Säker personuppgiftsbehandling i socialtjänsten

Rättsläge och utgångspunkter

Socialstyrelsen

Publikationen finns som pdf på Socialstyrelsens webbplats. Publikationen kan också tas fram i alternativt format på begäran. Frågor om alternativa format skickas till alternativaformat@socialstyrelsen.se

Artikelnummer 2019-2-6

Publicerad www.socialstyrelsen.se, februari 2019

Förord

I den här rapporten redovisas rättsläget för socialtjänstens arbete med en säker personuppgiftsbehandling i socialtjänsten. Bakgrunden till rapporten är ett regeringsuppdrag, dnr S2018/04039/FST. En utgångspunkt är vad som har kommit fram i rapporten E-hälsa och välfärdsteknik i kommunerna 2018. Fokus är en beskrivning av vad som gäller för att se till att rätt personer får del av rätt uppgifter i socialtjänstens verksamheter. Rapporten är främst avsedd att användas som ett underlag för vidare diskussion i arbetet med säker personuppgiftsbehandling för socialtjänstens verksamheter. Socialstyrelsen planerar att införa ett uppdaterat avsnitt om socialtjänstens personuppgiftsbehandling en ny upplaga av handboken Handläggning och dokumentation inom socialtjänsten.

I arbetet med rapporten har Socialstyrelsen hämtat in synpunkter och kunskap från flera aktörer, bland annat från Datainspektionen. Förhoppningen är att rapporten ska kunna bidra till arbetet med att skapa ett starkt integritetsskydd för den enskilde och en effektiv kommunal förvaltning. När detta skrivs i januari 2019 har EU:s allmänna dataskyddsförordning, GDPR, ännu inte tillämpats i ett år. Det kommer att finnas anledning att vara uppmärksam på det som framöver kommer att uttalas av tillsynsmyndigheter och domstolar.

Cecilia Östergren har varit projektledare och Mariana Näslund Blixt har varit ansvarig enhetschef. Socialstyrelsen vill tacka alla som har bidragit med kunskap och värdefulla synpunkter under arbetet med uppdraget.

Olivia Wigzell
Generaldirektör

Innehåll

Sammanfattning

I rapporten redogörs för rättsläget hösten 2018 och för vad som har kommit fram vid möten med personer som är verksamma inom e-hälsa[1] och säker personuppgiftsbehandling. Det saknas nationell reglering av säkerhetsåtgärder specifikt för socialtjänstens personuppgiftsbehandling. Regelverket för säkerhet vid behandling av personuppgifter inom socialtjänsten är övergripande och anger inte i detalj vad som krävs av personuppgiftsansvariga. Bestämmelser om säkerhet vid behandling av personuppgifter inom socialtjänsten finns huvudsakligen i EU:s allmänna dataskyddsförordning[2], GDPR, nedan benämnd dataskyddsförordningen. Bestämmelserna i dataskyddsförordningen ska tillämpas direkt av personuppgiftsansvariga. Följande punkter sammanfattar vad som har kommit fram under arbetet med rapporten.

- Arbete med säker personuppgiftsbehandling är en del av ett informationssäkerhetsarbete.
- Verksamhetskunskap är värdefull i arbete med exempelvis behörighet till åtkomst i verksamhetssystem.
- Sekretessregler och ändamål med personuppgiftsbehandlingen är viktiga utgångspunkter för vem som ska få ta del av vilken information. Personuppgifter inom socialtjänsten får bara behandlas om det är nödvändigt för att arbetsuppgifter inom socialtjänsten ska kunna utföras.
- Personuppgiftsansvariga behöver kontinuerligt överväga säkerhetsåtgärdernas lämplighet och alltid kunna visa att de grundläggande principerna för personuppgiftsbehandling följs.
- Socialtjänsten behandlar personuppgifter som är känsliga på samma nivå som de personuppgifter som behandlas inom hälso- och sjukvården. Vid överväganden om säkerhetsåtgärder för personuppgiftsbehandling inom socialtjänsten kan rimligen jämförelser göras med vad som gäller för hälso- och sjukvården.

En av utgångspunkterna för arbetet med den här rapporten är skillnader i utveckling av möjligheter för personal att exempelvis läsa och dokumentera mobilt inom hälso- och sjukvården och socialtjänsten. Hälso- och sjukvårdens regelverk tillämpas av alla kommuner inom ramen för den kommunala hälso- och sjukvården. Det har förekommit att Riksdagens ombudsmän (JO) i tidigare tillsynsbeslut som berört socialtjänstens möjligheter att använda e-post har gjort jämförelser med det regelverk som avser hälso- och sjukvården[3]. Både hälso- och sjukvården och socialtjänsten behandlar känsliga personuppgifter. Därför görs jämförelser med hälso- och sjukvårdens regelverk

[1] E-hälsa är att använda digitala verktyg och utbyta information digitalt för att uppnå och bibehålla hälsa, se div.socialstyrlsen.se.

[2] 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.

[3] JO beslut 2015-12-29, dnr 1376-2013.

för personuppgiftsbehandling i fråga om bland annat autentisering, behörighetsstyrning och dokumentation av åtkomst. Dessa åtgärder är för hälso- och sjukvården reglerade i nationell rätt genom lag och föreskrift.

Bakgrund

Socialstyrelsens rapport E-hälsa och välfärdsteknik i kommunerna 2018 publicerades i april 2018 [1]. Rapporten visade på att andelen kommuner som kräver säker roll- och behörighetsidentifikation i samtliga verksamhetssystem endast var cirka 22 procent och att utvecklingen varit svag sedan 2015. Ökningen av andelen kommuner där all mobil personal kan ta del av information mobilt var också mindre inom socialtjänsten än inom hälso- och sjukvården.

Socialstyrelsen fick därefter ett regeringsuppdrag angående automatiserad personuppgiftsbehandling i socialtjänsten[4]. I uppdraget framhålls det som angeläget att klargöra vilka krav som behöver uppfyllas vid automatiserad behandling av personuppgifter för att behandlingen ska överensstämma med gällande rätt med hänsyn till ett starkt integritetsskydd för den enskilde och en effektiv kommunal förvaltning.

Syfte och mål

Det övergripande syftet för arbetet med denna rapport har varit att visa på hur en säker personuppgiftsbehandling som är i överensstämmelse med gällande rätt och anpassad till de kommunala verksamheternas behov av effektiv personuppgiftsbehandling kan se ut inom socialtjänsten. Målet med projektet har varit att ta fram en rapport som klargör gällande rätt för säker personuppgiftsbehandling inom socialtjänsten och att beskriva praktiskt arbete med säker personuppgiftsbehandling.

Omfattning och avgränsningar

Redogörelsen koncentreras till gällande rätt för automatiserad behandling av personuppgifter inom socialtjänsten med utgångspunkt från skydd för den enskildes integritet, en effektiv kommunal förvaltning och vad som kommit fram i rapporten E-hälsa och välfärdsteknik i kommunerna 2018. Personuppgiftsbehandling inom den kommunala hälso- och sjukvården omfattas delvis av ett annat regelverk och uppmärksammas inte särskilt men jämförelser med regelverket för hälso- och sjukvård görs i rapporten. Rapporten beskriver också kort olika delar av arbete med säker personuppgiftsbehandling och anger på ett övergripande plan hur arbetet kan gå till men behandlar inte tekniska lösningar.

Metod och genomförande

Arbetet med rapporten har omfattat studiebesök, samtal och möten med personer som arbetar inom bland annat verksamhetsutveckling, informationssä-

[4] Regeringsbeslut 2018-04-12, S2018/02375/FST

kerhet och systemförvaltning i kommuner i syfte att få en bild av hur praktiskt arbete med säker personuppgiftsbehandling bedrivs i socialtjänstens olika verksamheter. Eftersom det är fråga om information från ett begränsat antal kommuner dras inga generella slutsatser i rapporten om hur arbete med säker personuppgiftsbehandling går till. Möten har också hållits med regionala e-hälsosamordnare och företrädare för Sveriges Kommuner och Landsting (SKL), Inera, Myndigheten för samhällsskydd och beredskap (MSB) och Datainspektionen.

Agenda 2030 för hållbar utveckling

Säker personuppgiftsbehandling anknyter delvis till mål 10 i Agenda 2030 för hållbar utveckling. Mål 10 handlar om att minska olikheten inom och mellan länder. Delmål 10.2 är att möjliggöra och verka för att alla människor, oavsett ålder, kön, funktionsnedsättning, ras, etnicitet, ursprung, religion eller ekonomisk eller annan ställning, blir inkluderade i det sociala ekonomiska och politiska livet. Delmål 10.3 handlar om att säkerställa möjligheter och minska förekomsten av ojämlika utfall, bland annat genom att avskaffa diskriminerande lagstiftning, politik och praxis och främja lagstiftning, politik och åtgärder av lämpligt slag.

Grundläggande rättsliga förutsättningar

Dataskyddsförordningen

I dataskyddsförordningen finns de grundläggande reglerna för personuppgiftsbehandling. Tidigare gällde det dataskyddsdirektiv[5] som implementerats i svensk rätt genom personuppgiftslagen (1998:204), PuL. Dataskyddsförordningen tillämpas med ett fåtal undantag på behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Vad som är en personuppgift definieras i artikel 4 i dataskyddsförordningen. Lite förenklat är personuppgifter uppgifter som kan knytas till en levande person.

En förutsättning för att personuppgifter ska få behandlas är att det finns en rättslig grund i artikel 6 i dataskyddsförordningen. Om det finns en rättslig grund som tillåter personuppgiftsbehandlingen behöver personuppgiftsansvariga också beakta de grundläggande principerna i artikel 5 om laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, lagringsminimering, integritet och konfidentialitet.

I artikel 9 finns ett generellt förbud mot att behandla särskilda kategorier av uppgifter inklusive uppgifter om hälsa. För att få behandla sådana personuppgifter måste det finnas något tillämpligt undantag mot förbudet. Behandlingen måste också i vissa angivna fall även ha stöd i nationell rätt.

