Beslut fastställande av Personuppgiftshantering – Riktlinje för SLSO

Ärendebeskrivning

Styrelsen för Stockholms läns sjukvårdsområde är personuppgiftsansvarig. I samband med införandet av dataskyddsförordningen 25 maj 2018 intensifierades arbetet inom förvaltningen med att anpassa och stärka skyddet av personuppgifter. Förvaltningen har tillsammans med hälso- och sjukvårdsförvaltningen arbetat fram en riktlinje för hantering av personuppgifter som samtliga medarbetare ska förhålla sig till.

Förslag till beslut

Styrelsen för Stockholms läns sjukvårdsområde föreslås besluta

att fastställa Personuppgiftshantering – Riktlinje för SLSO, samt

att uppdra åt sjukvårdsdirektören att kommunicera riktlinjen inom förvaltningen.

Mikael Ohrling
Sjukvårdsdirektör

Annika Jerhamre
Kanslichef

Stockholms läns sjukvårdsområde

RIKTLINJE

Dokumentnummer:
RIK-20500-v.0.15

Gäller från:

Godkännare: Mikael Ohrling
Upprättare: Camilla Heise Löwgren

Personuppgiftshantering - riktlinje för SLSO

Ännu ej publicerad version

Innehåll

1 Kort om förordningen ... 3

1.1 Vad är en personuppgift? ... 4
1.1.1 Känsliga personuppgifter ... 4

1.2 Visa att principerna följs ... 5

2 Registrera personuppgiftshantering ... 5

2.1 Vad ska rapporteras till registret? ... 6
2.1.1 Ansvarig kontaktperson ... 6
2.1.2 Kategorier av de registrerade, personuppgifter och mottagare ... 6
2.1.3 Ändamålet med hanteringen ... 6
2.1.4 Rättslig grund för hantering ... 7
2.1.5 Hantering av personuppgifter i e-post ... 7
2.1.6 Tidsintervall för bevarande/gallring ... 8
2.1.7 Dataskyddsförordningen och arkivering ... 9
2.1.8 Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna ... 9
2.1.9 Behörighet och loggning ... 10

3 Rapportera personuppgiftsincidenter ... 10

3.1 Så här rapporteras en incident ... 11

4 Informationsplikt ... 12

4.1 Registerutdrag ... 12

5 Personuppgiftsbiträdesavtal ... 13

Ännu ej publicerad version

Personuppgiftshantering - riktlinje för SLSO

1 Kort om förordningen

Hela EU/EES har samma lagstiftning som reglerar hur man får hantera personuppgifter - Dataskyddsförordningen (GDPR).

Syftet med lagen är att stärka personers grundläggande fri- och rättigheter och särskilt skyddet av personuppgifter.

- Den som hanterar uppgifterna ska kunna visa att lagen följs.
- Uppgifterna ska hanteras på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.
- Uppgifterna ska samlas in för ett särskilt ändamål.
- Uppgifterna ska vara korrekta.
- Uppgifterna ska lagras så kort tid som möjligt.
- Uppgifterna ska skyddas på ett korrekt sätt.



Lagen anger också att de registrerade ska få tydlig information om hur deras personuppgifter hanteras. En individ vars personuppgifter hanteras har rätt att få:

- tillgång till sin information
- veta vad uppgifterna används till (ändamål)
- sina uppgifter raderade – rätten att bli bortglömd
- sina uppgifter rättade om de anses felaktiga.

En myndighet som samlar in och hanterar personuppgifter ska därför:

- tillmötesgå förfrågningar från individen, exempelvis tillhandahålla registerutdrag
- informera individen vid insamling och hantering av personuppgifter
- dokumentera hanteringar i en registerförteckning
- rapportera personuppgiftsincidenter inom 72 timmar
- ha ett inbyggt dataskydd i system och processer.

Region Stockholm är ytterst ansvarig för all hantering av personuppgifter som sker inom organisationen. Däremot har ansvaret för att säkerställa efterlevnaden inom regionen delegerats ut på respektive nämnd/förvaltning. Detta innebär att SLSO:s styrelse är ansvarig för hur personuppgifter hanteras. I enlighet med lagen ska även varje myndighet utse dataskyddsombud, som bland annat ska:

- övervaka att organisationen följer dataskyddsförordningen
- ge råd om konsekvensbedömningar
- vara kontaktperson för de registrerade och personalen inom organisationen
- samarbeta med och vara kontaktperson till Datainspektionen.

