Dokumentnamn:	**Giltigt från:**
Behandling av personuppgifter inom Södra Älvsborgs Räddningstjänstförbund.docx	Publiceringsdatum
Diarienummer:	**Reviderat:**
	2020-03-27
Upprättad av: Bo Sandström	**Beslutad av:** Direktionen
Målgrupp: Alla anställda inom SÄRF	

Behandling av personuppgifter inom Södra Älvsborgs Räddningstjänstförbund, SÄRF

Bakgrund

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning General Data Protection Regulation (GDPR). I Sverige benämns denna även som Dataskyddsförordningen. Den ersätter den tidigare personuppgiftslagen (PuL). Skillnaderna är inte dramatiska men vissa delar av reglerna runt behandling av personuppgifter har skärpts. Dessutom kan böterna bli mycket kännbara om det uppmärksammas att organisationen inte följer regelverket i tillräcklig grad. Lagen berör endast personuppgifter gällande levande fysiska personer.

Syfte

Syftet med Dataskyddsförordningen är främst att stärka den enskildes integritet, frihet och rättigheter. Dataskyddsförordningen har också till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU.

Allmänt

Dataskyddsförordningen ställer höga krav på hur personuppgifter behandlas. Organisationen behöver därför löpande identifiera och ha koll på vilka personuppgifter som är nödvändiga och lagliga att behandla. Endast personuppgifter som är nödvändiga får samlas in, lagras och på andra sätt behandlas inom SÄRF. Behandling och rutiner för detta behöver ständigt vara aktuella och väl dokumenterade. SÄRF behöver därför ha en dynamisk och lättöverskådlig sammanställning över register och andra platser i vilka personuppgifter förekommer.

Personuppgiftsansvarig, anställda och andra berörda ska ha kännedom om regler och rutiner avseende behandling av personuppgifter i en grad som svarar mot aktuell roll/funktion i organisationen. Det ska finnas ett utsett dataskyddsombud som fungerar som stödfunktion för personuppgiftsansvarig, anställda och tillsynsmyndigheter avseende efterlevnad av Dataskyddsförordningen.

Grundstommen i GDPR – de 7 grundprinciperna

- Man får bara behandla personuppgifter om man uppfyller kraven i lagen.
- Man får bara samla in personuppgifter för ett angivet syfte.
- Man får bara samla in de uppgifter som är nödvändiga för att uppfylla syftet.
- Har man personuppgifter måste man hålla dem korrekta och uppdaterade.
- När syftet är uppnått ska uppgifterna tas bort.
- Personuppgifter ska förvaras säkert så de inte ändras eller stjäls.
- Man ska kunna bevisa att man uppfyller alla dessa krav.

Rättslig grund för personuppgiftsbehandling

Utan en rättslig grund är personuppgiftsbehandlingen inte laglig. Det finns sex rättsliga grunder.

Samtycke

Den registrerade har sagt ja till personuppgiftsbehandlingen. I många fall är det inte lämpligt eller kanske inte ens möjligt att stödja sig på den registrerades samtycke. Överväg därför alltid först om man kan stödja personuppgiftsbehandlingen på någon av de andra rättsliga grunderna.

Avtal

Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige.

Intresseavvägning

Den personuppgiftsansvarige får behandla personuppgifter utan den registrerades samtycke om den personuppgiftsansvariges intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet.

Rättslig förpliktelse

Det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet.

Myndighetsutövning och uppgift av allmänt intresse

Den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.

Grundläggande intresse

Den personuppgiftsansvarige måste behandla personuppgifter för att skydda en registrerad som inte kan lämna samtycke, till exempel om den är medvetslös.

Tillsyn

I Sverige föreslås **Datainspektionen** få tillsynsuppdraget. Som tillsynsmyndighet har Datainspektionen möjlighet att bland annat utfärda varningar och reprimander samt att förelägga organisationer att vidta åtgärder. Datainspektionen kan även besluta om att begränsa eller förbjuda behandling och att påföra administrativa sanktionsavgifter.

En nyhet med förordningen är att tillsynsmyndigheten kan utöva tillsyn och fatta beslut inte endast gentemot personuppgiftsansvariga utan även mot personuppgiftsbiträden.

Definition och kategorisering av personuppgift

I Dataskyddsförordningen återfinns allmänt hållna definitioner av begreppet personuppgift. För att underlätta den lokala förståelsen behöver man mer konkret beskriva vad SÄRF avser med en

personuppgift. Begreppet personuppgift och SÄRF:s förhållningssätt till vissa typer av personuppgifter, kan också till viss del förändras över tid. Det är därför lämpligt att ge faktiska exempel på detta och särskilt på sådant som kan upplevas som tveksamt.

Dataskyddsförordningen lägger särskild vikt vid uppgifter som kan betecknas som särskilt känsliga. Dessa uppgifter ska hanteras med extra varsamhet och det är därför viktigt att organisationen klargör vilka personuppgifter som är att betrakta som känsliga och särskilt känsliga. SÄRF har valt att kategorisera personuppgifter i en 3-gradig skala.