Dataskyddsförordningen är bindande och tillämpas direkt i varje medlemsstat. Nationell rätt får endast reglera frågor där dataskyddsförordningen medger kompletterande nationell reglering.

Vilka personuppgifter får socialtjänsten behandla?

I lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, SoLPuL, finns regler som anger när personuppgifter får behandlas inom socialtjänsten. En översyn av personuppgiftsbehandling inom Socialdepartementets verksamhetsområde har genomförts[6] och SoLPuL har utifrån översynen anpassats till dataskyddsförordningen.[7]

Enligt 6 § SoLPuL får socialtjänsten behandla personuppgifter bara om det är nödvändigt för att arbetsuppgifter inom socialtjänsten ska utföras. I förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten, SoLPuLF, begränsas[8] det övergripande ändamålet i 6 § SoLPuLF genom pre-

[5] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

[6] Se betänkandet Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning, SOU 2017:66.

[7] Se proposition 2017/18:171 Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning.

[8] Se prop. 2000/01:80 Ny socialtjänstlag m.m. s. 139 ff.

ciseringar av ändamål som tillåter personuppgiftsbehandling inom socialtjänsten för kommunala, statliga och privata aktörer. Ett exempel[9] på tillåtna ändamål för en kommunal myndighet är handläggning av ärenden om bistånd och annat stöd samt genomförande av beslut om bistånd, stödinsatser, vård och behandling samt annan social service som följer av bestämmelserna i SoL. Vid handläggning av ärenden enligt SoL gäller bland annat enligt 11 kap. 2 § första stycket SoL att en utredning inte ska göras mer omfattande än vad som är motiverat av omständigheterna i ärendet.

För socialtjänsten finns undantagen från förbud mot behandling av känsliga personuppgifter i artikel 9.2 b och h i dataskyddsförordningen. Där anges att det ska vara fråga om nödvändig behandling av känsliga personuppgifter för att personuppgiftsansvariga ska kunna

- fullgöra sina skyldigheter på områdena social trygghet och socialt skydd i den omfattning det är tillåtet enligt medlemsstaternas nationella rätt eller
- tillhandahålla social omsorg eller förvaltning av social omsorg och dess system på grundval av nationell rätt.

Enligt 7 § SoLPuL får känsliga personuppgifter behandlas om de har lämnats i ett ärende eller annars är nödvändigt för verksamheten.

Ansvar för att visa att dataskyddsförordningen följs

En nyhet som kommit med dataskyddsförordningen är krav på att kunna visa att förordningen följs. I artikel 5.2 fastslås att personuppgiftsansvariga ska kunna visa att de grundläggande principerna för personuppgiftsbehandling som anges i artikel 5.1 efterlevs. I artikel 24 anges också att den personuppgiftsansvariga ska genomföra lämpliga tekniska och organisatoriska åtgärder för att kunna visa att personuppgiftsbehandlingen utförs i enlighet med förordningen. Dessa åtgärder ska ses över och uppdateras vid behov. Om det står i proportion till behandlingen ska åtgärderna omfatta personuppgiftsansvarigas genomförande av lämpliga strategier för dataskydd. Tillämpning av godkända uppförandekoder eller godkända certifieringsmekanismer får användas för att visa att skyldigheterna är fullgjorda.

Säkerhetsåtgärder

Som en grundläggande princip gäller enligt artikel 5.1 f att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet.

I artikel 24 anges att personuppgiftsansvariga ska vidta tekniska och organisatoriska åtgärder för att säkerställa att behandlingen utförs i enlighet med förordningen. Det kan vara fråga om skyddsåtgärder som ingår i de it-system och administrativa stödrutiner som finns hos de personuppgiftsansvariga, exempelvis inbyggt dataskydd och dataskydd som standard, och åtgärder under behandlingen som en personuppgiftsansvarig anser behövs för att säkerställa en lämplig säkerhetsnivå.

I artikel 25 fastslås principerna om inbyggt dataskydd och dataskydd som standard. Datainspektionen informerar på webbplats om att inbyggt dataskydd innebär att hänsyn tas till integritetsskyddsreglerna redan när it-system

[9] Se 12 § 1 SoLPuLF.

och rutiner utformas. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Kravet på dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas [2].

I artikel 32 finns krav på att personuppgiftsansvariga ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. När personuppgiftsansvariga vidtar dessa åtgärder ska de beakta den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna av varierande sannolikhetsgrad och allvar. Vidare anges att det när det är lämpligt så kan åtgärderna avse pseudonymisering och kryptering av personuppgifter, förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och tjänsterna, förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident och ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

Dataskyddsförordningens reglering av säkerhetsåtgärder i artikel 32 beskriver mer utförligt vilka åtgärder som när det är lämpligt ska beaktas av personuppgiftsansvariga. Liksom som tidigare gällt enligt dataskyddsdirektivet och 31 § PuL så är det upp till personuppgiftsansvariga att bestämma vilka åtgärder som ska vidtas.

I SoLPuL anges inte krav på säkerhetsåtgärder vid behandling av personuppgifter.

Uppförandekoder och certifieringar

Anslutning till en godkänd uppförandekod eller en godkänd certifieringsmekanism får användas för att visa att krav för säkerhet i samband med personuppgiftsbehandling uppfylls. Det finns inte i dagsläget några godkända uppförandekoder eller certifieringsmekanismer som är av direkt och fullständig relevans för socialtjänstens arbete med just säker personuppgiftsbehandling. Det finns ISO-standarder i 27000-serien för informationssäkerhet [3]. I dessa finns detaljerade krav för exempelvis behörighetsstyrning.

Integritetskommittén anförde i sitt slutbetänkande SOU 2017:52 bl.a. följande. En uppförandekod i dataskyddsförordningens mening är en möjlighet för sammanslutningar som företräder personuppgiftsansvariga eller personuppgiftsbiträden att inom en viss bransch eller sektor specificera hur man i praktiken ska tillämpa dataskyddsförordningens bestämmelser. Ett samarbete mellan personuppgiftsansvariga inom hälso- och sjukvård och socialtjänst om gemensamma uppförandekoder skulle kunna vara ett sätt att lösa tillämpningsproblemen. Ett sätt att minska onödig spridning av känsliga personuppgifter inom både hälso- och sjukvården och socialtjänsten är att strukturera uppgifterna i informationssystemen så att användaren enklare kan ta del av

rätt information. Beroende på syftet med uppförandekoden och hur den utformas kan en uppförandekod om gemensam informationsstruktur vara en uppförandekod i dataskyddsförordningens mening.[10]

Vem utfärdar riktlinjer och stöd till dataskyddsförordningen?

Det är Europeiska dataskyddstyrelsen som har uppdraget att utfärda riktlinjer och rekommendationer till dataskyddsförordningen[11]. Dessutom har de nationella tillsynsmyndigheterna, i Sveriges fall Datainspektionen, också ett direkt uppdrag genom förordningen att bidra till en enhetlig tillämpning[12].

Vägledning för personuppgiftsansvarigas eller personuppgiftsbiträdens genomförande av lämpliga åtgärder och för påvisande av att behandlingen är förenlig med dataskyddsförordningen kan framför allt ges genom godkända uppförandekoder, godkänd certifiering, riktlinjer från Europeiska dataskyddsstyrelsen eller genom anvisningar från ett dataskyddsombud och då särskilt när det gäller att kartlägga den risk som är förknippad med behandlingen och bedöma dess ursprung, art, sannolikhetsgrad och allvar samt fastställa bästa praxis för att minska risken[13]. Även domstolspraxis kan klargöra tillämpningen av dataskyddsförordningen. Datainspektionen uppdaterar kontinuerligt information om personuppgiftsbehandling på sin webbplats.

Det kan finnas ett visst värde i att ta del av äldre domstolsavgöranden och tillsynsbeslut samt äldre information om säkerhet vid personuppgiftsbehandling. Det går däremot inte att helt förlita sig på äldre beslut och information eftersom den senaste utvecklingen ska beaktas när tekniska och organisatoriska åtgärder vidtas. Ett sätt att behandla personuppgifter som tidigare inte ansetts uppfylla kraven på säkerhet är rimligen inte ett sätt som är tillräckligt säkert idag.

Personlig integritet

Det finns ingen legaldefinition av personlig integritet.[14] Integritetskommittén hade ett uppdrag att utifrån ett individperspektiv kartlägga och analysera faktiska och potentiella risker för intrång i den personliga integriteten i samband med användning av it har fört utförliga resonemang om begreppet. En utgångspunkt för kommitténs arbete var den enskildes rätt till privata tankar och förtrolig kommunikation med andra, samt den enskildes möjligheter att själv avgöra vem som i olika sammanhang ska få ta del av uppgifter. I den rätten ligger även ett skydd mot registrering, spridning eller annan behandling av felaktiga kränkande eller påhittade uppgifter.[15]

[10] Integritetskommitténs slutbetänkande Så stärker vi den personliga integriteten, SOU 2017:52 s. 114.
[11] Artikel. 70.1.e.
[12] Artikel 51.2.
[13] Se skäl 77.
[14] För utförligt resonemang om begreppet personlig integritet se Integritetskommitténs delbetänkande Hur står det till med den personliga integriteten? SOU 2016:41 s. 135.ff.
[15] Se SOU 2016:41 s. 148.

Effektivisering – nya arbetssätt genom digitalisering

Digitalisering är en viktig del i utveckling och effektivisering av arbetssätt. Digitalisering används här i samma bemärkelse som i Vision e-hälsa 2025 och innefattar både informationsdigitalisering, dvs. processen där analog information förs över till digitalt format, och samhällelig digitalisering, dvs. den större samhällsprocess där olika former av it-stöd integreras allt tätare i verksamheter och påverkar dem i grunden [4]. Innan en tjänst utvecklas eller en del av en verksamhet digitaliseras är det förstås lämpligt att analysera vilken nytta digitaliseringen kan förväntas medföra. Digitalisering innebär nya arbetssätt och inte bara nya produkter. En åsikt som framhållits är att det inte räcker med att köpa ett system, det är också nödvändigt att arbeta systematiskt med säker och effektiv personuppgiftsbehandling.

