppgiftsansvarige ska självmant lämna den registrerade information om behandling av uppgifterna. I art 13-14 i dataskyddsförordningen listas vad man måste informera de personer vars uppgifter man behandlar. Informationen ska bl.a. innehålla uppgifter om ändamålen med och den rättsliga grunden för behandlingen. Även information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter ska anges. Det kan exempelvis vara uppgift om ändamålen med behandlingen, information om att man har rätt att ansöka om registerutdrag och att få felaktiga personuppgifter rättade. Den registrerade ska också få kontaktuppgifter till dataskyddsombudet och upplysas om rätten att klaga till Integritetsskyddsmyndigheten.

I Fyren finns information om GDPR som ska lämnas till de registrerade i samband med att de blir aktuella hos socialtjänsten.

När vi tar emot och skickar e-post behandlar vi också personuppgifter. Därför informerar vi om det i vår e-postsignatur. ”När du skickar e-post till Norrtälje kommun innebär det att vi behandlar dina personuppgifter. Läs mer om vad det innebär på norrtalje.se/personuppgifter.”

6.2 Rätt till registerutdrag

Den registrerade kan ansöka om att få veta vilka personuppgifter som behandlas om honom eller henne hos socialnämnden. En sådan ansökan kan antingen göras via Norrtälje kommuns e-tjänst för registerutdrag eller göras skriftligen till socialnämnden och vara undertecknad av den registrerade.

Den personuppgiftsansvarige är skyldig att lämna skriftlig information om bland annat:

- vilka uppgifter om den registrerade som behandlas,
- varifrån dessa uppgifter har hämtats,
- ändamålen med behandlingen och
- till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

6.3 Rätt att begära rättelse, radering och begränsning av uppgifter m.m.

Den registrerade har rätt att begära att uppgifter raderas eller rättas, samt att behandlingen av uppgifter begränsas eller i övrigt göra invändningar mot behandlingen. Den personuppgiftsansvarige är skyldig att på begäran av den registrerade snarast rätta eller radera sådana personuppgifter som inte har behandlats i enlighet med dataskyddsförordningen eller föreskrifter som har utfärdats med stöd av den.

6.4 Rätt till överklagbart beslut

Flera av rättigheterna för de registrerade som anges i dataskyddsförordningen gäller i begränsad omfattning i offentlig förvaltning. En begäran från den registrerade ska emellertid alltid prövas och den registrerade ska få ett beslut som kan överklagas om begäran nekas. Vilka beslut som kan överklagas framgår av 7 kap. 2 § dataskyddslagen (2018:2018). I Fyren finns processer för hur sådan begäran ska hanteras.

6.5 Rätt att klaga på behandlingen

Den registrerade har rätt att klaga på behandlingen till socialnämnden, till dataskyddsombudet och till Integritetsskyddsmyndigheten.

6.6 Skadestånd till den registrerade

Det finns förutsättningar för en person som har lidit skada på grund av att hans eller hennes personuppgifter har behandlats i strid med dataskyddsförordningen att få rätt till skadestånd av socialnämnden. Ersättningsskyldigheten kan sättas ner om den socialnämnden visar att felet inte berodde på nämnden.

7 Säkerhet för personuppgifter

7.1 Allmänt

Enligt artikel 5 f i dataskyddsförordningen ska den personuppgiftsansvarige behandla personuppgifter på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Enligt artikel 32 i dataskyddsförordningen ska den personuppgiftsansvarige vid behandling av personuppgifter vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, med beaktande av

- den senaste utvecklingen,
- genomförandekostnaderna och
- behandlingens art, omfattning, sammanhang och ändamål samt
- riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

Vidare ska den personuppgiftsansvarige vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvarige överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

7.2 Åtkomst till personuppgifter

Bestämmelser om sekretess utgör, tillsammans med reglerna i dataskyddsförordningen, en utgångspunkt för vilka uppgifter som någon får ta del av. Bara det att en person är aktuell inom socialtjänsten är en sådan uppgift som det råder sekretess för enligt 26 kap. 1 § offentlighets- och sekretesslagen (2009:400), och för att ett utlämnande ska kunna ske krävs det att det står klart att den enskilde eller någon närstående till denne inte lider men om uppgifterna lämnas ut.

