Samspelets behandling av personuppgifter

Uppdateringen har sin grund i parternas gemensamma underlag från Nationella Rådet genom http://www.finsam.se/rad_och_stod/gdpr

Vad är GDPR?

GDPR står för General data protection regulation. Det är EU:s gemensamma nya dataskyddsförordning som börjar gälla i alla medlemsländer den 25 maj 2018 och ersätter ett direktiv från 1995, samtidigt upphör personuppgiftslagen (PUL).

Vad är syftet med den nya lagstiftningen?

Syftet med den nya lagstiftningen är att skydda enskilda individers personuppgifter när dessa behandlas i förordningens mening. Personuppgifter är all slags information som direkt eller indirekt kan hänföras till en enskild individ som är i livet. Ett viktigt syfte med ny lagstiftning är att få till en ökad harmonisering mellan medlemsstaterna. Dataskyddsdirektivet från 1995 utgjorde visserligen en gemensam grund inom unionen, men direktivet skulle implementeras genom nationella lagstiftningar i varje medlemsland, de såg tämligen olika ut i olika länder. Nu gäller samma lagtext i alla medlemsländer.

Trots detta så ger GDPR vissa bemyndiganden för medlemsländerna att i begränsade delar komplettera förordningen med nationell lagstiftning. I Sverige kommer därför dataskyddslagen att gälla från och med den 25 maj 2018. Den speciella registerlagstiftning som tidigare funnits inom olika myndigheters verksamheter (t.ex. inom hälso- och sjukvården och inom socialtjänsten) kommer att få finnas kvar tills vidare, med vissa justeringar.

Stora delar av lagtexten i förordningen är densamma som i direktivet och PuL. Samtidigt är förordningen mer omfattande.

Vilka är de viktigaste förändringarna?

GDPR innehåller krav på att den personuppgiftsansvarige ska upprätta ett register över de slag av behandling denne ansvar för, där bl.a. ändamålen med behandlingen ska anges. Det innebär att samordningsförbunden behöver informera/dokumentera hur de hanterar uppgifter, vilka uppgifter och varför, se vidare artikel 30.

Den svenska missbruksregeln i PuL upphör, vilket innebär att all behandling av personuppgifter i verksamheten, även ostrukturerad behandling måste inordnas under ett behandlingsändamål. Det finns inte längre några ”bra-att-ha uppgifter” utan närmare ändamål. Till exempel kan man inte längre fotografera/filma deltagare på en konferens som ett tyst medgivande, utan det krävs ett uttryckligt samtycke.

För de fall den personuppgiftsansvarige har anlitat personuppgiftsbiträden så måste biträdesavtalen ses över och anpassas till förordningen, se artikel 28.

Skyldigheten att lämna en standardiserad information till den registrerade i samband med att uppgifter samlas in har utökats något jämfört med dagens lagstiftning, bl.a. ska den rättsliga grunden för behandlingen kunna anges, se artikel 13-14.

Den registrerade har rätt att begära ett så kallat registerutdrag, som tidigare, dock med den skillnaden att begäran ska kunna lämnas elektroniskt och beskedet ska också kunna lämnas elektroniskt. Utdraget ska lämnas kostnadsfritt men vid upprepade förfrågningar kan avgift tas ut, se artikel 15. Om begäran inkommer elektroniskt så måste myndigheten vara säker på identiteten hos den som ber om utdraget, normalt görs det med e-signatur (bankernas e-legitimation eller mobilt bank-id). Myndigheten måste då ha en tjänst där denna kan tas emot och läsas. I annat fall måste identiteten styrkas på annat sätt.

En rätt till radering införs men undantagen är många och för myndigheter är huvudregeln att den registrerade inte har rätt att få sina uppgifter raderade.

Alla myndigheter och offentliga organ är skyldiga att förordna ett dataskyddsombud, om de ö h t behandlar personuppgifter, om än i blygsam omfattning. Detta gäller även samordningsförbunden.

