Dataskyddspolicy

Itä-Uusimaa
Östra Nyland

Hyvinvointialue
Välfärdsområde

Innehållsförteckning

1. Godkännande

Östra Nylands välfärdsområdes dataskyddspolicy godkänns av välfärdsområdesstyrelsen. Policyn är i kraft tills vidare efter det bekräftade ibruktagandet. Policyn uppdateras vid behov och en ny uppdaterad version upphäver den gamla policyn med ett separat beslut av välfärdsområdesstyrelsen.

Användning: För användning av Östra Nylands välfärdsområdes personal och intressentgrupper
Användningsområde: Östra Nylands välfärdsområdes organisation

Datum	**Godkännande**	**Författare**	**Godkännare**
xx.xx.2022	Ibruktagande av dataskyddsplanen	Datasäkerhetsexpert Tuomas Lintula	Östra Nylands välfärdsområdesstyrelse

2. Ändringslogg

Originalversionen 1.0 av den här policyn upprättades 3.2.2022. Utförda ändringar:

3.2.2022/Version 1.0/Datasäkerhetsexpert Tuomas Lintula

-Första versionen av policyn har upprättats.

8.6.2022/Version 1.1/Datasäkerhetsexpert Tuomas Lintula

-Policyn har redigerats i Östra Nylands välfärdsområdes officiella dokumentmall.

23.6.2022/Version 1.2/Datasäkerhetsexpert Tuomas Lintula

-Sak- och strukturfel har korrigerats.

-Styckena Bilaga 2, Användningsrättigheter, Logguppgifter och Upphandlingar har lagts till.

-Varje arbetstagares ansvar har lagts till i ansvaren.

3. Inledning

”I Östra Nylands välfärdsområdes dataskyddspolicy definieras de principer som gäller datasäkerhet.”

3.1. Vad är datasäkerhet?

Östra Nylands välfärdsområdes verksamhet och tjänster baseras i allt större utsträckning på information. För att kunna användas effektivt ska informationsstödjande arrangemang fungera ändamålsenligt i alla situationer. Detta förutsätter effektivt ledarskap som ett stöd för tillförlitliga genomföranden och kompetent personal.

Med datasäkerhet avses administrativa och tekniska funktioner som används för att säkerställa följande för informationen:

- **Konfidentialitet**; uppgifter är tillgängliga endast för dem som är berättigade till att använda dem,
- **Integritet**; uppgifter får endast ändras av personer som är berättigade till det,
- **Tillgänglighet**; uppgifter är tillgängliga för och får nyttjas av dem som är berättigade till att använda dem.

3.2. Dataskyddspolicy

Med stöd av 4 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019) ska Östra Nylands välfärdsområdes informationshantering och dataskyddsverksamhet vara systematisk.

Östra Nylands välfärdsområdesstyrelse definierar här de principer, ansvar och målsättningar i Östra Nylands välfärdsområdes dataskyddspolicy som gäller datasäkerhet.

Policyn har ett allmänt innehåll varifrån man hänvisar till sektorspecifika dataskyddsplaner och -anvisningar.

Policyn fungerar som en grund för de sektorspecifika dataskyddsplaner och -anvisningar som gäller välfärdsområdets datasäkerhet och vars uppgift är att precisera de föreskrifter som anges i välfärdsområdets dataskyddspolicy samt ge anvisningar om den praktiska tillämpningen av dem. Sektorerna har sina egna dataskyddsplaner, eftersom de omfattas av egna speciallagstiftningar samt dataskyddskrav. Därtill är det enklare att hantera och underhålla de sektorspecifika planerna och anvisningarna.

Östra Nylands välfärdsområdes dataskyddspolicy gäller hela välfärdsområdets organisation samt representanter för alla dess intressentgrupper, som inom ramen för sina uppdrag behandlar information som ägs eller innehas av välfärdsområdet. Policyn omfattar de uppgifter som välfärdsområdet använder, äger och administrerar oavsett uppgifternas framställningssätt, form, skyddsnivå eller fasen av uppgifternas livscykel. Dataskyddspolicyn finns tillgänglig för användarna i elektronisk form på välfärdsområdets webbplats och vid behov som pappersversion.

4. Förpliktelser om välfärdsområdets datasäkerhet

”Östra Nylands välfärdsområdes dataskyddsverksamhet styrs av lagstiftning, anvisningar, referensramar och riktlinjer.”

Utvecklandet och underhållandet av välfärdsområdets dataskyddsverksamhet styrs till tillämpliga delar av lagstiftning, anvisningar och referensramar. I praktiken kan dessa styrande faktorer delas upp i tre viktiga helheter:

- Lagstiftning
- Anvisningar och referensramar
- Sektorspecifika riktlinjer

4.1. Lagstiftning

Välfärdsområdets allmänna dataskyddsprinciper regleras av **lagen om informationshantering inom den offentliga förvaltningen** (906/2019). Därutöver ställer **Europaparlamentets och rådets allmänna dataskyddsförordning** (2016/679, GDPR) krav på datasäker behandling av personuppgifter när välfärdsområdet fungerar som registeransvarig. Den nationella lagstiftningen om behandling av personuppgifter som kompletterar dataskyddsförordningen behandlas i **lagen om integritetsskydd i arbetslivet** (759/2004) samt i **dataskyddslagen** (1050/2018).