Sekretessen gäller gentemot utomstående, såväl enskilda som myndigheter, men också inom en nämnd om det finns olika delar av nämndens verksamhet som har att tillämpa sinsemellan helt olika set av sekretessregler. Det innebär att anställda inom en verksamhetsgren inte får ta del av uppgifter inom en annan verksamhetsgren utan föregående sekretessprövning.

I 1 kap. 1 § SoL finns bestämmelser om att verksamheten ska vara grundad på respekt för den enskildes självbestämmanderätt och integritet.

I 11 kap. 5 § andra stycket SoL anges att handlingar som rör enskildas personliga förhållanden ska förvaras så att obehöriga inte får tillgång till dem. Denna regel är ett komplement till reglerna om sekretess och syftar till att skydda dem som vänder sig till socialtjänsten från obehörig insyn i privatlivet.

Som obehörig räknas var och en inom en socialnämnd som inte har legitim anledning att ta del av handlingen i sin tjänsteutövning. Medarbetare är således endast behöriga att ta del av det som de måste för att kunna göra sitt jobb.

Vidare innebär regeln i 6 § SoLPuL att medarbetare endast får behandla personuppgifter om det är nödvändigt för att arbetsuppgifter inom socialtjänsten ska kunna utföras samt för uppgiftslämnande som föreskrivs i lag eller förordning.

7.3 Behörighetstilldelning i verksamhetssystem och IT-stöd

Behörighetsstyrning kan uttryckas som arbete med att avgöra hur stor tillgång till uppgifter i ett verksamhetssystem som en person med en viss funktion eller roll får. Behörighetsstyrning är grundläggande för att se till att ingen obehörig åtkomst sker inom en organisation. Behörigheterna ska enligt 10 § SoLPuL begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter inom socialtjänsten.

Förvaltningsdirektör har delegation på att fatta beslut om villkor för tilldelning av behörigheter.

Enhetschef tilldelar och avslutar behörigheter i enlighet med fastställda villkor för en medarbetare.

Se mer om tilldelning, revidering och avslut av behörigheter i kommunens riktlinjer för säkerhetsarbete.

7.4 Hantering av uppgifter rörande personer med skyddade personuppgifter

”Skyddade personuppgifter” är Skatteverkets samlingsrubrik för de olika skyddsåtgärderna sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter inom folkbokföringen. Socialnämnden är skyldig att ha rutiner som säkerställer korrekt hantering av skyddade personuppgifter.

7.5 Dataintrång

Det är viktigt att komma ihåg att även om en medarbetare har teknisk behörighet att se och komma åt ett ärende i ett verksamhetssystem som t ex Procapita/Lifecare har medarbetaren endast befogenhet, alltså rätt att, ta del av det den måste för att kunna göra sitt jobb.

För det fall en medarbetare olovligen (utan befogenhet) bereder sig tillgång till uppgifter som är avsedda för automatisk behandling gör sig denne skyldig till dataintrång enligt 4 kap. 9 c § brottsbalken. Ett förfarande är olovligt om det sker utan stöd av den som har rätt att förfoga över uppgiften och saknar stöd i gällande rätt. Det krävs inte att intrånget sker i visst syfte utan det är själva intrånget som straffbeläggs. Även om någon gett samtycke till slagningen eller uppmanat en användare att kontrollera något om sig i ett verksamhetssystem kan det resultera i ansvar för dataintrång för den som berett sig tillgång till uppgifterna.

7.6 Kommunicering av personuppgifter

Socialnämnden är skyldig att skydda personuppgifter även när vi kommunicerar med invånare och andra.

