Datasäkerhetspolicy för verksamhetsenheter inom social- och hälsovården

Godkänd: Social- och hälsovårdsnämnden, datum 25.9.2012
Uppdaterad: Pia-Maria Sjöström, datum 6.5.2016
Pia-Maria Sjöström/Solveig Sandvik-Nyberg, datum 9.5.2019

1. Inledning

Informationsbehandlingen stöder serviceproduktionen inom Social- och hälsovårdsverket i Jakobstad, och servicens effektivitet är i sin tur beroende av informationsbehandlingen. Informationsmaterialet innehåller sådana uppgifter om patienter, klienter, anställda och verksamheten som enligt finsk lagstiftning och EU:s dataskyddsförordning ska skyddas. Informationsbehandlingen bör vara effektiv, felfri och säker.

Datasäkerhetspolicyn definierar de principer, verksamhetssätt, det ansvar samt den uppföljning och övervakning som ska iakttas i verksamhetsenheten för att förverkliga och utveckla datasäkerheten. Datasäkerhetspolicyn kompletteras av **dataskyddets plan för egenkontroll**, i vilken ingår en årlig **datasäkerhetsplan** samt av detaljerade bestämmelser och anvisningar.

Datasäkerhetspolicyn styrs av följande principer:

- Datasäkerhet och datasekretess är enligt finsk lagstiftning en del av den dagliga verksamheten inom vår organisation och gäller hela verksamheten och personalen.
- Datasäkerheten bör iakttas i allt arbete, vilket betyder att data bör skyddas mot hot av olika slag i syfte att säkerställa verksamhetens kontinuitet, minimera riskerna i verksamheten samt maximera resultatet av verksamheten och investeringarna.
- Datasäkerhets- och datasekretessfrågor bör beaktas oberoende av medium.
- Pappersdokument, elektroniska datareserver, datanät, datatekniska anordningar, datasystem med tillhörande tjänster bör skyddas både i normala och i undantagsförhållanden.
- För att uppnå datasäkerhet ska man implementera skyddsmekanismer, som består av verksamhetsprinciper, processer, organisationsstrukturer samt programvaru- och maskinvarufunktioner.
- Konfidentiella, känsliga och övriga sekretessbelagda ärenden omfattas av tystnadsplikten oberoende av hur eller var de har lagrats eller på vilket sätt uppgifterna har erhållits.
- Förmännen och övriga ledningen ska se till att personalen får utbildning eller introduktion i datasäkerhetsbestämmelser och anvisningar.
- Styrningen, övervakningen och uppföljningen av datasäkerheten ska organiseras.

2. Omfattning

Verksamhetsenhetens datasäkerhetspolicy, som fastställts av social- och hälsovårdsnämnden, omfattar alla till verksamheten hörande informationsbehandlingsuppgifter inom verksamhetsenheten. Varje tjänsteinnehavare, anställd och förtroendevald inom Social- och hälsovårdsverket i Jakobstad samt var och en som använder verksamhetsenhetens data och datasystem bör känna

till den här datasäkerhetspolicyn och iaktta de anvisningar och bestämmelser som utfärdats på basis av den. Verksamhetsenhetens externa aktörer inom hälso- och sjukvård, leverantörer och andra utomstående instanser bör också förbinda sig att iaktta den här datasäkerhetspolicyn samt nationella normer och anvisningar som villkor för att – i den utsträckning uppgifterna förutsätter – få åtkomst till verksamhetsenhetens datasystem och informationsmaterialet i dem.

3. Datasäkerhet

Datasäkerhet innebär att man skyddar informationsbehandlingen och arkiveringen. Datasäkerheten består av uppgifternas konfidentialitet, integritet, tillgänglighet, användbarhet och oavvislighet samt av övervakningen av informationsbehandlingen.

