

# Informationsblad om vissa juridiska aspekter på systematisk uppföljning i socialtjänsten och EU:s dataskyddsförordning

Att följa upp arbetet i socialtjänsten är ett krav som är reglerat i lag. Kvaliteten i socialtjänstens verksamheter ska systematiskt och fortlöpande utvecklas och säkras, 3 kap. 3 § socialtjänstlagen (2001:453) SoL. Den som bedriver socialtjänst ska bland annat systematiskt följa upp och utvärdera den egna verksamheten (definitionen av egenkontroll i 2 kap. 1 § och 5 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd [2011:9] om ledningssystem för systematiskt kvalitetsarbete).

Det är i många fall nödvändigt att kunna behandla personuppgifter på individnivå (individdata) för att systematiskt utveckla kvaliteten i en viss verksamhet. Om en verksamhet exempelvis vill undersöka hur ofta de träffar barnen till mottagare av ekonomiskt bistånd behöver de under en tid dokumentera detta för att sammanställa och analysera resultatet i relation till önskad kvalitet i arbetet.

Förutom att systematisk uppföljning gör det möjligt att undersöka relevanta aspekter av kvalitet skapar det lokal kunskap och beprövad erfarenhet till stöd för en kunskapsbaserad socialtjänst. Verksamma på både lokal och regional nivå efterlyser stöd i arbetet med uppföljning för kvalitet och ökad kunskap med hjälp av systematisk uppföljning.

## Socialstyrelsen arbetar med stöd till systematisk uppföljning

Socialstyrelsen tillhandahåller flera olika kunskapsstöd till stöd för systematisk uppföljning (<http://www.socialstyrelsen.se/Lists/Artikelkatalog/Attachments/20208/2016-5-24.pdf>). Samtliga material utgår från samma tankemodell

om att systematisk uppföljning av klientarbete i kvalitetssyfte ibland förutsätter att uppgifter på individnivå aggregeras på gruppnivå för att möjliggöra analyser av klientarbetet ur exempelvis ett könsperspektiv. Datorbaserade verktyg, vidare SU-verktygen, har utvecklats för att erbjuda socialtjänsten möjligheter att förbättra kompetens i att *registrera*, *sammanställa* och *analysera* systematiskt insamlad information om klientarbetet för verksamhetsuppföljning, utvärdering och kvalitetssäkring. Nedan redogör Socialstyrelsen övergripande för hur EU:s nya dataskyddsförordning, även kallad GDPR – General Data Protection Regulation – förhåller sig till gällande nationell rätt (lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, SoLPuL, och förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten, SoLPuLF, och till hur SU-verktygen tillmötesgår krav i GDPR. Texten är inte uttömmande och för vägledning till GDPR hänvisas till Datainspektionen och till Europeiska dataskyddsstyrelsen (EDPB). Frågor om hur SU-verktygen är uppbyggda t.ex. utifrån kraven på inbyggt dataskydd och dataskydd som standard kan prövas av Datainspektionen.

## GDPR och systematisk uppföljning

GDPR är bindande för samtliga medlemsstater och är överordnad nationell rätt. Dataskyddsförordningen kräver dock stöd i nationell rätt för att vissa personuppgiftsbehandlingsåtgärder ska vara tillåtna, och därför kommer det även framöver finnas kompletterande nationella regler. För arbetet med systematisk uppföljning inom socialtjänsten finns stöd i nationell rätt i de kompletterande bestämmelserna i SoLPuL och SoLPuLF. En analys av om de bestämmelser som finns i SoLPuL och SoLPuLF är förenliga med GDPR har gjorts och bedömningen är att de bestämmelser som reglerar vilka typer av behandlingar och vilka uppgifter SoLPuL och SoLPuLF ska tillämpas på inte behöver ändras med anledning av GDPR<sup>1</sup>.

När det gäller systematisk uppföljning på individnivå inom socialtjänsten så är det fortfarande med stöd i SoLPuL och 3 kap. 3 § socialtjänstlagen (2001:453) SoL som denna behandling sker.