Myndigheten för digital förvaltning, DIGG, har uppdraget att samordna och stödja den förvaltningsgemensamma digitaliseringen i syfte att göra den offentliga förvaltningen mer effektiv och ändamålsenlig och har tagit fram en vägledning i nyttorealisering. Nyttorealisering är ett aktivt och systematiskt arbete med att säkerställa och optimera nyttan med de förändringar som ska genomföras. I vägledningen beskrivs bland annat en process för nyttorealisering, beslutsunderlag och frågor att ta ställning till. En nytta kan realiseras först efter en beteendeförändring. Det räcker oftast inte att ta fram en ny produkt eller tjänst för att människor ska börja agera på ett nytt sätt. Ofta hamnar styrnings- och uppföljningsfokus på projekten och dess leveranser istället för på den önskvärda förändringen. Realisering av nyttor kräver också aktivt arbete med förändringsledning, dvs. arbete med att skapa engagemang och bestående förändring hos både medarbetare och de som nyttjar tjänsterna. De verksamheter som ska förändras måste vara aktiva kravställare på möjliggörarna som tas fram och också ansvara för att driva och skapa förändringarna som ska uppnås. Ett steg i rätt riktning är alltså att börja prata mer om förändringen och förändringsinsatsen än vilka produkter som ska utvecklas och hur projekten drivs [5]. Ekonomistyrningsverket har också material om effektivisering som tagits fram för den statliga förvaltningen.

Det gäller att se till att de system och den fysiska utrustning i form av olika bärbara enheter motsvarar de behov som finns och att de går att använda på det sätt som det är tänkt. I en kunskapsöversikt anges som exempel att det förekommer att handläggare som arbetar med utredningar av barn och unga inom individ- och familjeomsorgen utrustats med mobiltelefon och bärbar dator men där arbetet inte underlättats eftersom de inte fått tillgång till de digitala systemen annat än vid den stationära uppkopplingen [6].

I en studie pekas ärendehanteringssystemen[16] ut som ett område som verkar ha stor utvecklingspotential. Där anges att de med fördel skulle kunna

[16] Med ärendehanteringssystem avses i studien de system som socialtjänstens handläggare dagligen använder i arbete med dokumentation.

vara mer formbara så att de går att anpassa efter såväl brukarens som socialarbetarens behov. För att underlätta en sådan anpassning, bör olika system som inte är väl integrerade med varandra undvikas. Det finns en stor risk att följden av reglering, kompetens och ett organisatoriskt upplägg där olika förvaltningar ansvarar för sina egna upphandlingar blir ett lapptäcke av icke-kompatibla mjukvaror [7].

Användning av välfärdsteknik[17] ökar i kommunerna. Exempel på välfärdsteknik är digitala trygghetslarm, tillsyn via kamera och sensorer för påminnelser. Ett mål med användning av välfärdsteknik är högre kvalitet och effektivitet i vård och omsorg på samhällsnivå. Socialstyrelsen har gjort en intervjustudie som visat att trygghetskameror upplevs positivt av enskilda och anhöriga, att personalens arbetssituation förbättrats och att kommunen gör effektivitetsvinster [8]. SKL driver ett beställarnätverk för välfärdsteknik. Lösningar med välfärdsteknik kan innehålla personuppgifter om den tekniska lösningen registrerar händelser som kopplas till en person. Även för välfärdsteknik gäller att personuppgiftsansvariga ansvarar för bedömning av säkerhetsnivå för personuppgiftsbehandlingen.

Förutom insatser genom välfärdsteknik finns det i kommunerna också pågående arbete med automation i rutinmässiga beslutsprocesser, utveckling av e-tjänster med mera.

[17] Välfärdsteknik är enligt Socialstyrelsens termbank digital teknik som syftar till att bibehålla eller öka trygghet, aktivitet, delaktighet eller självständighet för en person som har eller löper förhöjd risk att få en funktionsnedsättning.

Informationssäkerhet

Arbete med säker personuppgiftsbehandling är också en del av ett informationssäkerhetsarbete.

Integritetskommittén angav 2017 att informationssäkerhetsarbete beskrivs ofta som ett arbete med att uppnå önskad nivå av riktig, tillgänglig, spårbar samt konfidentiell information i en verksamhet[18]. MSB beskriver på sin webbplats att informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet. I dataskyddsförordningen förtydligas vad som menas med informationssäkerhet i skäl 47. Enligt Datainspektionen handlar informationssäkerhet framför allt om att hindra information från att läcka ut, förvanskas och förstöras. Det handlar också om att rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Information ska inte kunna hamna i orätta händer och missbrukas. De registrerade ska veta vem som använder deras personuppgifter och varför [9].

SKL har angett följande angående kunskaper om kopplingen mellan säker personuppgiftsbehandling inom socialtjänstens verksamheter och kommunernas informationssäkerhetsarbete. Kommuner lägger upp sitt informationssäkerhetsarbete på olika sätt och har sin organisation ordnad på olika sätt. Det innebär att det kan finnas en central informationssäkerhetssamordnare på kommunledningsnivå som arbetar gentemot de olika nämnderna i kommunen, bland annat socialnämnden, och att informationssäkerhetsarbetet då samordnas för de olika nämndernas verksamhet. Det förekommer dock att de olika nämnderna i sina respektive förvaltningar har informationssäkerhetssamordnare som fungerar mer självständigt och fokuserar sitt arbete inom den förvaltningen. Olikheterna kan bero på kommunens storlek men även på hur nämnderna är indelade. Arbetet med dataskydd och rutiner för säker personuppgiftsbehandling har normalt sett hanterats nära informationssäkerhetsarbetet. Men även här förekommer variationer i genomförandet. Genom dataskyddsförordningen finns nu mer tydlig beskrivning av kompetenser och arbetsuppgifter men för just kommuner skulle det även finnas behov av vägledning för genomförande på en mer praktisk nivå, liknande de vägledningar som MSB har tagit fram i metodstödet för systematiskt informationssäkerhetsarbete.[19]

Övergripande rekommendationer om informationssäkerhet

MSB har ett metodstöd för systematiskt informationssäkerhetsarbete för den som arbetar med informationssäkerhet i en organisation oavsett verksamhetsområde och storlek på organisation. I metodstödet finns vägledningar, verktyg och exempel med mera. Metodstödet finns på webbplatsen informationssäkerhet.se.

[18] SOU 2017:52 s. 111.

[19] Se SKL:s PM 2018-11-27, Socialstyrelsens dnr 4.3-24299/2018-3.

MSB rekommenderade följande för kommuner i en analys från 2015 [10]:

- Identifiera vilken information som hanteras i verksamheten. Klassa sedan informationen efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet. Fokusera på den mest kritiska informationen/känsliga informationen som är i behov av höga skyddskrav.
- Etablera och implementera en process för riskhantering och se till att den är spridd inom kommunen.
- Identifiera informationssäkerhetsrisker och bedöm dessa.
- Se sedan till att omsätta riskanalysens resultat i beslut samt konkreta åtgärder. Dessa beslut samt åtgärder bör vara dokumenterade. Detta är särskilt viktigt för de kritiska processerna i kommunen!
- Kommunledningen bör säkra upp så att den blir kontinuerligt informerad om informationssäkerhetsriskerna och hanteringen av dessa, särskilt vad avser samhällsviktig verksamhet i kommunen.
- Genomför riskanalyser vid varje förändring i kommunens kritiska system.

Datainspektionens information om informationssäkerhet

Datainspektionen informerar om informationssäkerhet på sin webbplats [11]. När det gäller informationssäkerhet framhåller Datainspektionen att det är varje organisations ansvar att planera och genomföra säkerhetsarbetet så att det uppfyller kraven i dataskyddsförordningen på bästa sätt.

I fyra steg ger Datainspektionen stöd för att arbeta strukturerat och därmed uppfylla dataskyddsförordningens krav:

1. Utgå från grundläggande principer och rättslig grund.
2. Analysera skyddsobjekt, omfattning och risker.
3. Analysera åtgärder och lämplighet.
4. Motivera era beslut och dokumentera kontinuerligt.

Äldre allmänna råd om säkerhet för personuppgifter

Datainspektionen har tidigare beslutat om allmänna råd[20] om säkerhet för personuppgifter utifrån PuL. På Datainspektionens webbplats anges att även om de allmänna råden *Säkerhet för personuppgifter* är utformade utifrån personuppgiftslagens krav kan de framöver vid sidan av särskild information i anslutning till dataskyddsförordningen vara av värde. I dessa allmänna råd anges också att en personuppgiftsansvarig bör ha en fastställd säkerhetspolicy där organisationens säkerhetsstrategi, ansvarsfördelning och övergripande mål för säkerheten redovisas. Säkerhetspolicyn bör vara tydlig och lätt att förstå och tillämpa i praktiken. Om det finns anställda i verksamheten bör policyn vara skriftlig och allmänt tillgänglig i organisationen.

I ovanstående allmänna råd anges också bland annat följande åtgärder för att motverka otillbörlig åtkomst:

[20] Numera ej gällande allmänna råd om säkerhet för personuppgifter finns på Datainspektionens webbplats https://www.datainspektionen.se/globalassets/dokument/ovrigt/faktabroschyr-allmannarad-sakerhet.pdf

- Rutiner vid besök
- Rutiner och regler vid distansarbete och internetanvändning
- Rutiner för att ta bort inaktuella användarkonton

Integritetskänsliga uppgifter

Det finns uppgifter som kan betraktas som integritetskänsliga utan att tillhöra de särskilda kategorier av personuppgifter som tas upp i artikel 9.1 i dataskyddsförordningen. I Datainspektionens tidigare gällande allmänna råd om säkerhet för personuppgifter anges exempel på personuppgifter som normalt inte är att anse som känsliga – personuppgifter som följer av medlemskap, anställningsförhållande, kundförhållande, eller något därmed jämförligt förhållande. Som exempel på personuppgifter som normalt är att anse som känsliga nämns uppgifter angående ekonomisk hjälp eller vård inom socialtjänsten, enskilds personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet, uppgifter inom kreditupplysning eller inkassoverksamhet. Ett uttryck för att det är fråga om känsliga uppgifter kan vara att uppgifterna omfattas av sekretess. Sekretess gäller inom socialtjänsten för uppgift om enskilds personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men[21]. Redan den omständigheten att vissa känner till en för någon ömtålig uppgift kan i många fall anses vara tillräckligt för att medföra men[22].