Till datasäkerheten hör datasäkerhetsorganisationen; databehandlarnas arbetssätt; metoder, verktyg och åtgärder för att skydda data; resurser för arbetet samt apparaturens och utrymmenas datasäkerhetsegenskaper.

Datasäkerhet i enlighet med den godkända datasäkerhetspolicyn bör ingå som en naturlig del i all verksamhet. Utvecklingen och underhållet av datasäkerheten är en del av verksamhetsenhetens allmänna säkerhetsverksamhet, riskhantering och interna kontroll.

4. Datasäkerhetsarbete

Datasäkerhetsarbetet går ut på att planera och genomföra de åtgärder som bör vidtas för att uppnå datasäkerhet. Målet för datasäkerhetsarbetet är att säkerställa att datasystem och datanät som är viktiga för verksamhetsenhetens verksamhet fungerar utan avbrott, att förhindra att uppgifter och datasystem hamnar hos utomstående samt förhindra att de används utan befogenheter, att data förstörs eller förvrängs oavsiktligt eller avsiktligt samt att minimera de skador som uppstår. Förutom att trygga informationsbehandlingen inom verksamheten under normala förhållanden, bereder man sig på risksituationer som avbryter verksamheten och på återhämtningen från dem.

En verksamhetsenhet inom social- och hälsovården ansvarar som en del av datasäkerhetsarbetet också för planeringen och förverkligandet av datasäkerhetsarbetet i anslutning till skyddet av patient- och klientjournaler och andra handlingar som innehåller patient- och klientuppgifter.

5. Organisering och ansvarsfördelning

Datasäkerheten leds och övervakas av stadsstyrelsen. Stadsdirektören beslutar om målen, organiseringen, resurserna och verksamhetsbefogenheterna inom olika delområden av utvecklingsverksamheten som gäller verksamhetsenhetens totala säkerhet samt utser datasäkerhetsansvarig och dataskyddsombud.

Den datasäkerhetsansvariga ansvarar för verksamhetsenhetens datasäkerhetsarbete som helhet inom ramen för de resurser och verksamhetsbefogenheter som ledningen har gett. Den datasäkerhetsansvarigas befogenheter och skyldigheter måste definieras. Den datasäkerhetsansvariga ansvarar också för informationen om datasäkerhetsfrågor utåt och inom verksamhetsenheten

på ett allmänt plan. Hen ansvarar för bestämningen och bedömningen av datasäkerhetsnivån i verksamhetsenheten och för rapporteringen samt för den övriga administrativa datasäkerheten. Hon eller han ansvarar för utarbetandet av utvecklingsplaner för datasäkerheten, för övervakningen av att de förverkligas, för främjandet av kunskapen om datasäkerheten och för användningen av säkra arbetssätt inom verksamhetsenheten och när det gäller tjänster som enheten köper samt för rapporteringen till ledningen.

Dataskyddsombudet ska fungera som sakkunnig åt registerupprätthållaren för att man ska uppnå ett bra sätt att hantera personuppgifter och en så hög nivå som möjligt på dataskyddet. Han eller hon har som uppgift att stöda personalen i dataskyddsfrågor och hjälpa till att förverkliga de förpliktelser som GDPR ålägger registerupprätthållaren.

Dataskyddsgruppen, som tillsätts av **social- och hälsovårdsdirektören**, representerar dataskyddsaspekterna i anslutning till verksamhetsenhetens centrala funktioner. För dataskyddsgruppen utses en ordförande och en sekreterare. Gruppens medlemmar ansvarar för beredningen av ärenden som gäller dataskyddsprocesserna inom det egna ansvarsområdet. Dataskyddsgruppen behandlar linjedragningar och direktiv för dataskyddsarbetet, innan de föreläggs ledningen för godkännande. Dataskyddsgruppens sammansättning bestäms av organisationen och dit hör bland annat dataskyddsombudet, den datasäkerhetsansvariga, de som ansvarar för verksamheten inom olika delområden, patientombudsmannen, ansvars- och kontaktpersoner för patient- och klientregister, samt ansvariga för patientuppgiftssystemen.