- Kategori 0 innebär uppgifter som normalt inte betraktas som känsliga, ex. namn eller signatur i ett fristående sammanhang.
- Kategori 1 är uppgifter som kan behöva behandlas med viss försiktighet, ex. namn på närmast anhörig, adress, personnummer, m.m.
- Kategori 2 innehåller uppgifter som betraktas som särskilt känsliga, ex. hälsa, etnicitet, m.m. Behandling av denna typ av personuppgifter regleras i artikel 9 i Dataskyddsförordningen.

Det är dock viktigt att beakta att personuppgifter som inte anses känsliga var för sig, kan tillsammans eller i ett visst sammanhang behöva hanteras som känsliga.

SÄRF har upprättat en särskild förteckning över de olika typer av personuppgifter som hanteras inom organisationen. Denna förteckning bör granskas och vid behov revideras med regelbundna intervaller.

Roller avseende GDPR inom SÄRF

Personuppgiftsansvarig: Direktionen för Södra Älvsborgs Räddningstjänstförbund

Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter men personuppgiftsansvaret kan aldrig överlåtas.

Den personuppgiftsansvarige måste se till att behandlingen sker i enlighet med Dataskyddsförordningens samtliga bestämmelser. Dess personal får enbart behandla personuppgifter enligt de instruktioner som getts av den personuppgiftsansvarige.

Den personuppgiftsansvarige har ett generellt ansvar att, utifrån de integritetsrisker som finns med behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen, exempelvis att organisationen antagit en policy med lämpliga strategier för dataskydd och ser till att genomföra den i organisationen.

GDPR-samordning

Samordnare utses av ledningsgruppen för SÄRF.

Person med särskilt ansvar för intern samordning, utbildningsinsatser och omvärldsbevakning avseende GDPR.

Ansvarar för regelbunden översyn av lokala styrdokument, SÄRF:s förteckning över register med personuppgifter, listan över personuppgiftstyper samt andra övergripande dokument avseende organisationens GDPR-arbete.

Dataskyddsombud

Utses av Dataskyddsansvarig.

SÄRF är som myndighet skyldig att utse dataskyddsombud. Dataskyddsombudet ska vara en namngiven fysisk person.

Ombudets roll är:

- Att informera och ge råd till den personuppgiftsansvarige och till de anställda som hanterar personuppgifter om deras skyldigheter enligt förordningen och andra dataskyddsbestämmelser
- Att övervaka efterlevnaden av dataskyddsförordningen och annan dataskyddslagstiftning, samt interna riktlinjer och policydokument
- Att samarbeta med tillsynsmyndigheten och att vara en kontaktpunkt för tillsynsmyndigheten
- Den registrerade får kontakta ombudet i frågor som gäller behandlingen av dennes uppgifter och utövandet av dennes rättigheter gentemot den personuppgiftsansvarige
- Att på begäran ge råd vad gäller konsekvensbedömningar avseende dataskydd. (Registerföringsskyldigheten i PuL går över från ombudet till den personuppgiftsansvarige)

Personuppgiftsbiträden

Återfinns i förekommande fall för respektive objekt i förteckningen över de register och platser hos SÄRF som innehåller personuppgifter.

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ. Exempel på detta kan vara företag som utövar systemövervakning, support, konsulter, m.fl.

Den personuppgiftsansvarige och personuppgiftsbiträdet måste upprätta ett så kallat biträdesavtal.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

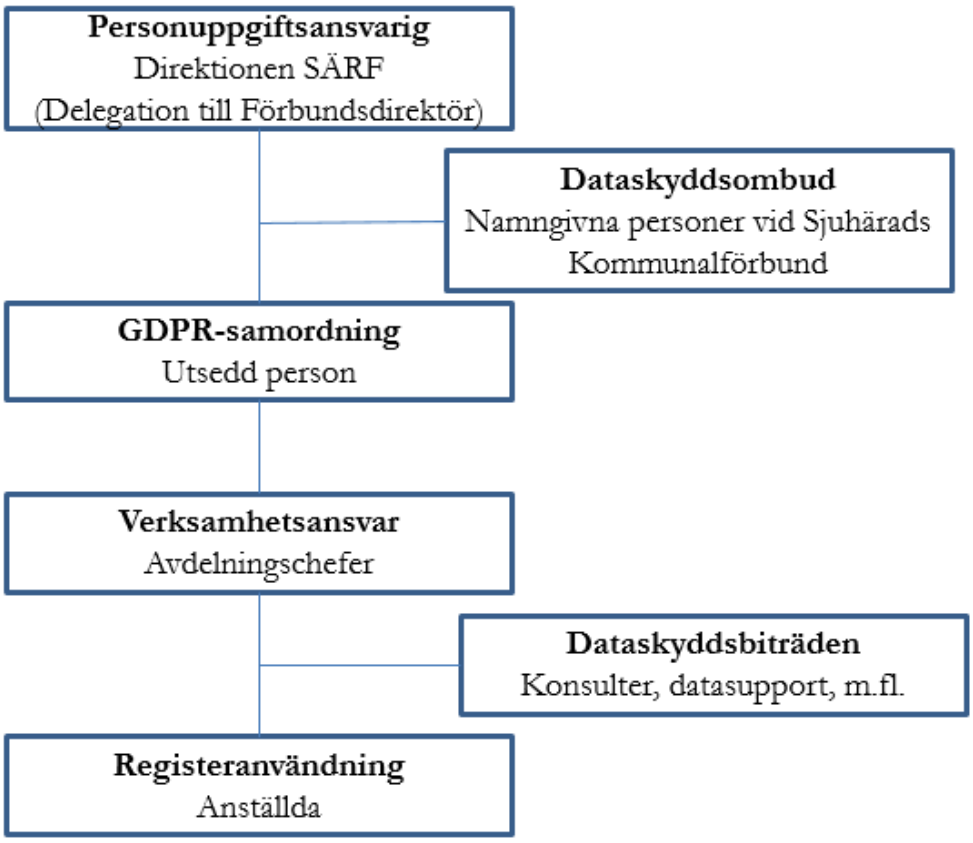
Verksamhetsansvar: Respektive avdelningschef