Om personuppgifterna inte hanteras på ett lagligt och korrekt sätt kan sanktionsavgift utdömas av Datainspektionen som är tillsynsmyndighet. Även de registrerade kan begära skadestånd/ersättning av ansvarig nämnd.

1.1 Vad är en personuppgift?

Personuppgifter är all information som direkt eller indirekt kan knytas till en person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Ett organisationsnummer är en personuppgift om det handlar om en enskild firma. Registreringsnumret på en bil är en personuppgift om det går att knyta till en person, medan registreringsnumret på en firmabil som används av flera anställda, inte är en personuppgift. I vissa fall räknas även olika slags elektroniska identiteter, som exempelvis IP-adress, som personuppgifter om de kan kopplas till en viss person.

1.1.1 Känsliga personuppgifter

I dataskyddsförordningen skiljer man mellan vanliga personuppgifter och känsliga personuppgifter. Med känsliga personuppgifter menas:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter* som entydigt identifierar en person.

*biometriska data används då man använder olika matematiska och statistiska metoder för att känna igen en person baserat på en fysiologisk eller beteendemässig egenskap. Exempelvis ansiktet, fingeravtryck, handavtryck, handskrift, ögats iris.

Känsliga uppgifter är förbjudet att registrera såvida de inte omfattas av undantag för sådan registrering.

1.2 Visa att principerna följs

Nämnden ska kunna visa att dataskyddsförordningen följs vilket innebär att omvänd bevisbörda tillämpas. Datainspektionen (som är tillsynsmyndighet) behöver inte visa att nämnden gjort fel, utan nämnden måste istället visa att den gjort rätt.

Denna riktlinje beskriver vad och hur nämnden ska arbeta med personuppgiftshanteringar för att tillgodose efterlevnaden av lagkraven.

2 Registrera personuppgiftshantering

Alla personuppgiftsansvariga (respektive nämnd) ansvarar för sina personuppgiftshanteringar och har en skyldighet att föra ett register över dem. Här registreras alla hanteringar, både det som sker i system och manuellt. Stockholms läns sjukvårdsområdes (SLSO) register ligger i ett system som för närvarande heter Personuppgiftshantering (PuH). Det är viktigt att alla personuppgifthanteringar anmäls via systemet eller på annat sätt till dataskyddsombudet. För att få tillgång till systemet, maila Helpdesk som ansvarar för behörighetshantering. Tänk på att endast den som ansvarar för registreringen, det vill säga den som arbetar aktivt i systemet (alternativt behörig chef) ska ha behörighet.



Dataskyddförordningen ställer krav på att vissa förutsättningar måste uppfyllas för att personuppgiftshanteringen ska vara laglig. Kraven ska finnas dokumenterade i registret, vilka beskrivs utförligare i detta dokument.

För stora, övergripande system som flera nämnder använder - till exempel Take Care eller Heroma - är det systemägaren centralt inom Region Stockholm som ansvarar för hur personuppgifterna som finns registrerade hanteras.

2.1 Vad ska rapporteras till registret?

Det finns ett antal informationsmängder som ska finnas dokumenterade i registret:

- Ansvarig kontaktperson för hanteringen
- Kategorier av de registrerade, av personuppgifter och av mottagare
- Ändamål med hanteringen
- Rättslig grund för hanteringen
- Tidsintervall för bevarande/gallring
- Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna

2.1.1 Ansvarig kontaktperson

Även om nämnden är personuppgiftsansvarig ska det alltid finns en ansvarig kontaktperson i linjeorganisationen som ansvarar för hanteringen och säkerställer efterlevnaden av lagstiftningen. I händelse av att en personuppgiftsincident inträffar, se kapitel 3, är det också viktigt att kontaktuppgifter är uppdaterade så att man snabbt kan komma i kontakt med ansvarig person.