Jämfört med tidigare regelverk ställer GDPR tydligare krav på tekniska och organisatoriska åtgärder som innebär att dessa ska utformas utifrån kraven på inbyggt dataskydd och dataskydd som standard. Nedan beskrivs kraven kort och relateras till de SU-verktyg som Socialstyrelsen tillhandahåller <http://www.socialstyrelsen.se/publikationer2016/2016-5-24>. Socialstyrelsen har beaktat de kraven i samband med framtagandet av SU-verktygen. Varje kommun som använder verktyget behöver dock förhålla sig till regelverket om personuppgiftsbehandling i samband med att verktyget används.

<sup>1</sup> Se Socialdataskyddsutredningens betänkande Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning, SOU 2017:66, s 209 och 405 samt regeringens proposition 2017/18:171 Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning s. 183 f.

- Personuppgifter får inte behandlas i onödan. Personuppgifter får samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Vidare ska uppgifterna vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas, så kallad uppgiftsminimering (artikel 5). Det kan till exempel handla om att de förvalda inställningarna i en tjänst är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas. I stödmaterialen för SU-verktygen betonas vikten av att göra avgränsade uppföljningar med tydliga syften och de delar av uppföljningsformulären som inte används kan helt döljas. Inga uppgifter visas automatiskt för användaren. Enligt förvald inställning visas endast sammanställda uppgifter.
- Lämplig säkerhet ska säkerställas 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 (integritet och konfidentialitet) (artikel 5). SU-verktygens modell för kryptering i kombination med att varje handläggare enbart ser sina egna ärenden samt administratörens möjlighet att hantera olika handläggares ärenden så att de kan ”byta” handläggare syftar till att tillmötesgå denna punkt. En förutsättning vid användandet av SU-verktygen är att sedvanliga krav på it-säkerhet åtföljs i verksamheten, till exempel att medarbetare har separata inloggningar till Windows.
- Dataskydd ska vara inbyggt (privacy by design) vilket innebär att man tar hänsyn till integritetsskyddsreglerna redan när man utformar it-system och rutiner såsom krav på uppgiftsminimering, kryptering och pseudonymisering (artikel 25). För uppgiftsminimering kan det konkret innebära att system inte bör innehålla fritextsfält. Basen i SU-verktygen är frågor med fasta svarsalternativ. De fritextfält som finns har syftet att förtydliga svaret på den fasta frågan med koppling till uppföljning. Det ökar chansen att ha korrekt information. Fritextfältet har således en tydlig koppling till en fråga och därmed minskar risken att annan icke relevant information förs in i fritextfältet.
- Krav på dataskydd som standard (privacy by default) vilket kort innebär 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 är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas (artikel 25). I stödmaterialen för SU-verktygen betonas vikten av att göra avgränsade uppföljningar med tydliga syften och de delar av uppföljningsformulären som inte används kan helt döljas.
- Den registrerades rättigheter ska tillgodoses. Det avser bland annat rätten till rättelse av uppgifter, rätten till radering, rätten till begränsning av behandling av personuppgifter, rätten till dataportabilitet och rätten att göra invändningar (artiklarna 13-23). Dessa rättigheter kan tillgodoses i SU-verktygen genom att t.ex. en handläggare om en registrerad önskar det kan skriva ut uppgifterna i SU i ett registerutdrag. Det är vidare möjligt att ändra och radera ärenden om det bedöms att så ska ske.

Utöver de krav som beskrivits ovan finns flera allmänna krav på dataskydd, exempelvis skyldighet att informera den registrerade (artikel 12–14), krav på säkerhet vid behandling av personuppgifter (artikel 32) och krav på konsekvensbedömningar i vissa fall (artikel 35). Liksom tidigare gäller också att personuppgifter bara får behandlas inom socialtjänsten för att arbetsuppgifter inom socialtjänsten ska kunna utföras (6 § SoLPuL). Känsliga personuppgifter enligt artikel 9 GDPR får bara behandlas om de lämnats i ett ärende eller är nödvändiga för verksamheten och dess kvalitet (7 § SoLPuL).