Avdelningschefen ansvarar för att den personal som hanterar personuppgifter inom avdelningens område har nödvändig kännedom om reglerna runt behandling av personuppgifter samt att tydliga arbetsrutiner upprättas och underhålls i enlighet med gällande regler/lagar. Vid införande av nya tekniska system eller liknande görs detta vid behov i samverkan med IT-samordnare inom SÄRF och vid behov även Dataskyddsombud för att säkerställa att kraven i Dataskyddsförordningen tillgodoses.

Registeranvändare: Anställda

Anställda ska i en omfattning som svarar mot den anställdes organisatoriska uppgifter, ha kännedom om och följa de regler och rutiner som berör hantering av personuppgifter inom SÄRF.

Schematisk översikt



Stöd, rutiner och utbildning

För att kunna hålla en hög nivå av efterlevnad avseende GDPR krävs att organisationen arbetar strukturerat och rutinstyrt. Det förutsätter att personalen har grundläggande kännedom om villkoren för behandling av personuppgifter och hur SÄRF definierar en personuppgift. Information och utbildning avseende hantering av personuppgifter ska erbjudas vid nyanställning och vid förändrade arbetsuppgifter. Dessutom behöver rutiner, organisatoriska förutsättningar och teknik ständigt anpassas till aktuella förhållanden.

Teknik

Vid införande och anpassning av system och register ska lättarbetad GDPR-funktionalitet eftersträvas. Det ska vara smidigt att i systemet uppfylla regler och intentioner avseende korrekt hantering av personuppgifter.

Skydd

Enligt GDPR ska personuppgifter skyddas från stöld, förstöring och obehörig åtkomst. Skyddet kan vara fysiskt, tekniskt och/eller organisatoriskt.

Fysiska barriärer

Personuppgifter som återfinns i fysiska dokument skyddas i SÄRF:s lokaler av dörrar med ett centralt system för passagebehörigheter samt låsta godkända dokumentskåp. Åtkomst till primärt serverrum sker genom användning av både passerkort, kod och nyckel.

Tekniskt skydd
Digitala register skyddas från obehörig åtkomst genom brandväggar och individbaserade rättighetsbegränsningar. Backup tas dagligen på alla aktuella register för möjlighet till återställning om data oönskat raderats, förstörts eller krypterats.

Organisatoriskt skydd
- Rutiner rörande behandling av personuppgifter hålls uppdaterade och kända.
- Personal med särskild behörighet kontrolleras genom polisens belastningsregister
- Användarnas lösenord för åtkomst till SÄRF:s nätverk ska hålla hög komplexitet och måste bytas med fastställt tidsintervall, f.n. 180 dagar.
- Personuppgiftsbiträden ska kunna uppvisa hög, teknisk säkerhet och avtal ska upprättas för reglering av sekretess och andra säkerhetsaspekter.

Personuppgiftsincidenter
Uppmärksammade incidenter som kan relateras till behandlingen av personuppgifter ska anmälas till Dataskyddsombudet och till Datainspektionen. Anmälan ska ske till Datainspektionen inom 72 timmar efter att incidenten upptäckts. Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste Datainspektionen meddelas. Om det är osannolikt att en personuppgiftsincident medför risker behöver den inte anmälas till Datainspektionen. Om incidenten inte anmäls, ska beslutet motiveras och dokumenteras.

Dataskyddsansvarig ska utreda incidenten och vid behov vidta åtgärder för att minimera följder och förhindra upprepning.

Begrepp

Personuppgift
Som personuppgift räknas varje upplysning som avser en identifierad eller identifierbar fysisk person, som direkt eller indirekt kan identifieras med hjälp av namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Registrerad
Den person som en registrerad personuppgift avser.

Behandling
Som behandling räknas en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Mottagare
En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ till vilket personuppgifterna utlämnas. En mottagare kan finnas både inom och utanför egen organisation.

Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.