Säkerhet handlar inte enbart om teknik

Det är inte tillräckligt att arbeta med it-säkerhet för att uppnå tillfredsställande informationssäkerhet. En medvetenhet om informationssäkerhet och genomtänkta arbetssätt för dem som behandlar personuppgifter är också viktigt. Något som också påtalas av regionala e-hälsosamordnare som Socialstyrelsen träffat är att ett problem kan vara brist på förståelse för säkerhetsaspekterna. Det gäller att förstå att värdet av exempelvis säker inloggning är skydd för information och inte bara ett sätt att komma in i systemet och komma åt informationen. Samverkan av arbete med informationssäkerhet organiseras olika i kommunerna. I någon region finns utpekade personer på varje förvaltning och på någon it-avdelning som samordnar informationssäkerhetsarbetet. Det finns också samordnare i mindre kommuner, resurserna ser dock olika ut. Arbete med informationssäkerhet kan vara ett uppdrag bland andra i tjänsten.

En insikt som framhållits av verksamma är den risk det innebär att ha verksamhetssystem som inte ger tillräckligt bra verktyg för anställda i det dagliga arbetet. Då finns risk för att personuppgifter därmed hamnar utanför verksamhetssystemen, kanske på en lokal hårddisk. Om personuppgifter hamnar utanför verksamhetssystem riskerar de att bli sökbara på sådant sätt som inte är tillåtet. Dessutom riskerar de att skyddas på fel säkerhetsnivå.

[21] 26 kap. 1 § offentlighets- och sekretesslagen (2009:400), OSL.
[22] Se proposition 1979/80:2 med förslag till sekretesslag m.m. s. 83.

Klassning av information

Över 200 kommuner och 6 landsting använder SKL:s verktyg Klassa som är ett verktyg där användaren kan informationssäkerhetsklassa och få en handlingsplan med förslag på informationssäkerhetskrav som stöd vid upphandling. Vid klassningen i verktyget informationssäkerhetsklassas information i ett verksamhetssystem utifrån vilka konsekvenser som uppstår om till exempel informationen inte kan nås, om den förvanskas eller om det finns brister i vem som får komma åt informationen. En del av arbetet med informationsklassning i verktyget innebär att fastställa säkerhetsnivåer för dessa konsekvenser utifrån *försumbar* till *synnerligen allvarlig* i tre olika perspektiv: konfidentialitet, riktighet och tillgänglighet [12].

I verktyget finns handlingsplaner för autentisering, behörighetsstyrning och åtkomstkontroll. I den handlingsplan som klassningen resulterar i finns förslag på säkerhetsåtgärder som verksamheten ska vidta för att uppnå rätt säkerhet i förhållande till den klassade nivån. I verktyget finns referenser till dataskyddsförordningen och ISO-standarder med mera. Om verksamheten är inne i en upphandling kan säkerhetskraven tas ut formulerade som upphandlingskrav. Socialtjänstens information om brukare hamnar liksom hälso- och sjukvårdens patientinformation oftast i den högsta säkerhetsnivån som går att använda med Klassa. Att genomföra den klassificeringsworkshop som ska göras i Klassa tar ca en halv dag.

En uppfattning från regionala e-hälsosamordnare är att informationsklassning ligger naturligt till för socialtjänstens verksamheter eftersom de har lång erfarenhet av att hantera sekretessbelagd information.

Klassning av information beskrivs också i MSB:s vägledning om att upphandla informationssäkert. Vägledningen riktar sig till alla typer av organisationer och fokuserar på hur informationssäkerhetskrav kan identifieras så att informationen hanteras på ett säkert sätt under upphandlingsarbetet och så att informationen som hanteras av den vara eller tjänst som upphandlas får lämpligt och bibehållet skydd. I vägledningen beskrivs bland annat hur arbete med initial och fördjupad informationsklassning och riskbedömning går till [13].

Jämförelse med hälso- och sjukvården

I patientdatalagen (2008:355), PDL, finns grundläggande bestämmelser om inre sekretess och elektronisk åtkomst inom en vårdgivares verksamhet. Det innebär att det finns bestämmelser om personuppgiftsbehandling för journalföring inom hälso- och sjukvården i lagstiftning där Socialstyrelsen har möjlighet att utfärda kompletterande föreskrifter. Sådana finns i Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter inom hälso- och sjukvården. Motsvarande regler finns inte i SoLPuL.

I 3 kap. HSLF-FS 2016:40 regleras frågor om bland annat informationssäkerhet. I 3 kap. 2 § anges att vårdgivaren genom ledningssystemet ska säkerställa att

- dokumenterade personuppgifter hos vårdgivaren är åtkomliga och användbara för den som är behörig (tillgänglighet),

- personuppgifterna är oförvanskade (riktighet),
- obehöriga inte ska kunna ta del av personuppgifterna (konfidentialitet), och
- åtgärder kan härledas till en användare (spårbarhet) i informationssystem som är helt eller delvis automatiserade.

I 3 kap. 4 § HSLF-FS 2016:40 anges också att vårdgivaren ska ansvara för att det finns en informationssäkerhetspolicy. Den ska ange vårdgivarens övergripande mål för och inriktning på verksamhetens arbete med informationssäkerhet i syfte att säkerställa personuppgifters tillgänglighet, riktighet, konfidentialitet och spårbarhet.

Skydd för den enskildes integritet genom uppgiftsminimering

Utgångspunkter

Förutom lämplig säkerhetsnivå enligt artikel 32 i dataskyddsförordningen ska personuppgiftsansvariga tillämpa de grundläggande principerna i artikel 5. En av de grundläggande principerna är uppgiftsminimering. Datainspektionen har på sin webbplats utvecklat vad som kan vara viktigt för personuppgiftsansvariga att tänka på när det gäller uppgiftsminimering [14]. Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Personuppgiftsansvariga ska aldrig behandla fler personuppgifter än vad som behövs och de personuppgifter som behandlas ska vara tydligt kopplade till ändamålet. Det är enligt Datainspektionen inte tillåtet att samla in personuppgifter för obestämda framtida behov för att de kan vara bra att ha. Datainspektionen uppmanar också till att avskilja personuppgifter som lagras utifrån lagkrav på bevarande från den dagliga verksamheten. Det kan exempelvis göras genom att separera informationen från ett visst ärendehanteringssystem eller genom att införa tekniska begränsningar av åtkomst och behörighet till samma system.

I det dagliga arbetet kan det förekomma olika situationer där uppgiftsminimering kan bli aktuellt. Det kan till exempel bli aktuellt när någon ska flytta in i en särskild boendeform och personalen intervjuar någon för att nedteckna en levnadsberättelse. Då kan det förekomma att den som intervjuar får information om en mängd olika personer. Dessa uppgifter om andra personer är kanske inte nödvändiga att dokumentera i levnadsberättelsen för att kunna genomföra beslutet om bistånd till särskild boendeform.

Stöd för att se till att behovet av information är tillgodosett

Det finns många författningsreglerade krav på dokumentation för socialtjänsten. Socialstyrelsen utvecklar gemensam informationsstruktur vilket är nationell informationsstruktur (NI) och det nationella fackspråket, till exempel, ICF, KSI och KVÅ. Syftet med utvecklingen är att ge stöd till ändamålsenlig och strukturerad dokumentation. Den gemensamma informationsstrukturen kan bidra till målet att varje behov av information tillgodoses. NI och fackspråket fungerar som en gemensam referens vid utveckling av en ändamålsenlig och strukturerad dokumentation, och bidrar med en gemensam förståelse för den aktuella verksamheten och den information som behöver hanteras kring en individ som är föremål för vård och omsorg.

Med NI som referens får både beställare och leverantörer av processorienterade it-stöd en gemensam bas för kravställning och utveckling. Detta ger bland annat bättre möjligheter att kombinera it-stöd från olika leverantörer som används i olika delar av individens process, vilket bidrar till konkurrensneutralitet. Detta gäller inte enbart vid upphandling av nya it-stöd utan

även vid arbetet med att anpassa och vidareutveckla it-stöd. En ändamålsenlig och strukturerad dokumentation i det här sammanhanget innebär att varje behov av information är tillgodosett [15].

Skydd för den enskildes integritet genom att rätt personer tar del av rätt uppgifter i verksamheten

Vem tar del av uppgifter – autentisering

Att autentisera innebär att kontrollera identitet vid kommunikation mellan två system. Ett begrepp som används i det sammanhanget är säker roll- och behörighetsidentifikation. Med det avses i de flesta fall en stark autentisering där inloggningen även kopplas till en roll [1]. Enligt regionala e-hälsosamordnare talas det ibland om identitet- och behörighetshantering istället för roll- och behörighetsidentifikation.

Datainspektionen har i sin tillsyn tidigare på ett enkelt sätt beskrivit stark autentisering som att åtkomst till uppgifterna föregås av en autentisering med två faktorer[23]. Datainspektionen har också anfört i ett beslut att om känsliga eller integritetskänsliga personuppgifter får lämnas ut över öppet nät, till exempel internet, så ska användarnas identitet säkerställas med en teknisk funktion som ger en stark autentisering. I beslutet beskrivs att önskvärda egenskaper hos starka autentiseringslösningar innefattar att användare ska kunna förlora kontrollen över en faktor utan att säkerheten för skyddsobjektet helt går förlorad samt att det ska gå att upptäcka och vidta åtgärder om det händer[24].I samtal med regionala e-hälsosamordnare framkommer att de har uppfattat att det förekommer föreställningar om att tvåfaktorsinloggning kan vara detsamma som att en användare har ett användarnamn och ett lösenord vilket inte är korrekt.

I Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården definieras stark autentisering som kontroll av uppgiven identitet på två olika sätt.

Det finns kammarrättsavgöranden som behandlat frågan om stark autentisering i förhållande till de regler som tidigare gällde. Kammarrätten konstaterade att även om uppgifter inte är känsliga personuppgifter enligt PuL så kan de ändå i många sammanhang vara av särskilt känslig natur. Kammarrätten ansåg vidare att personuppgiftsbehandlingen i fråga varit av känslig art eftersom den avsett uppgifter om enskildas personliga och ekonomiska förhållanden. Avgörandena behandlade inloggningskrav för tillgång till kreditupplysningsuppgifter genom internet. Att endast använda användarnamn och lösenord för att komma åt uppgifterna bedömdes inte uppfylla krav på tillräcklig säkerhetsnivå enligt 31 § PuL[25].

[23] Se. t.ex. Datainspektionens beslut 2015-07-03, dnr 643-2015.
[24] Se Datainspektionens beslut 2016-02-17, dnr 1805-2015.
[25] Kammarrätten i Stockholms avgöranden i målen 2415–2419-12 och 8237-12.

Enligt regionala e-hälsosamordnare som Socialstyrelsen varit i kontakt med så förekommer det inom socialtjänsten att anställda använder sitt personliga mobila BankID och att en del användare kan uppleva att det är smidigare än annan säker inloggning. En sådan lösning säger emellertid inte något om användarens roll på arbetsplatsen. Det förekommer att personal inom hemtjänsten har en personlig inloggning där utrustningen delas, exempelvis kan personligt BankID då finnas på en smart telefon eller surfplatta som flera använder.

Teknikneutralitet

Dataskyddsförordningen pekar inte ut någon särskild teknik som bör användas. I skäl 15 anges att skyddet för fysiska personer bör vara teknikneutralt och inte beroende av den teknik som används. Istället ska personuppgiftsansvariga beakta den senaste utvecklingen när de vidtar lämpliga tekniska åtgärder i samband med säkerhet vid personuppgiftsbehandling. Det finns inte heller någon för alla tider fastslagen särskild teknik för autentisering utan det sätt personuppgiftsansvarig väljer att använda ska ske just med beaktande av den senaste utvecklingen. Personuppgiftsansvariga behöver därför kontinuerligt analysera säkerhetsåtgärdernas lämplighet. Det är svårt att visa att den senaste utvecklingen har beaktats, vilket är ett krav enligt artikel 32, om det gått lång tid sedan övervägandena gjordes. Med den här regeln kommer det alltid att finnas ett behov av att återkommande analysera säkerheten i den teknik som används. En lösning som har fullgod säkerhet vid en viss tidpunkt kan vara otillräcklig vid en senare tidpunkt.

Olika lösningar för autentisering

E-legitimation

Legitimering med elektronisk legitimation kan ske för olika syften, exempelvis tillträde i syfte att elektroniskt få tillgång till uppgifter som får lämnas ut till den person som legitimerat sig och få skydd mot att någon annan släpps in under sken av att vara den som legitimerat sig.

I en del organisationer använder de anställda sin privata e-legitimation även i arbetet. I andra organisationer förser arbetsgivare sina anställda med e-legitimationer i tjänsten. Det finns många frågor att ta ställning till. Att använda en privat e-legitimation i tjänsten strider till exempel mot principen om att skilja mellan det som görs privat och i tjänsten. Det kan också finnas ett behov av en e-legitimation som inte exponerar den anställdes personuppgifter. En lösning är att arbetsgivaren förser sina anställda med e-legitimationer i tjänsten. E-legitimering i tjänsten förenklar även samarbetet mellan olika förvaltningar och myndigheter [16].

E-sam[26] anger i sin juridiska vägledning för införande av e-legitimering och e-underskrifter att riskerna för missbruk vid e-legitimering och e-underskrift har tekniskt minimerats genom olika skyddsåtgärder som hittills fungerat väl. Mindre nogräknade aktörer har istället inriktat sig på att antingen försöka komma över användares lösenord och e-legitimation för att missbruka

[26] E-sam är ett medlemsdrivet program för samverkan mellan 23 myndigheter och SKL. Samarbetet syfter till att underlätta och påskynda digitaliseringen av det offentliga Sverige.

dem eller förmå användare att medvetet eller omedvetet använda sin e-legitimation felaktigt så att identitetsintyg eller e-underskrivna handlingar missbrukas av en annan person. Missbruk av en e-legitimation genom att vilseleda innehavaren kan normalt inte förhindras tekniskt. Därför bör de som erbjuder en e-tjänst utforma dem så att straffrättsligt skydd tas tillvara fullt ut [17].

Myndigheten för digital förvaltning, DIGG, granskar och godkänner e-legitimationer för kvalitetsmärket Svensk e-legitimation. Företag och offentliga myndigheter som behöver e-legitimeringar i sina digitala tjänster har möjlighet att ställa krav på att eID-leverantören ska leverera lösningar som är godkända enligt tillitsramverket för svensk e-legitimation. E-legitimationsutfärdare kan dra nytta av kännetecknet Svensk e-legitimation i sin marknadsföring. På sikt är det tänkt att kännetecknet ska hjälpa användare och ansvariga för digitala tjänster att veta vilka inloggningsmetoder som det finns anledning att hysa tillit för [18].

En vanlig lösning för säker roll- och behörighetsidentifikation i kommunerna är de så kallade SITHS-korten som innehåller en personlig legitimation och ett tjänstecertifikat. För en mer utförlig beskrivning se Socialstyrelsens rapport Utveckling av e-hälsa i kommunerna Uppföljning av stimulansmedel 2014 [19]. Inera och Försäkringskassan har ett samverkansprojekt för att utveckla e-identitet för offentlig sektor, Efos, som är tänkt att ersätta SITHS-korten.

Jämförelse med hälso- och sjukvården

I 3 kap. 15 § HSLF-FS 2016:40 anges att om vårdgivaren använder öppna nät vid behandling av personuppgifter, ska denne ansvara för att överföring görs på ett sådant sätt att inte obehöriga kan ta del av dem och att elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering.

Om en vårdgivare gör uppgifter om patienter tillgängliga över öppna nät, exempelvis för att hälso- och sjukvårdspersonalen ska kunna utföra arbetsuppgifter på distans, måste det göras på ett sådant sätt att ingen obehörig kan nå uppgifterna. I praktiken innebär det bland annat att uppgifter om patienter måste överföras genom en krypterad förbindelse eller genom att kryptera uppgifterna. Teknikutvecklingen medför att krypteringsmetoderna hela tiden kan behöva förbättras för att minimera risken för obehörig åtkomst. För att en behörig användare ska få tillgång till personuppgifter via öppna nät måste vårdgivaren se till att åtkomsten föregås av en så kallad stark autentisering. Det innebär i praktiken att vårdgivaren använder inloggningslösningar som ställer krav på att identiteten kontrolleras **på minst två olika sätt**, exempelvis:

- med någonting användaren kan − till exempel lösenord eller pinkod
- med någonting användaren har − till exempel kodbox, certifikat, smartkort, engångskoder eller mobiltelefon
- med hjälp av användaren själv – till exempel fingeravtryck eller avläsning av iris [20].

Vem får ta del av vad – behörighetsstyrning

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 fundamentalt för att se till att ingen obehörig åtkomst sker inom en organisation.

Utgångspunkt från sekretessregler

Bestämmelser om sekretess utgör en utgångspunkt för vilka uppgifter som någon får ta del av. Enligt 26 kap. 1 § offentlighets- och sekretesslagen (2009:700), OSL, gäller sekretess inom socialtjänsten för en uppgift om enskilds personliga förhållanden om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider men. JO har uttryckt att det förhållandet att en enskild är aktuell hos en kommuns socialtjänst typiskt sett är en uppgift som skyddas av sekretess[27]. Enligt 8 kap. 2 § OSL gäller sekretess mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra. I förarbetena till denna bestämmelse om sekretess inom en myndighet förklaras att om det finns olika delar av en myndighets verksamhet som har att tillämpa sinsemellan helt olika set av sekretessbestämmelser är det fråga om olika verksamhetsgrenar i sekretesslagens mening[28]. 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 och i 6 § LSS finns bestämmelser om att verksamheten ska vara grundad på respekt för den enskildes självbestämmanderätt och integritet. Samtidigt finns det inom socialtjänsten en mängd uppgifter om en mängd personer registrerade i verksamhetssystemen.

I 11 kap. 5 § andra stycket SoL anges att handlingar ska förvaras så att obehöriga inte kan ta del av dem. Regeln är av väsentlig betydelse som ett komplement till reglerna om sekretess. På samma sätt som sekretessreglerna syftar den till att skydda dem som vänder sig till socialtjänsten från obehörig insyn i privatlivet. Regeln tar alltså närmast sikte på sådana handlingar som innehåller uppgifter som omfattas av sekretess. Obehörig är den som inte har legitim anledning att ta del av handlingen i sin tjänsteutövning[29].

Vem får se vad i kommunerna?

I hearing med kommunanställda framkom bland annat följande. Det finns exempel på att om en anställd ingår i beredskapsarbete så ges behörighet i system till flera förvaltningar inom en nämnds ansvarsområde medan det för andra anställda endast ges behörighet inom det område eller den verksamhet som den anställde har sina ärenden. För den som inte ingår i beredskapsarbete så finns inte åtkomst till övriga förvaltningars dokumentation men det går att se om en person förekommer och vilken handläggare den personen

[27] JO beslut 2013-01-10, dnr 5352-2011.
[28] Proposition 2008/09:150 Offentlighets- och sekretesslag, s. 359
[29] Se proposition. 1979/80:1 Om socialtjänsten, s. 563.

har. Handläggarna har inte tillgång till uppgifter från annan nämnds verksamhet. Systemförvaltarna upplever att handläggarna uppfattar en begränsad behörighet som gammalmodig och att det finns önskemål som går i riktning mot att öppna systemen mer. I någon kommun finns möjlighet för samtliga handläggare hos barn- och ungdomsförvaltningen att se ärenden hos vuxenförvaltningen. Den kommunen har då sett till att anpassa kontroll av åtkomsten till personuppgifter utifrån tillgången till dem. Det går dock inte att förlita sig på att justeringar av åtkomstkontroll innebär att det går att ge användarna åtkomst till fler uppgifter. Datainspektionen har i tillsynsbeslut som avsåg hälso- och sjukvården konstaterat att en vid behörighetstilldelning inte kan hanteras med hjälp av loggkontroll[30].

