Rutiner gällande efterlevnad av GDPR inom Vård och Omsorg

Dokumenttyp:		Detta dokument gäller för:
Rutin		Vård och omsorg
Fastställd/upprättad		Dokumentansvarig:
2020-01-30		GDPR-ansvarig verksamhetsresurs
Senast reviderad:	Giltighetstid:	Dnr:
2020-01-30	Tillsvidare	0000-000

Rutiner gällande efterlevnad av GDPR inom Vård och Omsorg

Innehåll

Bakgrund

GDPR (General Data Protection Regulation) tillämpas inom hela EU och syftar till att stärka och harmonisera dataskyddet för medborgare. Den primära målsättningen är att ge individen bättre kontroll över sina personuppgifter.

Syfte

I dataskyddsförordningen finns ett krav om att det ska föras register över alla personuppgiftsbehandlingar som finns i kommunen. Att skapa en översikt över vilka behandlingar av personuppgifter som finns i organisationen utgör basen i arbetet med att uppfylla GDPR. I samarbete med närliggande kommuner har en mall av registerförteckning tagits fram som sedan har justerats för att passa Vård och omsorg. Syftet med att registrera alla uppgifter i en förteckning är att skapa kontroll över vilka uppgifter vi behandlar.

1. Vad är en personuppgift?

Personuppgifter innebär all information relaterad till en identifierad eller identifierbar fysisk levande person. Det omfattar bland annat genetisk, mental, kulturell, ekonomisk eller social information.

En personuppgift är uppgifter som berör en person som är vid liv, som är identifierad eller går att identifiera indirekt eller direkt. Det kan exempelvis vara; email, ip-adress, adressuppgifter, bilregistreringsnummer, bilder, telefonnummer, personnummer

2. Känslig personuppgift

Känsliga personuppgifter är personuppgifter som avslöjar ras, etniskt ursprung, religion, filosofiska eller politiska åsikter, hälsa eller sexuell läggning är endast tillåtet om det finns en lagstadgad tystnadsplikt såsom för socialtjänstpersonal eller hälso- och sjukvårdspersonal. Behandlingen skall då ske i slutna system som Magna Cura, Companion, Alfa-E eller Phoniro. Att en personuppgift krypteras eller på liknande sätt anonymiseras gör inte att behandlingen inte behöver registreras.

3. Vad är en behandling?

Definitionen av ’behandling’ är vid och omfattar alla åtgärder som vidtas i fråga om personuppgifter.

Det kan exempelvis vara; insamling, registrering, lagring, spridning, samkörning, register över brukare, elever, politiker, klienter inom individ- och familjeomsorg, leverantörregister, individer registrerade för ansökningar, kommuntjänster, överklaganden, passersystem. Förenklat uttryckt så är allt som förekommer i våra system en behandling.

4. Är behandlingen laglig?

För att en behandling ska vara laglig krävs att vissa grunder är uppfyllda t.ex. med stöd i lag.

5. Är allmänna principer tillgodosedda?

För att en personuppgiftsbehandling ska få ske måste alla grundläggande principer vara uppfyllda.

- **Lagstöd:** Uppgifterna ska behandlas med stöd i lag.
- **Ändamålbegränsning:** Får enbart användas och sparas till de ändamålet som uppgifterna samlades in till.
- **Uppgiftsminimering:** Mer uppgifter än nödvändigt ska inte behandlas.
- **Lagringsminimering**: Uppgifter får inte sparas längre tid än nödvändigt för ändamålen.

- **Krav på säkerhet**: Tex genom skydd i tekniska system, verksamhetssystem eller behörigheter.

Ansvarsfördelning; Registerförteckning, PUB-avtal och informationstexter/blanketter

Uppföljningsmöten på APT alternativt verksamhetsmöte 1 gång under våren och 1 gång under hösten. Under uppföljningsmötet går vi igenom hur registerförteckningen ser ut, vilka Pub avtal och blanketter som verksamheten har idag, vilka ändringar, kompletteringar vi behöver göra. Inför kommande APT/verksamhetsmöten, där GDPR ska vara med på dagordningen, tar enhetschef kontakt med GDPR ansvarig verksamhetsresurs inom Vård och omsorg. GDPR ansvarig verksamhetsresurs skickar en kopia av enhetens flik i registret till ansvarig enhetschef. Enhetschefen och/eller verksamhetsresursen kontrollerar att uppgifterna i registret stämmer, ändrar, tar bort eller lägger till uppgifter. Fliken skickas sedan tillbaka till GDPR-ansvarig verksamhetsresurs inom två veckor. Observera att originaldokumentet finns hos GDPR-ansvarig verksamhetsresurs, så det är fritt att redigera i den kopia som skickas ut.

Förutom ovanstående uppföljning på ett av höstens och vårens APT/ verksamhetsmöte rapporterar verksamhetens personal fortlöpande ändringar till GDPR-ansvarig inom Vård och omsorg.

Uppföljning bör ske tre veckor efter punkten GDPR varit uppe på APT eller verksamhetsmöte. Uppföljning sker också mellan GDPR-ansvarig inom VO till administratör på IT.

Registerförteckningen

Registerförteckningen innehåller registrering av de dokument/mappar som innehåller personuppgifter på enheten.