2.1.2 Kategorier av de registrerade, personuppgifter och mottagare

Alla typer av personuppgifter ska specificeras och dokumenteras. I registerförteckningen ska därför anges:

1. Vem som registreras. Med detta avses exempelvis patienter anställda/medarbetare, medlemmar etc.
2. Vilka personuppgifter som registreras. Med detta avses exempelvis namn, kontaktuppgifter, personnummer, uppgifter om hälsa, diarienummer, IP-adress etc.
3. Vilka kommer att ta del av informationen. Med detta avses till vilka personuppgifterna lämnas ut till, exempelvis Socialstyrelsen, SKL, Skatteverket, namngivet personuppgiftsbiträde etc.

2.1.3 Ändamålet med hanteringen

Personuppgifter får endast samlas in för ett särskilt ändamål, och syftet med den aktuella personuppgiftshanteringen ska dokumenteras och tydligt beskrivas i registerförteckningen. Uppgifterna får inte användas på något annat sätt än vad som angavs i ändamålet när anmälan gjordes. Detta innebär att fler uppgifter än nödvändigt för att tillgodose ändamålet, inte får samlas in.

Tänk på att det inte är syftet med IT-systemet, utan syftet med personuppgiftshanteringen som ska dokumenteras.
Ett bra exempel för ändamål för ett loggningsverktyg är : " Syftet[1] med kontrollen är övervakning av säkerhets- eller tekniska skäl eller uppföljning av interna regler".

[1] https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/

Det räcker normalt inte heller att ett ändamål enbart är att "förbättra användarnas upplevelse", "it-säkerhet" eller "framtida forskning". Det är alltför brett uttryckt, och de registrerade kan inte bedöma vad sådan personuppgiftshantering kan innebära, enligt information hämtad från Datainspektionens hemsida.

2.1.4 Rättslig grund för hantering

Utan en rättslig grund är personuppgiftshanteringen inte laglig. Det finns sex rättsliga grunder i dataskyddsförordningen som kan vara aktuella för personuppgiftshanteringar: Samtycke, intresseavvägning, rättslig förpliktelse, myndighetsutövning, allmänt intresse och avtal. Inom SLSO används huvudsakligen nedanstående angivna rättsliga grunder:

- **Rättslig förpliktelse**: Det finns lagar eller regler som gör att den personuppgiftsansvarige måste hantera vissa personuppgifter i sin verksamhet.
- **Myndighetsutövning och uppgift av allmänt intresse**: Den personuppgiftsansvarige måste hantera personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse.
- **Avtal**: Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige, exempelvis anställningsavtal.
- **Samtycke:** Den registrerade har sagt ja till personuppgiftshanteringen.

Den rättsliga grunden samtycke bör endast användas *i undantagsfall*. Samtycket kan återkallas, den registrerade kan begära att uppgifterna raderas, vilket måste ske om samtycke är enda grunden för hanteringen. Samtycke kan bara användas när det verkligen föreligger ett fritt val för den registrerade. Ett exempel på det, är deltagande i forskning. Verksamheten har ansvar för att visa att den registrerade har fått tydlig information och gjort ett fritt och aktivt val att samtycka.

Hantering av känsliga personuppgifter är i grunden olagligt men lagstiftningen möjliggör att känsliga personuppgifter får hanteras enligt undantaget i art 9.2 h dataskyddsförordningen samt 2 kap. 4 § PDL.