En kommun har nyligen förberett upphandling av verksamhetssystem genom att göra en grundlig riskanalys per verksamhetsgren av vilka roller som ska tilldelas vilken behörighet. I någon kommun genomfördes den hittills största riskanalysen i samband med en omorganisation.

Hur kan arbete med behörighetsstyrning se ut?

Det är i regel en enhetschef eller motsvarande som beslutar om behörighet för en anställd och en systemförvaltare eller motsvarande som ser till att den anställde får den beslutade behörigheten i ett visst verksamhetssystem.

När en person påbörjar en tjänst behöver personen få tillgång till de system som behövs för att personen ska kunna utföra sina arbetsuppgifter. Det märks av naturliga skäl om en anställd inte har tillgång till ett verksamhetssystem i tillräcklig stor utsträckning för att kunna utföra sina arbetsuppgifter. Det finns emellertid en risk att det inte märks på samma sätt när en person byter tjänst inom en och samma kommun eller nämnd och behörigheten inte längre motsvarar personens arbetsuppgifter. Liksom vid beslut om att en person ska tilldelas en viss behörighet när en tjänst tillträds så är det också viktigt att se till att behörigheten till aktuella verksamhetssystem upphör när personen avslutar en tjänst som inneburit behov av tillgång till viss information.

Det förekommer att löneadministratörer deltar i arbetet med behörighetsstyrning på så sätt att de uppmärksammar ansvarig chef i samband med att en anställd byter roll eller tjänst och att vederbörande chef i sin tur skickar signalen vidare till systemförvaltningen som ser till att den anställde har korrekt behörighet till verksamhetssystemen.

Det är förstås problematiskt om den tekniska möjligheten att styra behörigheter inte svarar mot behovet av styrning. En åsikt som kommer fram i samtal med verksamhetsföreträdare är att verksamhetskunskap är nödvändig för att kunna göra en analys av roll- och behörighetstilldelning – att arbete med att definiera rollerna och koppla dessa till en behörighet är en verksamhetsfråga och inte en it-fråga.

[30] Se Datainspektionens beslut 2018-05-23, dnr 2248-2017.

Tydlighet med vem som får ta del av vad – trygghet för den enskilde och de anställda

Den som olovligen bereder sig tillgång till uppgifter som är avsedda för automatisk behandling gör sig skyldig till dataintrång, se 4 kap. 9 c § brottsbalken. Ett förfarande är olovligt i det här sammanhanget om det sker utan tillstånd 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[31]. Även om någon gett samtycke till slagningen eller uppmanat en användare att kontrollera något om sig i ett verksamhetssystem så kan det resultera i ansvar för dataintrång för den som berett sig tillgång till uppgifterna[32]. Det är i sig en anledning till att se till att den som har behörighet till uppgifter i ett system känner till att det inte är tillåtet att bereda sig tillgång till andra uppgifter än de som behövs i arbetet. Det kan också vara så att utrednings- och anmälningsskyldigheter enligt 7 kap. 6 § och 14 kap. 6–7 §§ SoL (lex Sarah) aktualiseras[33].

Datainspektionen har i sin tillsyn konstaterat att en nämnd behandlat personuppgifter i strid med 6 § SoLPuL genom att ge behörighet till fler personuppgifter än vad som var nödvändigt för att kunna utföra arbete inom socialtjänsten. Datainspektionen har också ansett att det är rimligt att hemtjänstpersonal har teknisk tillgång till uppgifter om kunder inom olika geografiska områden men att det för att minska risken för intrång var nödvändigt att ge personalen anvisning av hur verksamhetssystemet fick användas så att både sekretess- och dataskyddsreglerna följdes[34].

Enligt artikel 32.2 dataskyddsförordningen ska den personuppgiftsansvarige i samband med bedömning av lämplig säkerhetsnivå bland annat ta särskild hänsyn till risker i synnerhet från bland annat obehörig åtkomst till personuppgifter.

Hur bedrivs ett behörighetsarbete på ett bra sätt?

Utgångspunkten blir naturligen att behörigheten ska begränsas till vad som behövs för att användaren ska kunna fullgöra sina arbetsuppgifter. Ju bredare behörighet en anställd har desto viktigare torde det vara med tydliga riktlinjer för när det är tillåtet att ta del av information i verksamhetssystemet. Behörighetstilldelning blir beroende av flera faktorer, som hur arbetsuppgifterna ser ut, hur många personer det är som har samma arbetsuppgifter och hur socialtjänsten är organiserad. Det är sällan möjligt att ge en exakt behörighet och ges en för låg behörighet riskerar arbetsuppgifter inom socialtjänsten att inte kunna utföras. En för hög behörighet kan medföra att personer får tillgång till personuppgifter och personliga förhållanden som de inte behöver ha tillgång till. Lösningen blir att hitta en lagom nivå som ger den anställde tillgång till de uppgifter hen kan komma att behöva ta del av och tydliga rutiner och instruktioner för den anställde om vad hen har rätt att ta del av.

[31] NJA 2014 s. 221.
[32] Se t.ex. Hovrätten för Skåne och Blekinges dom den 11 mars 2014 i mål B 1532-13.
[33] Se Inspektionen för vård och omsorgs beslut 2016-12-13, dnr 8.1.2-25162/2016-8.
[34] Datainspektionens beslut 2016-02-17, dnr 1805-2015.

Datainspektionen har i ett äldre informationsblad[35] som publicerats före tiden för dataskyddförordningens tillämpning angett bl.a. följande. Möjligheten att arbeta med och ta del av personuppgifter ska begränsas till de som behöver det för att kunna utföra sina arbetsuppgifter och sättet att arbeta måste vara utformat efter den principen. Ibland sker det naturligt eftersom olika avdelningar och projektgrupper ägnar sig åt sina respektive arbetsuppgifter. Men när uppgifterna samlas i samma it-system kan det bli lättare att kunna ta del av sådant som inte är relaterat till ens arbetsuppgifter. It-system bör därför vara utformade med behörighetsstyrning som kan anpassas efter organisationens arbetssätt. Här bör först arbetssättet kritiskt granskas för att förvissa sig om att det inte i sin tur är framtvingat av it-system med otillräcklig behörighetsstyrning eller andra brister i säkerhet och integritet. Ett idealiskt system för kontroll av behörigheter ska kunna se till att identifierade användare kommer åt rätt information enkelt men hindras att komma åt ”fel” information, det vill säga personuppgifter som inte behövs för att lösa ens arbetsuppgift [21].

Datainspektionen anger för hälso- och sjukvårdens område i sin vägledning om hur obefogad spridning av patientuppgifter förhindras att behovs- och riskanalyser har en avgörande betydelse för en väl avvägd behörighetstilldelning. Om en vårdgivare inte har genomfört dessa analyser före tilldelningen av behörigheter, riskerar vårdgivaren att ha en alltför vidsträckt och grovmaskig eller till och med felaktig behörighetstilldelning vilket leder till en obefogad spridning av patientuppgifter [22].

Jämförelse med hälso- och sjukvården

Det kan konstateras att det inte finns detaljerade regler om behörighetsstyrning och åtkomstkontroll inom socialtjänsten på samma sätt som inom hälso- och sjukvården[36]. Inom hälso- och sjukvården gäller krav i 4 kap. 2 § PDL att vårdgivaren ska bestämma villkor för tilldelning av behörighet för åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat och att sådan behörighet ska begränsas till vad som behövs för att den enskilde ska kunna fullgöra sina arbetsuppgifter inom hälso- och sjukvården. I 4 kap. 2 och 3 §§ HSLF-FS 2016:40 finns också mer preciserade regler om bland annat styrning av behörigheter som alla vårdgivare måste följa. Vårdgivaren ska ansvara för att varje användare tilldelas en individuell behörighet för åtkomst till personuppgifter. Vårdgivarens beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys. Rutiner ska tas fram för ändring, borttagning och regelbunden uppföljning av behörigheterna för att säkerställa att dessa är riktiga och aktuella.

Dokumentation av åtkomst till uppgifter

För att kunna kontrollera åtkomsten av olika uppgifter behöver det finnas behandlingshistorik. När historik över personuppgiftsbehandling förs är en grundläggande utgångspunkt att det behöver finnas möjligheter att utreda vem som har gjort vad med vilka uppgifter och när.

[35] Informationsbladet har markerats som ej gällande.
[36] Se t.ex. SOU 2014:23 s. 40.

Behov av loggуppföljning (loggning) följer av säkerhetskraven i artikel 5.1 f och artikel 32 i dataskyddsförordningen, liksom det tidigare följde av 31 § PuL eftersom personuppgiftsansvariga enligt dessa bestämmelser ska vidta tekniska och organisatoriska åtgärder för att skydda de uppgifter som behandlas.

Datainspektionens inte längre gällande, men till viss del alltjämt relevanta, allmänna råd om säkerhet för personuppgifter anger följande när det gäller behandlingshistorik:

- För att åtkomsten ska kunna kontrolleras bör det, beroende på känsligheten hos personuppgifterna, finnas en behandlingshistorik som sparas en viss tid.
- En behandlingshistorik behövs normalt inte om endast en person använder utrustningen.
- En behandlingshistorik bör följas upp och skyddas mot otillåtna ändringar.
- En behandlingshistorik bör normalt vara så detaljerad att den kan användas för att utreda felaktig eller obehörig användning av personuppgifter.
- Behandlingshistoriken bör, beroende på känsligheten hos personuppgifterna, ange till exempel läsning, ändring, utplåning eller kopiering av personuppgifter.
- En behandlingshistorik bör inte utformas eller utnyttjas så att den medför risk för intrång i personalens integritet.
- En behandlingshistorik har också en förebyggande funktion. Förutsättningen för det är att användarna informeras om att det förs en behandlingshistorik och att den kontrolleras.