Det är inte tillåtet att skicka känsliga personuppgifter via sms. Det är inte heller tillåtet att använda sociala medier eller chatforum för att kommunicera med klienter.

För mer information om på vilket sätt vi får skicka information se kommunens riktlinjer för säkerhetsarbete med tillhörande dokument.

7.7 Digitala möten

Vid genomförande av digitala möten behandlas personuppgifter. Förvaltningsdirektör har antagit Rutiner för möten vid Socialkontoret som finns tillgängliga i Fyren. Dessa rutiner reglerar säkerhet vid alla typer av möten, såväl fysiska som digitala. För digitala möten gäller vad som anges nedan.

7.7.1 Generellt kring digitala möten

Det är viktigt att säkerställa att det är rätt person du har mötet med. Vidare är det viktigt att vid mötet informera mötesdeltagare om vikten av att ingen obehörig kan höra samtalet.

7.7.2 Digitala möten med klienter

Möten med klienter innebär att både sekretesskyddade och integritetskänsliga personuppgifter behandlas och det förekommer också att känsliga personuppgifter avhandlas vid dessa möten. Vid användning av den kommunens säkra mötestjänst finns möjlighet för extern part att identifiera sig med bank-id eller via sms-kod. Av kommunen tillhandahållet säkert mötesverktyg ska användas, ingen annan digital mötestjänst får användas.

7.7.3 Digitala möten med kollegor/externa parter där sekretesskyddad information kan komma att avhandlas

Vid möten med kollegor/externa parter kan det ibland hanteras sekretesskyddade, integritetskänsliga och känsliga personuppgifter. Av kommunen tillhandahållet säkert mötesverktyget ska användas - ingen annan mötestjänst får användas.

7.8 Skicka personuppgifter till tredje land

Det är särskilt känsligt från ett integritetsskyddsperspektiv att lämna ifrån sig personuppgifter till ett annat land, som kanske inte har samma skydd för den personliga integriteten som vi har i Sverige. I 16 § SoLPuLF står det att det bara är i ärenden om fastställande av faderskap och om internationella adoptioner som det är tillåtet för socialtjänsten att föra över personuppgifter till så kallade tredjeland, det vill säga ett land som inte ingår i EU eller EES.

Gäller ärendet någonting annat får man alltså inte lämna ifrån sig uppgifter till tredjeland. Behöver man göra det i alla fall av någon anledning, bör man vända sig till Socialstyrelsen och/eller Integritetsskyddsmyndigheten för vägledning.

Observera att socialnämnden även ansvarar för personuppgifter som överförs till personuppgiftsbiträde, till exempel vid köp av tjänst eller system, och att socialnämnden då behöver utreda huruvida personuppgiftsbiträdet eller någon av dennes eventuella underbiträden har åtkomst till personuppgifterna från tredje land samt om så är fallet fastställa laglig grund för överföringen till tredje land samt i övrigt säkerställa att överföringen i övrigt är förenlig med dataskyddsförordningen.

7.9 Säker lagring/förvaring av personuppgifter

Personuppgifter måste förvaras/lagras säkert. För mer information om hur kommunens information får lagras, se kommunens riktlinjer för säkerhetsarbete.

7.9.1 Särskilt om e-post och gemensamma lagringsytor

E-posten är en kommunikationskanal och får inte vara en lagringsyta för personuppgifter. Handlingar som kommer in via e-post och innehåller uppgifter om klienter eller i övrigt känsliga eller ömtåliga personuppgifter ska skrivas ut och därefter raderas från e-posten. Det är viktigt att regelbundet, minst en gång i veckan, rensa e-posten från sådana personuppgifter. Observera att det gäller samtliga korgar i e-posten, dvs. inkorg, utkorg, skickat, arkiv och borttaget.

Gemensamma lagringsytor som Teams eller andra samarbetsytor får inte innehålla personuppgifter om klienter eller i övrigt känsliga eller ömtåliga personuppgifter.