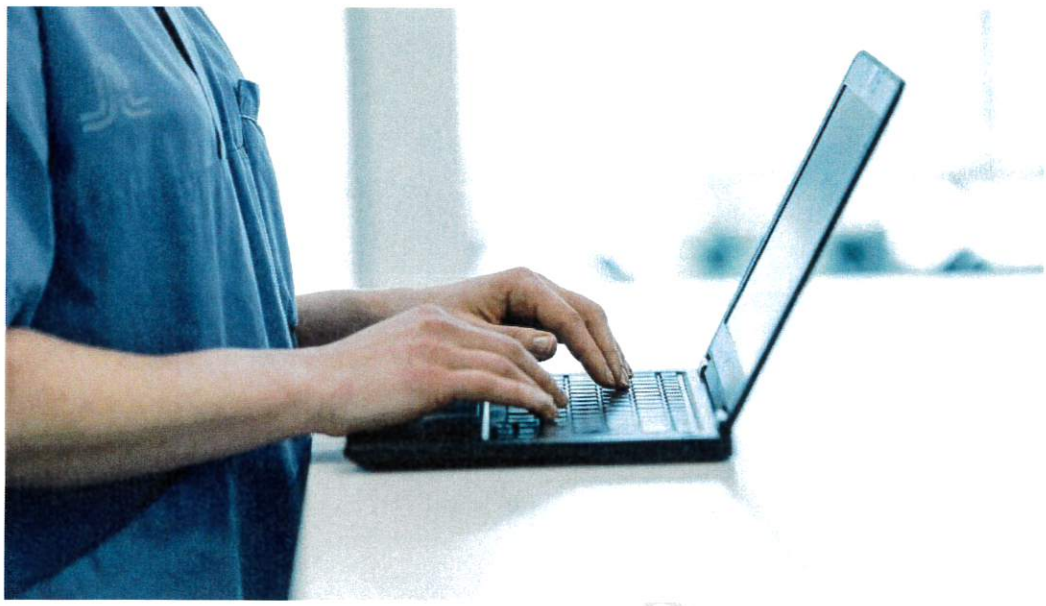
Patientdatalagen

GDPR / Dataskyddsförordningen

2.1.5 Hantering av personuppgifter i e-post

Hantering av personuppgifter ska främst ske i andra system än e-post. Exempel på system är Take Care eller Heroma. Hantering av personuppgifter i e-post räknas också som hantering av personuppgifter och samma krav gäller som för alla andra hanteringar.

Användaren ska betrakta e-post som oskyddad och Region Stockholms nätverk som öppna (osäkra). Detta innebär att meddelanden som skickas okrypterat via e-post inte kan betraktas vara skyddade från insyn, och att det därmed finns risk för att andra än den avsedda mottagaren kan ta del av innehållet.



Det finns inget absolut förbud mot att skicka personuppgifter i e-post. Ett e-postmeddelande med personuppgifter får inte ligga kvar i inkorgen eller i skickat-mappen hur lång tid som helst. När din hantering av personuppgifter är klar ska informationen antingen flyttas över till lämpligt system eller raderas. Den tid som en personuppgift lagras i e-posten ska begränsas till ett strikt minimum. Spara aldrig mejl med personuppgifter i Outlook "för att det kan vara bra att ha". Informera alla anställda på din enhet om ovanstående punkter.

I e-posten får du inte alls hantera eller spara personuppgifter som är **känsliga eller sekretessbelagda**. Om känsliga eller sekretessbelagda personuppgifter inkommer kan du till exempel inte vidarebefordra eller svara på mailet när det innehåller uppgifterna.

Skicka aldrig känsliga eller sekretessbelagda personuppgifter via e-post, till exempel uppgifter om någons hälsa eller politiska åsikter. Undvik även att skicka andra integritetskänsliga uppgifter som exempelvis värderingar av en person såsom social förmåga eller provresultat via e-post.

För över personuppgifter till andra system och radera mejlet. Om en anställd till exempel mejlar in och sjukanmäler sig, registrera det i lönesystemet och radera mejlet. Samma regler gäller vare sig du skickar e-post internt eller externt. Läs mer i dokumentet: *E-postanvändning riktlinje för SLSO (RIK-01681)*

2.1.6 Tidsintervall för bevarande/gallring

En av de grundläggande principerna i dataskyddslagstiftningen är principen om lagringsminimering, det vill säga att samla in så få personuppgifter som möjligt. Samla bara in de uppgifter som behövs för att kunna utföra arbetet.

Enligt dataskyddslagstiftning ska uppgifterna gallras/arkiveras vid inaktualitet. För vår verksamhet tar annan lagstiftning över och hanteras i enlighet med våra

informationshanteringsplaner som ska hanteras enligt Verksamhetsbaserad Informationsredovisning (VIR). Den talar om hur allmänna handlingar ska hanteras och förvaras.

När det gäller allmänna handlingar [2]har arkivlagstiftningen företräde framför dataskyddsförordningens bestämmelser om längsta bevarandetid för personuppgifter. Intresset av att bevara allmänna handlingar ska prioriteras framför integritetsskyddsintresset.