Datainspektionen har i sin tillsyn tidigare anfört att det är viktigt att genomföra loggуppföljning för att på förekommen anledning eller genom stickprover kontrollera om det sker obehöriga slagningar. För att obehörig åtkomst ska upptäckas och för att loggуppföljningar ska få en preventiv effekt behövs rutiner för loggуppföljningar och tydlig information bör ges till personalen[37].

Jämförelse med hälso- och sjukvården

Enligt 4 kap. 3 § PDL ska en vårdgivare se till att åtkomst till sådana uppgifter om patienter som förs helt eller delvis automatiserat dokumenteras och kan kontrolleras. Vårdgivare ska göra systematiska och återkommande kontroller av om någon obehörigen kommer åt uppgifter. I 4 kap. 9 § HSLF-FS 2016:40 anges att vårdgivaren ska ansvara för att

- det av dokumentationen av åtkomsten (loggar) framgår vilka åtgärder som har vidtagits med uppgifter om en patient,
- det av loggarna framgår vid vilken vårdenhet eller vårdprocess åtgärderna vidtagits,
- det av loggarna framgår vid vilken tidpunkt åtgärderna vidtagits,
- användarens och patientens identitet framgår av loggarna,
- systematiska och återkommande stickprovskontroller av loggarna görs,
- kontroller av loggarna dokumenteras, och

[37] Se Datainspektionens beslut 2016-02-17, dnr 1805-2015.

- loggarna sparas minst fem år för att möjliggöra kontroll av åtkomsten till uppgifter om en patient.

Något om arbete med överföring av information

Enskildas tillgång till uppgifter inom socialtjänsten

I flera kommuner pågår arbete med att låta enskilda följa sin ansökan från början till slut. Det finns kommuner där det finns möjlighet att göra det exempelvis vid ansökningar om ekonomiskt bistånd för den som har BankID. De personerna kan då följa sitt ärende elektroniskt och inga beslut eller beräkningar på papper skickas då ut via vanlig post. Detta sätt att ta del av sitt ärende har emellertid inte fått önskat genomslag. Det har uppstått svårigheter när enskilda företräds av någon annan, exempelvis en god man.
Tillgänglighet på webbplatser regleras såväl internationellt som på EU-nivå och nationellt. En sammanfattning av detta finns i Socialstyrelsens rapport E-hälsa och välfärdsteknik i kommunerna 2018 s. 55–56 [1].

Varje kommun svarar för socialtjänsten inom sitt område och har det yttersta ansvaret för att enskilda får det stöd och den hjälp som de behöver. Som huvudregel är det den kommun där den enskilde vistas som ansvarar för stöd och hjälp. Alla som vistas i en kommun och som tar emot eller är har behov av insatser från socialtjänsten har emellertid inte BankID eller ens personnummer.

Vid en hearing som Socialstyrelsen har hållit hösten 2018 med kommunanställda it-samordnare med flera framhölls bland annat följande. När det gäller barn och hemlösa är det inte säkert att BankID är den lämpligaste lösningen för autentisering. Det behöver finnas beredskap även för dessa grupper. Det finns också en problematik när personal behöver använda sitt eget BankID vid inloggningar i vissa system och i kontakter mellan olika myndigheter. Säker e-post har inte slagit igenom som något som används i vardagen.

E-post och SMS

Det kan inträffa att enskilda vill skicka e-post direkt till en handläggare inom socialtjänsten. Datainspektionen informerar på sin webbplats om säkerhet för personuppgifter i e-post [23]. Informationen tar upp risker med e-post, personuppgiftsansvarigas ansvar och vad personuppgiftsansvariga måste göra. Av informationen framgår bland annat att krav på säkerhetsåtgärder inte kan frångås ens med den registrerades samtycke och att ökad användning av, och synkroniseringen med, mobila enheter gör att det blir svårare att tala om intern e-post eftersom sådana enheter ofta används utanför den egna organisationens lokaler och nätverk. Där anges också att personuppgiftsansvariga bör

- göra en risk- och sårbarhetsanalys avseende hanteringen av personuppgifter i e-post
- kartlägga riskbilden för e-posthanteringen. Om risken bedöms som hög, kan ni behöva göra en konsekvensbedömning
- införa lämpliga säkerhetsåtgärder vid behandling av personuppgifter i e-post

- fastställa policy för säkerhetshanteringen
- upprätta regler och rutiner
- informera och utbilda kontinuerligt avseende hanteringen av personuppgifter i e-post
- följa upp att regler och rutiner efterlevs och respekteras
- testa säkerheten regelbundet.

Riksdagens ombudsmän (JO) har 2015 uttalat i ett beslut att det på socialtjänstens område saknas föreskrifter som talar om i vilken utsträckning och under vilka förutsättningar e-post får användas men generellt gäller att det måste ställas höga krav på säkerhet vid överföring av uppgifter som omfattas av sekretess. JO anför i samma beslut att föreskrifter som finns på hälso- och sjukvårdsområdet kan ge viss vägledning när det gäller personuppgifter som inte är känsliga ur integritetssynpunkt. JO uttalar vidare att när ett e-postmeddelande innehåller känsliga personuppgifter krävs särskilda säkerhetsåtgärder för att säkerställa att rätt person får åtkomst till uppgifterna och att de överförs på ett säkert sätt, (t.ex. genom kryptering). Om det däremot rör sig om personuppgifter som inte är känsliga ur integritetssynpunkt bör viss kommunikation kunna ske även utan kryptering eller liknande. I samma beslut anges att för att undvika att integritetskänsliga uppgifter hanteras felaktigt bör det finnas tydliga rutiner inom socialnämnden som talar om i vilken utsträckning e-post får användas[38].

JO har i ett annat beslut uttalat att hantering av personuppgifter i e-post innefattar särskilda risker och att det därför krävs en hög säkerhetsnivå vid sådan hantering. Beslutet rör utbildningsområdet, ett område som liksom socialtjänsten saknar föreskrifter som talar om i vilken utsträckning och under vilka förutsättningar e-post får användas. I beslutet gör JO en jämförelse med bland annat de regler som gäller för hälso- och sjukvården[39].

I en förfrågan[40] till Datainspektionen 2011 som berörde användning av SMS inom socialtjänsten angav Datainspektionen att det som gäller inom hälso- och sjukvården för SMS-påminnelser kan utgöra en vägledning även för verksamhet inom socialtjänsten vid en bedömning av om det är möjlighet att skicka påminnelser via SMS om påminnelserna skickas under samma förutsättningar som de som anges i hälso- och sjukvårdens föreskrifter[41] och under förutsättning att hänsyn tas till eventuella specifika bestämmelser och/eller omständigheter som gäller för socialtjänstens verksamhet.

Datainspektionen har i ett beslut uppmärksammat ett landsting på att funktioner för webbmail och synkronisering till mobila enheter kan leda till att en distinktion mellan intern och extern e-post förlorar sin betydelse[42]. I ett annat beslut som rörde rutiner för e-post inom socialtjänsten angav Datainspektionen att om den ursprungliga informationen som skickas innehåller integritetskänsliga uppgifter så ska dessa skyddas på samma sätt som om de upprättats inom socialtjänsten. Ett alternativ är att utelämna sådana uppgifter ur svaret, det vill säga se till att den ursprungliga frågan inte följer med ett

[38] JO beslut 2015-12-29, dnr 1376-2013.
[39] JO beslut 2017-11-23, dnr 6466-2015.
[40] Datainspektionens frågesvar 2011-12-13, dnr 1370-2011.
[41] Datainspektionen hänvisade till den då gällande föreskriften SOSFS 2008:14 som ersatts av HSLF-FS 2016:40.
[42] Datainspektionens beslut 2011-12-12, dnr 750-2011.

svar som lämnas via e-post[43]. JO har utifrån de krav på säkerhetsåtgärder som gällde enligt 31 § PuL uttalat att kraven på säkerhet inte kan frångås ens med den registrerades samtycke[44].

Mobila enheter

Behov av att dokumentera mobilt kan finnas inom en mängd olika verksamhetsområden. Till övervägande del finns behovet för alla personalgrupper som har hela eller en del av sitt arbete mobilt, det vill säga ute hos kunder, brukare, patienter, inom hemtjänst med flera. Det finns även jourteam inom olika typer av social- och vårdverksamhet där sådant behov aktualiseras. Sådana jourteam kan vara organiserade genom kommunal samverkan, där behov för flera kommuner hanteras gemensamt. Beroende på hur socialnämndernas verksamhet är organiserad kan det även finnas socialt arbete inom arbetsmarknads- och integrationsområdet. Det är även vanligt att medarbetare inom olika delar av social omsorg och vård arbetar del av sin tid på mindre lokalkontor i stadsdelar och liknande där det kanske inte finns full åtkomst till it-resurser och där mobil åtkomst då blir nödvändig. Inom välfärdsteknik finns en mängd olika lösningar som kan ha en dokumentation, registrering av händelser eller kommunikationsutrustning inbyggd. Sådan utrustning kan vara placerad hos kunder, brukare, eller patienter och vara uppkopplad mot verksamhetssystem och också vara helt fristående.