Krav på incidentrapportering införs, alltså när en incident inträffat som innebär olagligt eller brottsligt intrång i system, förlust av uppgifter eller att uppgifter läckt ut eller liknande. En personuppgiftsincident ska rapporteras till Datainspektionen, enligt huvudregeln senast 72 timmar efter det att den personuppgiftsansvarige upptäckt densamma.

Överträdelser mot förordningens bestämmelser kan leda till särskilda sanktionsavgifter, både för den personuppgiftsansvarige och för personuppgiftsbiträdet. Dessutom finns skadeståndsbestämmelser.

Registrering av deltagarens medverkan i insatser

Personuppgifter och samtyckeshantering

Innan du kan registrera personuppgifter i SUS behöver du inhämta deltagarens samtycke. Du får aldrig registrera personuppgifter om personer som inte lämnat sitt samtycke till detta. Du behöver inhämta ett nytt samtycke varje gång en deltagare ska registreras in i en insats. De deltagare som inte vill lämna sitt samtycke ska registreras som anonyma deltagare. De enda uppgifter som då registreras är deltagarens kön samt vilket budgetår deltagaren startade i insatsen. Ingen koppling kan göras till den specifike personen.

Samtycken ska alltid inhämtas skriftligt på Försäkringskassans blankett 9443 Samtycke som finns publicerad på www.susam.se. Blanketten ska alltid skickas in i original till Försäkringskassan. Aktuell adress finns angiven på blanketten samt på www.susam.se. Blanketten är översatt till 18 olika språk som finns att ladda ner på www.susam.se. Det är dock alltid den svenska versionen som ska fyllas i och skickas in. Observera att du inte kan ändra eller lägga till text i samtyckesblanketten. Blankettens innehåll är anpassat från 3 a § förordning (2003:766) om behandling av personuppgifter inom

socialförsäkringens administration12. Samtycket för SUS behöver dessutom hållas isär från andra samtycken så att det tydligt framgår vad en person har gett sitt samtycke till.

Vill man behandla uppgifter med stöd av samtycke krävs det att samtycket är en frivillig, specifik och otvetydig viljeyttring. Det går därför inte att använda sig av i förväg ikryssade rutor på webbplatsen. Samtycket ska vara dokumenterat.

Ett nytt samtycke måste inhämtas varje gång en deltagare ska registreras in i en samverkansinsats. Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade. Det ska vara dokumenterat.

Information till den registrerade om personuppgifter

Informationen ska innehålla tydlig angivelse av den rättsliga grunden för behandlingen, ändamålet för behandlingen, hur länge uppgifterna kommer att sparas samt information om var den registrerade kan vända sig med klagomål. Informationen ska vidare vara kortfattad och tydlig.

Återtagande av medgivande

Om en person återtar sitt medgivande angående registrering av uppgifter i SUS ska inga personuppgifter registrera framledes. Däremot de uppgifter som finns i SUS har Försäkringskassan fortsatt rätt att behandla med stöd av en rättslig grund i socialförsäkringsbalken, 114 kap. 7 § 5. (Uppföljning av samverkan mellan flera myndigheter inom rehabiliteringsområdet.)

Samtycken från underåriga deltagare

Avseende underåriga (under 18 år) deltagare är grundprincipen att den unges mognad och utveckling i kombination med samtyckets omfattning är avgörande om samtycket ska anses vara giltigt eller inte. I Datainspektionens information, Samtycke enligt personuppgiftslagen (s. 13), står följande: Om uppgifter om underåriga ska behandlas är det särskilt viktigt att göra en seriös bedömning av den unges förmåga att förstå de totala konsekvenserna av en behandling. En tumregel kan vara att den som fyllt 15 år normalt är kapabel att ta ställning i samtyckesfrågan. Om den underårige inte bedöms vara kapabel till att ta ställning till samtyckesfrågan behöver målsmans underskrift finnas för att registrering ska få ske i SUS.