Läs mer om informationshanteringsplaner se länk

Regionarkivet

Insidan

2.1.7 Dataskyddsförordningen och arkivering

Dataskyddsförordningen reglerar hantering av personuppgifter i verksamheten. Ett syfte är att säkerställa bättre kontroll och säkerhet kring hanteringen.

Offentlighetsprincipen (med reglerna i tryckfrihetsförordningen, offentlighets- och sekretesslagen samt arkivlagen) syftar till att säkerställa allmänhetens tillgång till allmänna handlingar.

Dataskyddsförordningen hindrar inte regionen från att lämna ut allmänna handlingar enligt offentlighetsprincipen.

Arkivlagen reglerar skyldigheten för bland annat regioner att bevara sina allmänna handlingar.

Dataskyddsförordningen ställer krav på att personuppgifter ska arkiveras alternativt gallras när verksamhetens syfte/grund för hanteringen upphört. Det är därför viktigt att se över och ha väl övervägda tidsfrister i informationshanteringsplanerna.

2.1.8 Beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna

För att kunna dokumentera de vidtagna tekniska och organisatoriska säkerhetsåtgärderna i registerförteckningen ska ansvarig säkerställa efterlevnaden av Region Stockholms policy och riktlinje för informationssäkerhet.

Systemägaren ansvarar för att informationssäkerhet i enlighet med informationsägarens krav uppnås i det IT-system systemägaren ansvarar för.

Personuppgifter ska vara korrekta och uppdaterade. Den som hanterar personuppgifter måste se till att rätta eller radera felaktiga uppgifter omgående

Det är informationsägaren som ska klassificera informationen, bedöma risker och ställa säkerhetskrav, eftersom det är hos denne konsekvenserna av bristande

[2] Allmänna handlingar - riksdagens hemsida

Manual ej publicerad version

informationssäkerhet kan uppstå. Systemsäkerhet kräver ett samarbete mellan flera olika kompetenser, både någon från verksamheten som kan arbetsprocessen och vilka krav som finns och någon som har IT-kompetens och känner till vilka krav som ställs på IT-system utifrån policy/ riktlinje för informationssäkerhet och dataskyddsförordningen.

- Informationssäkerhetsklassning genomförs för att veta vilken typ av information systemet hanterar och vilka krav som ställs på hantering av denna. Informationen ska klassas utifrån konfidentialitet, riktighet, och tillgänglighet.
- Regelefterlevnad: Baserat på hur informationen klassats analyseras de krav som ställs på systemet. Läs mer om informationsklassning här.
- Riskanalyser: Identifiering och bedömning av risker vars konsekvenser kan leda till störningar i informationstillgången, allvarliga händelser eller extraordinära händelser. Föreligger en hög risk för den registrerades integritet ska en konsekvensbedömning genomföras för att visa att personuppgiftsansvarig har vidtagit tillräckliga åtgärder för att skydda den registrerades integritet och rättigheter.

2.1.9 Behörighet och loggning

Säkerhetskraven på IT-system som hanterar personuppgifter stärks genom dataskyddsförordningen. Personuppgifter ska exempelvis skyddas så att bara de som är behöriga kan se eller arbeta med uppgifterna. Uppgifterna måste även skyddas så de inte förstörs genom olyckshändelse.

Ett grundkrav på system som innehåller personuppgifter är att de går att behörighetsstyra. Säkerheten kring behörigheter beror mycket på tilldelning och avslutande av behörigheter. Om det dessutom gäller tillgång till känsliga personuppgifter är kraven ännu högre på fungerande rutiner för behörighetshantering och även loggningsfunktioner i systemen, exempel vem som gjorde vad och när.

Skapa arbetsrutiner för behörigheter:

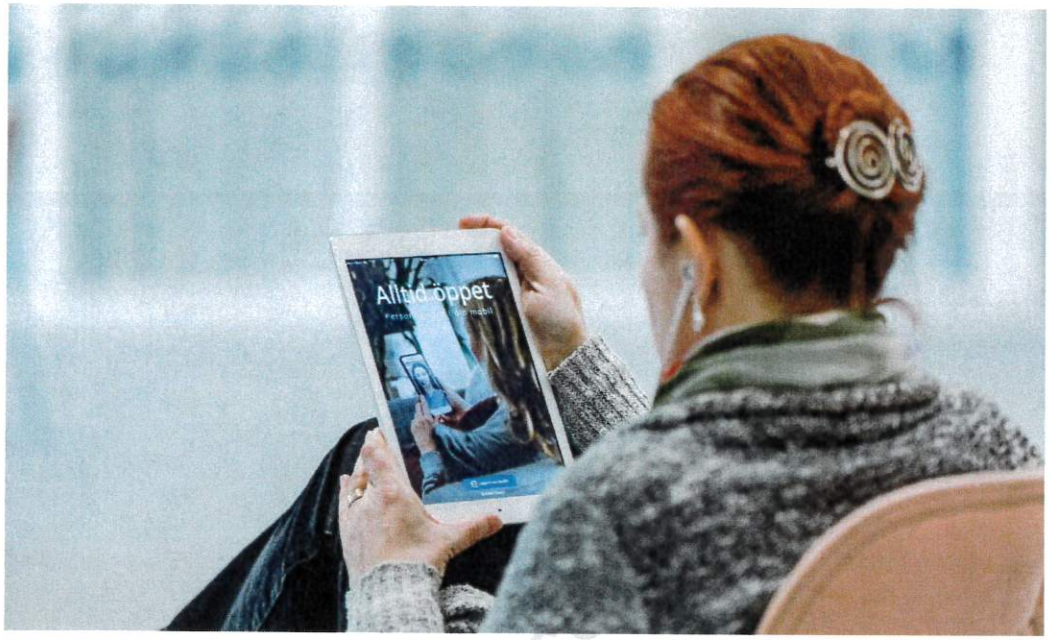
- Säkerställ att enheten har fungerande rutiner även när en medarbetare byter tjänst internt.
- Ha rutiner för att minst årligen kontrollera att behörigheterna är korrekta.
- Kraven på behörigheter gäller även våra leverantörer. Se därför regelbundet över vilka behörighet som finns hos våra leverantörer.

3 Rapportera personuppgiftsincidenter

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. Exempel på incidenter:

- Någon har kommit över ett lösenord som gör att den skulle kunna logga in i system som hanterar personuppgifter.
- Ett mail med känsligt eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- Ett glömt papper i skrivare som innehåller uppgifter om namn och sjukdomstillstånd.

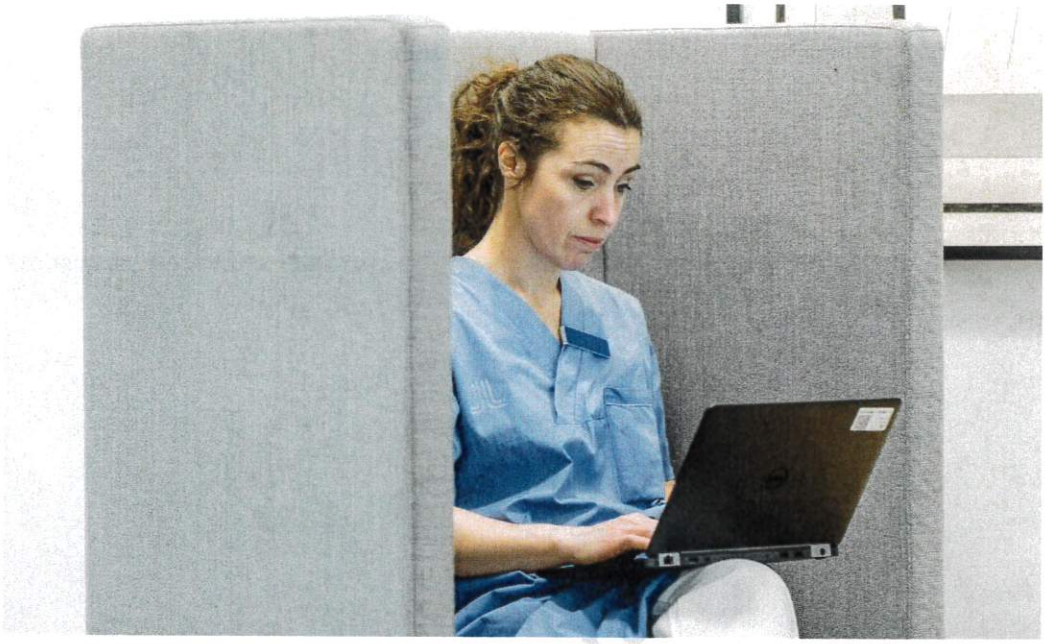
- En dator har fått skadlig kod som gör att obehörig skulle kunna komma åt personuppgifter.