### Sammanfattningsvis

- Det är möjligt att behandla personuppgifter, även känsliga personuppgifter, i sammanställningar som rör socialtjänstens uppföljning, utvärdering och kvalitetssäkring (7 a § SoLPuL).
- Personuppgifter får bara behandlas om det är nödvändigt för att arbetsuppgifter ska kunna utföras (6 § SoLPuL). Från manualen: Det är inte ok att dokumentera personuppgifter för verksamhetsuppföljning utan att på förhand ha gjort en bedömning av huruvida uppgifterna är nödvändiga för uppföljning av kvalitet i det avseende som verksamheten har tänkt.

### **Samarbete om systematisk uppföljning mellan nämnder**

Om kommuner i ett län vill bedriva gemensam systematisk uppföljning kan uppgifter behöva överföras från kommuner till en regional aktör, t ex kommunförbund eller en FoU-enhet. Regeringen har tidigare gett i uppdrag till Socialstyrelsen, SKL och de regionala samverkans- och stödstrukturerna att upprätta en gemensam plan för långsiktig samverkan till stöd till en kunskapsbaserad socialtjänst. Denna plan innebär förstärkt fokus på de fördelar som uppföljning på regional nivå rymmer. För små kommuner, med ett litet antal brukare, kan regionalt samordnad uppföljning göra uppgifter om det egna arbetet med brukare lättare att tolka och värdera om de relateras till samma uppgifter från flera verksamheter i länet. Som framgår nedan medför dock en önskan om att delta i samordnad uppföljning över nämnd- eller kommungränser att en bedömning behöver ske om hur det arbetet skulle kunna realiseras enligt regelverken om sekretess respektive personuppgiftsbehandling.

Om en regional aktör samordnar uppföljning innebär det att flera nämnder samarbetar om uppföljningen.

Om en nämnd vill samarbeta med andra nämnder i samma kommun eller i andra kommuner för att bedriva systematisk uppföljning behöver nämnden beakta om det är möjligt att lämna ut de aktuella uppgifterna enligt regelverken om sekretess respektive personuppgiftsbehandling. Om det är personuppgifter som lämnas ut så behövs i sådana fall en rättslig grund för att få behandla personuppgifterna.

Om uppgifter går att hänföra till en enskild som får en socialtjänstinsats så omfattas uppgifterna av sekretess enligt 26 kap. 1 § offentlighets- och sekretesslagen (2009:400), OSL<sup>2</sup>. För att sådana uppgifter ska kunna lämnas ut måste OSL möjliggöra detta, genom en s.k. menprövning eller en sekretessbrytande bestämmelse. Om uppgifterna inte går att hänföra till en enskild individ så anses inte en enskild kunna lida skada eller men och OSL hindrar då inte ett utlämnande<sup>3</sup>. Om uppgifterna inte går att hänföra till en individ så är de inte heller personuppgifter enligt det personuppgiftsrättsliga regelverket<sup>4</sup>. Även om sådana direkt utpekande uppgifter som namn och personnummer inte ingår bland uppgifterna kan det ändå vara frågan om uppgifter som går att hänföra till en viss individ, alltså personuppgifter. I varje enskilt fall måste man bedöma om det finns så pass unika uppgifter som gör att man förstår vem det handlar om. I korthet kan man uttrycka det som att om någon kan förstå vem det handlar om så är det personuppgifter som också omfattas av sekretessregleringen. Om uppgifterna sammanställs på gruppnivå i kommunen på ett sätt som gör att enskilda individer inte kan identifieras och förmedlas sammanställda från kommun till regional aktör så ska de inte falla under sekretessregleringen i OSL.

---

<sup>2</sup> Prop. 1979/80:2 del A s. 84

<sup>3</sup> Prop. 1979/80:2 del A s. 84

<sup>4</sup> Läs mer om när uppgifter går att hänföra till en person i det personuppgiftsrättsliga regelverket, bl.a. art 4 GDPR.