För att utföra arbete med dokumentation på andra platser än på arbetsplatsens kontor, exempelvis i samband med ett hembesök, behövs någon form av mobil enhet. Det finns olika lösningar, allt från bärbara datorer till olika speciallösningar. Det finns hemtjänstpersonal som har telefoner där de dokumenterar att de utfört en insats. I kommuner pågår arbete med effektivisering av arbetssätt, exempelvis genom att arbeta med möjligheter att registrera insats via smart telefon. Från säkerhetsansvarig vid en kommun som arbetar med taligenkänning inom individ- och familjeomsorgen anförs att det vore önskvärt att ha en välfungerande sådan även inom äldre- och funktionshinderomsorg vid alla tillfällen när något behöver dokumenteras. Det skulle kunna innebära att handläggaren slipper dokumentera på bärbar dator eller liknande under ett möte och sparar tid i och med att det kan gå fortare att läsa in en text jämfört med att skriva ned den [24].

Det finns vissa svårigheter med mobila enheter, exempelvis svårigheter att säkerställa vem som förfogar över en mobiltelefon. En mobiltelefon är stöldbegärlig och lätt att tappa bort. Därigenom kan svårigheter uppstå när det gäller att säkerställa att endast behörig personal eller avsedd mottagare tar del av uppgifter i ett skickat SMS. Likaså kan det vara svårt att förhindra att ett SMS, medvetet eller omedvetet vidarebefordras utanför kretsen av behöriga mottagare[45].

Datainspektionen har i ett tillsynsbeslut uppmärksammat att funktioner för webbmail och synkronisering med mobila enheter kan leda till att skillnaden mellan intern och extern e-post förlorar sin betydelse[46].

[43] Datainspektionens beslut 2011-12-12, dnr 755-2011.
[44] Se JO beslut 2017-11-23, dnr 6466-2015 och där hänvisad litteratur.
[45] Datainspektionens frågesvar dnr 1370-2011.
[46] Datainspektionens beslut 2011-12-12, Dnr 750-211.

Den teknik som används behöver vara anpassad för det arbete som ska utföras. Om till exempel en surfplatta delas av flera användare så uppstår problem om historik ligger kvar när en annan person ska använda den och inte behöver historiken för att utföra sina arbetsuppgifter.

Datainspektionen har informerat om användning av mobila enheter i ett informationsblad som inte längre är gällande [25]. Informationsbladet behandlar bland annat särskilda risker som användning av mobila enheter innebär. Det anges exempelvis att mobila enheter kan kommunicera över öppna nät, användas utanför arbetsgivarens lokaler och att de som regel är stöldbegärlig egendom. Delar av innehållet i informationsbladet kan därför alltjämt vara av värde för personuppgiftsansvariga som använder mobila enheter i sin verksamhet.

En jämförelse med hälso- och sjukvården

För hälso- och sjukvården gäller att vårdgivaren ska se till att överföring av personuppgifter över öppna nät görs på ett sådant sätt att obehöriga inte kan ta del av dem och att elektronisk åtkomst eller direktåtkomst till uppgifterna föregås av stark autentisering. För påminnelser och kallelser till vård och behandling som riktar sig till patienter finns det undantag från kraven på säker överföring. Efter att ha gjort en behovs- och riskanalys får vårdgivaren besluta om undantag från krav som gäller för överföring av uppgifter över öppna nät. Behovs- och riskanalysen och beslutet ska dokumenteras. Sådana påminnelser och kallelser får endast göras efter medgivande av patienten och överföringen får inte avslöja detaljer om hälsotillstånd eller andra personliga förhållanden. Vårdgivaren bör ha rutiner som säkerställer att patientens kontaktuppgifter är riktiga och aktuella, se 3 kap. 15–17 §§ HSLF-FS 2016:40 och därtill hörande allmänna råd.

Slutsatser

Regelverket för säkerhet vid behandling av personuppgifter inom socialtjänsten är övergripande och anger inte i detalj vad som krävs av personuppgiftsansvariga. Eftersom det endast är ett mindre antal verksamhetsföreträdare som kunskaper om det praktiska arbetet hämtats in från så dras inte några generella slutsatser av hur arbetet med säker personuppgiftsbehandling ser ut i kommunerna. Följande förtjänar ändå att uppmärksammas.

- Den senaste utvecklingen ska beaktas vid övervägande av säkerhetsåtgärder. Arbete med säker personuppgiftsbehandling behöver därför bedrivas kontinuerligt. En lösning som har fullgod säkerhet vid en viss tidpunkt kan vara otillräcklig vid en senare tidpunkt.
- För att följa dataskyddsförordningen och se till att rätt personer ska ta del av rätt uppgifter räcker det inte med att köpa ett system eller en autentiseringslösning. Varje personuppgiftsansvarig behöver analysera behov och risker med personuppgiftsbehandlingen för sin verksamhet.
- De som arbetar inom socialtjänsten har kännedom om den information som de hanterar, vilka uppgifter som behöver dokumenteras och vad informationen ska användas till. Verksamhetskunskap är värdefullt i det säkerhetsarbete som är kopplat till den information som finns i verksamhetssystemen.
- Sekretessreglerna och reglerna för ändamålet med personuppgiftsbehandlingen är viktiga utgångspunkter för vem som ska få ta del av vilken information. Personuppgifter inom socialtjänsten får bara behandlas om det är nödvändigt för att arbetsuppgifter inom socialtjänsten ska kunna utföras. För att en anställd inom socialtjänsten ska vara behörig att ha en viss tillgång till uppgifter krävs därför att socialtjänsten har behov av att den anställde har sådan tillgång.
- De personuppgifter som socialtjänsten behandlar kan ofta innehålla uppgifter om hälsa som är en sådan särskild kategori av uppgifter som har ett starkare skydd i dataskyddförordningen. Dessutom är i regel uppgifterna som behandlas integritetskänsliga även om de inte tillhör de särskilda kategorierna i dataskyddsförordningen. Ett uttryck för att det är fråga om uppgifter som normalt sett är att anse som känsliga är att uppgifterna omfattas av sekretess. De uppgifter om personliga förhållanden som socialtjänsten behandlar omfattas som huvudregel av sekretess. Det är därför rimligt att säkerhetsåtgärder som vidtas inom socialtjänsten sker på en nivå som motsvarar vad som gäller för personuppgiftsbehandling inom hälso- och sjukvården.
- Det går inte att visa vad som har beaktats om det arbete med säker personuppgiftsbehandling som genomförts inte har dokumenterats. Personuppgiftsansvariga behöver därför se till att arbetet med säker personuppgiftsbehandling dokumenteras i sådan utsträckning som behövs för att alltid kunna visa att de grundläggande principerna för personuppgiftsbehandling har följts.

Referenser

1. E-hälsa och välfärdsteknik i kommunerna 2018 – Redovisning av en uppföljning av utvecklingen inom e-hälsa och välfärdsteknik i kommunerna. Socialstyrelsen; 2018.
2. Datainspektionen. Inbyggt dataskydd och dataskydd som standard. Hämtad 2018-12-04 från https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/inbyggt-dataskydd-och-dataskydd-som-standard/.
3. SIS. Informationssäkerhet. Hämtad 2018-12-04 från https://www.sis.se/utbildning/vrautbildningsomrden/informationsskerhet/.
4. Vision e-hälsa 2025 – gemensamma utgångspunkter för digitalisering i socialtjänst och hälso- och sjukvård. Regeringskansliet och SKL; 2016.
5. Vägledning i Nyttorealisering, version 2.0. Myndigheten för digital förvaltning; 2018.
6. Larsson S, Svensson L. Digitalisering och socialt arbete – en kunskapsöversikt. Lunds universitet; 2017.
7. Larsson S, Svensson L. Digitalisering av kommunal socialtjänst En empirisk studie av en organisation och profession i förändring. FoU Helsingborg; 2018.
8. Välfärdsteknik – En studie av användningen av trygghetskameror och GPS-larm i 12 kommuner. Socialstyrelsen; 2018.
9. Datainspektionen. Informationssäkerhet. Hämtad 2018-12-04 från https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/.
10. Informationssäkerheten i Sveriges kommuner – Analys och rekommendationer utifrån MSB:s kommunenkät. Myndigheten för Samhällsskydd och beredskap; 2015.
11. Datainspektionen. Informationssäkerhet. Hämtad 2018-12-04 från https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/.
12. SKL. Klassa Informationsklassning och handlingsplan. Hämtad 2018-12-04 från https://klassa-info.skl.se/.
13. Upphandla informationssäkert – en vägledning. MSB; 2018.
14. Datainspektionen. Uppgiftsminimering. Hämtad 2018-12-04 från https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/#Uppgiftsminimering.
15. Socialstyrelsen. Nationell e-hälsa och gemensam informationsstruktur. Hämtad 2018-12-19 från http://www.socialstyrelsen.se/nationellehalsa/.
16. Myndigheten för digital förvaltning. E-legitimering som offentlig tjänsteman. Hämtad 2018-12-04 från https://www.elegnamnden.se/elegitimering/elegitimeringitjansten/elegitimeringsomoffentligtjansteman.4.4498694515fe27cdbcff5.html.

17. Juridisk vägledning för införande av e-legitimering och e-underskrifter 1.1. e-Sam; 2018.
18. Myndigheten för digital förvaltning. Frågor och svar, Vilka berörs. Hämtad 2018-12-04 från https://elegnamnden.se/vanligafragor/frago-rochsvar.4.4498694515fe27cdbcf157.html.
19. Utveckling av e-hälsa i kommunerna Uppföljning av stimulansmedel 2014. Socialstyrelsen; 2015.
20. Journalföring och behandling av personuppgifter i hälso- och sjukvården. Socialstyrelsen; 2017.
21. Inbyggd integritet. Datainspektionen; 2012.
22. Datainspektionen. Hur förhindrar man obefogad spridning av patientuppgifter. Hämtad 2018-12-04 från https://www.datainspektionen.se/lagar--regler/patientdatalagen/hur-forhindrar-man-obefogad-spridning-av-patientuppgifter/.
23. Datainspektionen. Säkerhet för personuppgifter i e-post. Hämtad 2019-01-04 från https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/informationssakerhet/sakerhet-for-personuppgifter-i-e-post/
24. Slutrapport taligenkänning utvecklingsarbete gällande digitalt stöd inom den sociala barnavården. SKL; 2018.
25. Mobila enheter. Checklista för behandling av personuppgifter. Datainspektionen; 2013.