Skyddade personuppgifter

Av säkerhetsskäl ska aldrig personuppgifter om deltagare med skyddade personuppgifter registreras i SUS. Dessa deltagare ska hanteras på samma sätt i SUS som de deltagare som inte lämnar samtycke för registrering av uppgifter i SUS, det vill säga registreras som anonyma deltagare. Om en deltagare får skyddade personuppgifter under tid i insats kommer SUS att hantera detta på följande sätt:

- SUS tar bort uppgifter om namn, personnummer och KundId för deltagaren
- Registrerade uppgifter vid inregistreringen kommer att tas bort ur SUS-databasen
- SUS registrerar automatiskt deltagaren som en anonym deltagare i insatsen

Personuppgiftsansvar och registerutdrag

Enligt personuppgiftslagen (1998:204) har en person rätt att begära registerutdrag om information som behandlas om denne. En person har även rätt att begära att felaktiga personuppgifter rättas. Försäkringskassan är som systemägare ansvariga för personuppgifter i SUS. En begäran om registerutdrag ur SUS och/eller rättning av felaktiga personuppgifter i SUS ska alltid göras till Försäkringskassan.

Felregistrerade deltagare

Felregistrerade deltagare får inte finnas i SUS-databasen. Om du upptäcker en felaktigt registrerade deltagare i en insats ska du genast göra följande:
Registrera ut deltagare med avslutningsanledning Felregistrering. Deltagaren kommer då automatiskt att tas bort ur databasen. Inga uppgifter om insatsen kommer att finnas kvar.

Deltagare som har lämnat sitt samtycke

Deltagarens medverkan i insats är grunden för uppföljningen i SUS. Du ska registrera en deltagare när denne startar i en insats (inregistrering) och du ska registrera när deltagaren avslutar sin medverkan i insatsen (utregistrering). SUS ger inget stöd till registrering av delinsatser eller delaktiviteter. I samband med in- och utregistreringen ska du besvara ett antal frågor om deltagarens situation och aktivitetsförmåga. Skillnaderna mellan deltagarens status vid tidpunkten för inregistreringen och vid utregistreringen utgör resultatet för deltagarens medverkan i insatsen.

Deltagare som inte har lämnat sitt samtycke och personer med skyddade personuppgifter

Deltagarens medverkan i insats är grunden för uppföljningen i SUS. För anonyma deltagare registrerar du uppgift om kön samt vilket år deltagaren påbörjat insatsen. Ingen uppgift går att knyta till den specifika personen. Observera att du aldrig kommer att ”registrera ut” anonyma deltagare. Detta är en logisk följd av att det inte får finnas någon koppling till en enskild deltagare i SUS. Det vill säga du kan inte registrera ut en anonym deltagare då SUS inte vet vem denne är.

Deltagaransvariga och insatser

Deltagaransvariga kan registrera uppgifter om deltagare för de insatser som de har tilldelats uppdrag i. Det finns ingen direkt koppling mellan en registrerad deltagare och en deltagaransvarig. Det innebär att samtliga deltagaransvariga för en insats kan registrera uppgifter om deltagaren i denna specifika insats. En deltagare kan därför registreras in och ut av två olika deltagaransvariga.

Tillgång till uppgifter på individnivå

Deltagaransvariga kan se uppgifter om enskilda deltagare direkt i SUS. Det vill säga att de har direktåtkomst till deltagaruppgifter i SUS för de insatser de har ett uppdrag i. Ingen annan behörighetsroll i SUS har tillgång till personuppgifter på individnivå.

Respektive myndighet är ytterst ansvariga för att enbart de personer som arbetar i de lokala samverkansaktiviteter där deltagaren deltar har behörighetsrollen deltagaransvarig.
Den deltagaransvariga ska dessutom enbart ha uppdrag för de insatser som denne arbetar för.

Försäkringskassan har möjlighet att genom särskilda registeruppdrag ta ut deltagaruppgifter ur SUS-databasen i uppföljningssyfte. Denna behörighet är begränsad till ett fåtal personer på Försäkringskassans IT-avdelning.