7.10 Incidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över personuppgifter eller att rättigheterna inskränks. Dataskyddsförordningen ställer krav på att incidenter som sker med personuppgifter ska rapporteras och det innebär för socialnämndens del att alla incidenter ska rapporteras till dataskyddsombudet.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade eller på annat sätt kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter och det gäller för personuppgiftebehandling som sker både manuellt och tekniskt/digitalt/automatiskt. Det är bättre att anmäla en trolig incident för mycket än ingen alls till dataskyddsombudet. Dataskyddsombudet utreder det som inträffat. Är det en allvarligare incident ska den rapporteras till Integritetsskyddsmyndigheten inom 72 timmar.

Exempel på incidenter:

- Borttappad eller stulen dator, mobil, surfplatta och USB som innehåller personuppgifter. Det är en incident även om kryptering och lösenord finns.
- Lämnat personuppgifter till obehörig person via digitala enheter eller system/molntjänst/app
- Obehörig person har fått tillgång till personuppgifter
- Misstanke om dataintrång
- Någon har ändrat personuppgifter utan tillstånd
- Personuppgifterna är inte tillgängliga för den som behöver dem och det leder till negativa effekter för de registrerade.

7.11 Webbpublicering

Norrtälje kommun har antagit riktlinjer för hantering av personuppgifter i samband med webbpublicering: https://www.norrtalje.se/globalassets/kommun-och-politik/forfattningssamling/policydokument-och-riktlinjer/riktlinjer-for-hantering-av-personuppgifter-i-samband-med-webbpublicering.pdf

7.12 Sociala medier

Sociala medier ska inte användas för kommunikation med klienter. Däremot kan sociala medier vara ett sätt att sprida information.

7.13 Utbildning för medarbetare om personuppgiftsbehandling

Vid introduktion av ny medarbetare ska reglerna om personuppgiftsbehandling inom socialtjänsten och riktlinjerna för personuppgiftsbehandling inom socialnämnden gås igenom. Medarbetare ska dessutom årligen få en sådan utbildning.

8 Inför ny eller förändrad behandling av personuppgifter

8.1 Påbörja ny behandling av personuppgifter

Innan en ny behandling av personuppgifter påbörjas ska verksamhetsansvariga klargöra och fastställa bl.a. följande;

- Ändamål och syfte med behandlingen
- Vilka personuppgifter som måste behandlas för att ändamålet ska uppfyllas och att inte fler personuppgifter än nödvändigt behandlas
- Laglig grund för behandlingen
- Hur personuppgifterna ska lagras
- Vilka som ska ha åtkomst till personuppgifterna
- Hur länge personuppgifterna måste sparas för att ändamålet ska uppfyllas
- Hur och när radering av personuppgifterna ska ske
- Vilka säkerhetskrav som ska ställas på organisatoriska och tekniska lösningar samt på fysisk säkerhet

Observera att detta gäller såväl vid upprättande av nya listor eller sammanställningar som vid organisationsförändringar och införande/inköp/upphandling av tekniska hjälpmedel och verksamhetssystem eller annat IT-stöd.

8.2 Informationssäkerhet

Arbete med säker personuppgiftsbehandling är en del av ett informationssäkerhetsarbete. Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet. Inför upphandling av tekniska hjälpmedel, verksamhetssystem eller annat IT-stöd ska verksamhetsansvariga informationssäkerhetsklassa den information som ska behandlas för att kunna bedöma vilken nivå av säkerhet som ska ställas på administrativa, organisatoriska, tekniska lösningar samt på fysisk säkerhet. Socialnämnden använder SKR:s verktyg KLASSA för detta.

Utöver detta är det är också viktigt att ta ställning till om informationen som ska behandlas är sekretessreglerad och fastställa om behandlingen innebär att informationen kommer att lämnas ut, t ex till leverantören. Om behandlingen innebär att sekretessreglerade uppgifter ska lämnas ut måste socialnämnden antingen grunda utlämnandet på en sekretessbrytande bestämmelse eller genomföra skadeprövning som visar att det står klart att uppgifterna kan lämnas ut utan att någon enskild lider men.