3.1 Så här rapporteras en incident

En personuppgiftincident ska anmälas till Datainspektionen inom 72 timmar efter att den har upptäckts. Anmälan görs av dataskyddsombudet. Detta gäller även om incidenten inträffat hos ett av våra biträden, det vill säga någon av våra leverantörer. Därför är det viktigt att varje medarbetare rapporterar inträffad personuppgiftsincident.

Ännu ej publicerad



Alla personuppgiftsincidenter ska rapporteras. Det är viktigt för att vi ska kunna agera vid både allvarliga och mindre allvarliga brister. Varje medarbetare ansvarar för att rapportera risk för, misstanke om eller inträffande av en personuppgiftsincident. Inrapportering sker via Helpdesk alternativt till funktionsbrevlåda gdpr.slso@sll.se

Länk till rutin

4 Informationsplikt

Den registrerade har rätt att få information när hans eller hennes personuppgifter hanteras. Information om personuppgiftshanteringen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

4.1 Registerutdrag

Varje medborgare har rätt att få veta om myndigheten hanterar dennes personuppgifter. Personuppgiftsansvarig är skyldig att, vid förfrågan, ge ut dessa uppgifter till medborgaren genom ett så kallat registerutdrag.

Ett registerutdrag inkluderar både strukturerade och ostrukturerade data (Word-filer, Excel-filer, enklare listor etc.). Undantag finns: ett registerutdrag omfattar till exempel inte personuppgifter som finns i löpande text som utgör ett utkast eller en minnesanteckning.

Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk. I dataskyddsförordningen anges utförligt vilken information som ska ges.

Följande information ska lämnas:

- vem som är personuppgiftsansvarig
- kontaktuppgifter till dataskyddsombudet
- ändamålen med hanteringen
- den rättsliga grunden för hanteringen
- vilka som har tillgång till uppgifterna
- den period personuppgifterna kommer att lagras
- rätten att korrigera felaktiga uppgifter
- möjligheten att kontakta Datainspektionen som är tillsynsmyndighet.

Länk till riktlinjen för registerutdrag:

5 Personuppgiftsbiträdesavtal

Den som samlar in personuppgifter med stöd av en rättslig grund är personuppgiftsansvarig (PuA). SLSO är personuppgiftsansvarig för exempelvis patientdata som samlas i samband med vård eller smittskydd. Personuppgiftsansvarig ansvarar för vilken data som samlas in och på vilket sätt den ska hanteras. Personuppgiftsbiträde (PuB) är en extern part såsom en annan organisation eller leverantör som hanterar personuppgifter för den personuppgiftsansvariges räkning.

Ett PuB-avtal är ett avtal som skrivs mellan personuppgiftsansvarig och personuppgiftsbiträdet (leverantör som utför en tjänst eller levererar ett IT-system och i samband med detta hanterar person-uppgifter). PuB - avtalet blir då en bilaga till leverantörsavtalet.

Varje enhet ansvarar för att PuB-avtal ingås med samtliga leverantörer och externa aktörer där personuppgifter överlämnas för hantering.

Ärnu ej fastställd version



OBS! Om en enhet sluter avtal med en annan vårdgivare eller laboratorieverksamhet behövs inget PuB-avtal då motparten i detta fall måste följa patientdatalagens regler i andra kapitlet.

I avtalet anges att personuppgiftsbiträdet får hantera personuppgifterna bara i enlighet med instruktionerna och vidta de säkerhetsåtgärder som den personuppgiftsansvarige kräver.

Även personuppgiftsbiträden har fått skadeståndssanktionerade skyldigheter, till exempel att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter. Detta kommer att påverka inte minst många IT-leverantörer som hanterar personuppgifter för vår räkning.

PUB-avtal som upprättats innan 25 maj 2018 ska uppdateras.

Kontakta dataskyddsombudet för stöd i arbetet med PUB-avtal.

Länk till och instruktion till PuB-avtal, avtalsmall samt mall till bilaga till PuB-avtal :