GDPR-ansvarig vill få kännedom om:

- Nya personuppgifter som ska registreras
- Ändringar av registrerade uppgifter
- Registrerade uppgifter utgår

Personuppgifter kan lagras på dessa sätt:

- T-katalogen
- Egna mappar på datorn
- Teams
- SharePoint
- Fysiska pärmar, mappar, plastbackar och anslagstavlor

För att se hur en ny behandling kan registreras i registerförteckningen se bilaga 1.

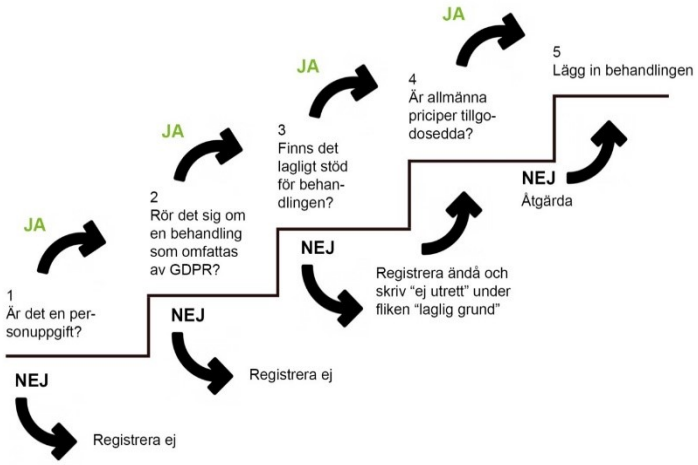
Enhetschefen har ansvar för att samtliga personuppgiftshanteringar som finns på enheten blir registrerade.

Genomförande av registerförteckningen

Skapa en bra struktur bland mappar och dokument på datorn så blir det enklare att arbeta med registret. Samtliga dokument behöver inte registreras var för sig, det räcker att en ”grupp” av liknande dokument registreras på en rad i registret så länge de har samma sökväg och innehåller liknande personuppgifter.

Alla uppgifter som kan sparas i något av våra datasystem ska i första hand sparas där. Systemen är godkända utifrån GDPR och Hjo kommun har ingått ett GDPR-anpassat avtal, s.k. personuppgiftsbiträdesavtal (PUB-avtal), med leverantörerna. Vissa dokument med personuppgifter behöver ändå finnas. Uppgifter som är av känslig karaktär, som inte kan sparas i verksamhetssystemet/personalsystemet och som rör brukare eller personal, bör sparas i T-katalogen och inte i egna dokument.

Ta för vana att **gallra** dokument/mappar som inte används eller som **inte längre uppfyller ändamålet.** Vi har ansvar att gallra enligt dokumenthanteringsplanen. Saknas någon dokumenttyp i dokumenthanteringsplanen kontakta GDPR-ansvarig verksamhetsresurs inom Vård & Omsorg.
Innan en behandling registreras i förteckningen ska dessa steg gås igenom:



PUB-avtal

Ett PUB-avtal ska finnas i de fall där kommunen använder verksamhetssystem som hanterar personuppgifter. Det kan tex vara journalföring, kvalitetsregister etc.

När PUB (**P**erson**u**ppgifts**b**iträde) avtal ska upprättas ska detta ske enligt SKL:s mall. Systemansvarig/systemägare ska enligt kommunens rutiner kontakta leverantörerna för PUB-avtalsskrivning. Avtalet måste undertecknas av kommunens firmatecknare. Avtalet ska skickas till Personuppgiftsbiträdet med mottagningsbevis för att säkerställa att avtalet mottagits och undertecknas. När PUB avtalet är undertecknat av båda parter ska detta diarieföras.

GDPR-ansvarig vill få kännedom om:

- Nya verksamhetssystem som hanterar personuppgifter
- När avtal med verksamhetssystem löper ut och ska förnyas, behöver även PUB-avtalet ses över

Blanketter

Varje ny personuppgift vi registrerar (blankett, formulär, samtycke etc.) ska föras in i vår registerförteckning oavsett om den är analog eller digital.

När verksamheten skapar en ny blankett eller formulär där avsikten är att samla in personuppgifter, behövs en tilläggstext som beskriver kommunens hantering av individens personuppgifter utifrån GDPR. Detta gäller även blanketter, formulär eller samtycken som sker internt inom förvaltningen eller inom organisationen.

Blanketter används och finns:

- Internt
- Externt
- E-formulär
- E-tjänst

GDPR-ansvarig vill få kännedom om:

- Nya blanketter
- Ändringar av blanketter
- Utgående blanketter

Bilaga 1

Behandlingens namn	Kategorier av registrerade	Ändamålen med behandlingen	Kategorier av personuppgifter	Känsliga personuppgifter*	Applikationer/system Lagringsställe
APT	Anställda	Minnesanteckningar, uppföljning av möten, närvaro	Namn	Nej	Teams
APT	Anställda	Minnesanteckningar, uppföljning av möten, närvaro	Namn	Nej	Pärm
Verksamhetsmöten	Anställda, brukare	Underlag inför verksamhetsmöten	Namn	Nej	Teams
Checklista	Anställda	Används vid introduktion som ett arbetsredskap för att veta vad för information personalen har fått under sin introduktion	Namn	Nej	Pärm
Medarbetarsamtal	Anställda	Underlag inför medarbetarsamtal	Namn	Nej	T-katalogen

*Om ja = uppgifterna ska hanteras i ett verksamhetssystem