Varje datasystem har en **ägarenhet** och en **ansvarsperson.** Till ansvarspersonens skyldigheter hör att definiera de krav som ställs på datasystemets funktion och säkerhet (t.ex. hur kritiskt systemet är, planeringen av kontinuiteten och förfarandet vid säkerhetskopiering) samt att bevilja och övervaka användarrättigheter. **Enhetens förman** ansvarar för att anvisningar om datasäkerhetsfrågor följs, samt för information om och övervakning av datasäkerheten inom den egna enheten.

Inom organisationen är verksamhetsenhetens alla **anställda**, alla som hanterar information, alla upprätthållare och användare av datasystem och datanät för egen del ansvariga för att datasäkerheten förverkligas samt för att datasäkerhetsanvisningarna iakttas. Varje person är skyldig att rapportera hot och avvikelser i anslutning till datasäkerheten åt sin förman eller åt dataskyddsombudet.

6. Förverkligandet av datasäkerheten

Förverkligandet av datasäkerheten grundar sig på den här skriftliga datasäkerhetspolicyn som godkänts av social- och hälsovårdsnämnden och som ska delges varje anställd och alla som använder datasystem i verksamhetsenheten.

Verksamhetsenhetens datasäkerhetsprinciper grundar sig på förpliktande europeiska, nationella, allmänna och branschspecifika bestämmelser, anvisningar och standarder som är normgivande för datasäkerhet, personregister, god informationshanteringssed och informationens kvalitet.

Ändringar i lagstiftning och regelverk beaktas när man utvecklar datasäkerheten inom verksamhetsenheten.

Förverkligandet och upprätthållandet av datasäkerheten beskrivs detaljerat i **dataskyddets plan för egenkontroll**. Förverkligandet av datasäkerheten bör utgå från de krav som verksamheten

och servicen samt säkerhetsklassen för varje uppgift och datasystem ställer på informationsbehandlingen i fråga om säkerhet, användbarhet, sekretess och kvalitet samt i fråga om verksamhetens kontinuitet och bedömningen av de risker som verksamheten är utsatt för. Med hjälp av regelbundet utförda säkerhetsanalyser utreder man kraven, bedömer riskerna och fastställer säkerhetsåtgärder utgående från dem.

Att uppnå målen för datasäkerheten är en fortgående process, som sker med hjälp av administrativa och tekniska lösningar. De beskrivs i planen för egen kontroll och vid behov i särskilda utvecklingsplaner för datasäkerheten som uppgjorts för användarmiljöerna och enheterna.

Användarnas verksamhet styrs av de regler för användningen som ingår i planen för egen kontroll och av verksamhetsdirektiv som fastställts och finns tillgängliga samt genom utbildning i datasäkerhet. Varje användare undertecknar en datasekretessförbindelse när hen får rätt att använda datasystemen och informationsmaterialet i den utsträckning som uppgifterna förutsätter.

7. Uppföljning och övervakning av datasäkerheten

Användarna och upprätthållarna bör anmäla brister i dataskyddet och datasäkerheten som de observerat, missbruk som rör datasäkerheten eller misstankar om brott mot datasäkerheten åt sin förman eller åt den datasäkerhetsansvariga eller dataskyddsombudet.

Enhetens förman är skyldig att övervaka förverkligandet av datasäkerheten inom den egna enheten.

Dataskyddsombudet har som uppgift att följa upp och övervaka förverkligandet av dataskyddet i datasystemen som används inom Social- och hälsovårdsverket i Jakobstad och vidta åtgärder för att korrigera de svagheter i dataskyddet som observerats. Dataskyddsombudets uppgift är att följa med och övervaka att hanteringen av personuppgifter sker i enlighet med finsk lagstiftning och EU:s dataskyddsförordning och att fungera som sakkunnig i dataskyddsfrågor.