För mer information om informationssäkerhet se kommunens riktlinjer för säkerhetsarbete.

8.3 Konsekvensbedömning enligt artikel 35 dataskyddsförordningen

Om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Det handlar om att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter. Syftet med konsekvensbedömning är att förebygga risker innan de uppkommer.

Om konsekvensbedömningen visar att det finns en kvarstående hög risk med personuppgiftsbehandlingen ska socialnämnden samråda med Integritetsskyddsmyndigheten innan behandlingen av personuppgifter påbörjas.

8.4 Personuppgiftsbiträdesavtal

I samband med överföring av personuppgifter till ett personuppgiftsbiträde, t ex en leverantör av system eller tjänster, ska socialnämnden upprätta ett personuppgiftsbiträdesavtal med personuppgiftsbiträdet. Avtalet blir en bilaga till huvudavtalet. Innehållet i avtalet regleras av dataskyddsförordningen. Den som är behörig att teckna huvudavtalet med leverantören för nämndens räkning är också behörig att teckna biträdesavtalet.

9 Dataskyddsombudets tillsyn

Dataskyddsombudet ska en gång per år, eller oftare vid behov, genomföra tillsyn över hur socialnämnden behandlar personuppgifter. Det kan t ex ske genom att utföra stickprov, eller genom en genomgång av registerförteckningen. Resultatet av tillsynen och förslag till eventuella åtgärder med anledning av det som kommit fram ska sammanställas i en rapport till förvaltningsdirektörenen och resultatet ska redovisas till ledningsgruppen.

10 Integritetsskyddsmyndighetens korrigerande befogenheter, sanktionsavgift

Integritetsskyddsmyndigheten är tillsynsmyndighet och kan t ex utfärda varning om planerad behandling sannolikt kommer att bryta mot bestämmelserna i dataskyddslagstiftning. Vidare kan Integritetsskyddsmyndigheten förelägga den personuppgiftsansvarige att vidta vissa åtgärder avseende behandling samt utfärda förbud mot behandling.

Integritetsskyddsmyndigheten kan påföra den personuppgiftsansvarige administrativa sanktionsavgifter för överträdelser av dataskyddsförordningen utöver eller i stället för övriga korrigerande åtgärder som Integritetsskyddsmyndigheten kan använda. För att bestämma hur hög sanktionsavgiften blir kommer Integritetsskyddsmyndigheten bland annat att titta på hur allvarlig överträdelsen är, hur stor skada som skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig. Integritetsskyddsmyndigheten ska se till att en eventuell sanktionsavgift är effektiv, proportionerlig och avskräckande.

För myndigheter uppgår avgiften för mindre allvarliga överträdelser till högst 5 miljoner kronor och för allvarligare överträdelser till högst 10 miljoner kronor.

Integritetsskyddsmyndigheten kan även utfärda varningar och reprimander. Dessutom kan Integritetsskyddsmyndigheten förelägga personuppgiftsansvariga att de måste upphöra med en viss behandling.

11 Referenser

Lagar

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG - Dataskyddsförordningen

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning – dataskyddslagen

Lag (2001:454) om behandling av personuppgifter inom socialtjänsten - SoLPuL

Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten - SoLPuLF

Handböcker från Socialstyrelsen

Handläggning och dokumentation inom socialtjänsten

NORRTÄLJE KOMMUN

Revisionshistorik

Version	Beskrivning	Datum	Antagna av	Författare
1.0	Första version	2021-09-30	Socialnämnden § 97, SN 21-630 002	Nicklas Grandin och Therese Lantz
1.1	Andra version	2022-08-18	Socialnämnden § 89, SN 21-630 002	Nicklas Grandin
1.2	Tredje version	2024-04-25	Socialnämnden § SN 24-50	Nicklas Söderblom Gräns