4.2. Anvisningar och referensramar

Välfärdsområdets datasäkerhet styrs i tillämpliga delar av följande referensramar:

- Lagstiftning som förpliktar välfärdsområdet
- Välfärdsområdets strategi och därifrån härledda krav
- Välfärdsområdets dataskyddspolicy, sektorernas dataskyddsplaner och -anvisningar

- Rekommendationer från Delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA)
- Anvisningar från statsförvaltningens informationssäkerhet (VAHTI)
- Anvisningar och rekommendationer från Statens center för informations- och kommunikationsteknik (Valtori)

4.3. Sektorspecifika riktlinjer

Sektorspecifika riktlinjer och detaljerade villkor gällande datasäkerhet har registrerats i välfärdsområdets sektorers egna dataskyddsplaner och -anvisningar.

5. Datasäkerhetsmål

”Datasäkerheten ska åtminstone ligga på grundläggande nivå i hela välfärdsområdet.”

Avkall på datasäkerheten äventyrar verksamhetens kontinuitet och tjänsternas tillgänglighet inom
välfärdsområdet. Datasäkerhetsavvikelser orsakar reparationskostnader, serviceavbrott och dåligt rykte, samt kan leda till rättsliga följder.

5.1. Riskbaserat tillvägagångssätt

Dataskyddsåtgärder ska alltid ställas i proportion till informationen som ska skyddas; för att skydda offentlig information krävs inte likadana åtgärder som för att skydda sekretessbelagd information. Genom att kartlägga datasäkerhetshot bildar man sig en uppfattning om risker som riktas mot informationen som ska skyddas. Dessa risker utvärderas och utifrån dem genomförs dataskyddsåtgärder.

Dataskyddsarrangemangen som baseras på riskbedömningen genomförs enligt principen för skydd på flera nivåer. Dataskyddsåtgärdernas tillräcklighet bedöms mot den offentliga förvaltningens allmänna kravnivåer och etablerade standarden inom branschen. Exempel på dessa är de nationella utvärderingskriterierna för (data)säkerhet (Katakri) och säkerhetskriterier för molntjänster (Pitukri).

Vid hantering av informations- och ICT-risker tillämpar man välfärdsområdets anvisningar och föreskrifter om riskhantering. Sektorerna bedömer behovet av skyddsåtgärder för sina uppgifter
och informationssystem och fastställer dataskyddsarrangemang.

5.2. Dataskyddsnivåer

Informationssystemets skyddsnivå bestäms enligt den information som kräver mest skydd. Man måste ta hand om informationsmaterialens skyddsbehov med hjälp av nödvändiga tekniska lösningar och administrativa processer på så sätt att de alltid dimensioneras med betydelsen av det objekt som ska skyddas. Man ska se till att informationsmaterialet är tillgängligt, även om det finns strikta krav kopplade till dess konfidentialitet.

5.2.1. Grundläggande nivå för dataskydd

Man ska ha kartlagt datasäkerhetsriskerna kring verksamheten och fastställt uppgifter och ansvar gällande skötseln av datasäkerhet och behandlingen av dokument. Uppgifternas åtkomst och användbarhet ska tryggas i olika situationer, även i undantagssituationer.

Om systemet omfattar sekretessbelagd information som regleras i offentlighetslagen (24.1 1–32)
eller i speciallagar, ska dess dataskydd genomföras åtminstone enligt den grundläggande nivå som beskrivs
i VAHTI-anvisningarna (i anvisningarna använder man beteckningen säkerhetsnivå IV, skyddsnivå IV eller begränsad användning).

Myndigheternas säkerhetsklassificerade information ska behandlas enligt de krav som angetts för den aktuella säkerhetsklassen. Behandling av säkerhetsklassificerad information kan ske både elektroniskt och på andra sätt (t.ex. på papper).

5.2.2. Upphöjd nivå för dataskydd

För en del av välfärdsområdets verksamheter ska målnivån vara högre än grundläggande nivå.

Den högre kompetensnivån för den allmänna grundläggande nivån för dataskydd inom dataskyddskompetensen kan behövas i penning- och betalningsrörelsen, behandlingen av sekretessbelagda personuppgifter samt personuppgifter som ingår i särskilda personuppgiftsgrupper (t.ex. hälsouppgifter), verksamhet kopplad till säkerhet, dataskydd

och beredskap, samt när man behandlar dokument som statsförvaltningen sekretessbelagt, eller annat sekretessbelagt material.

Sådana här specialarrangemang är i praktiken exempelvis kommunikationssystem på upphöjd
dataskyddsnivå (krypterad e-post, krypterad mobiltelefon), grupparbetsmiljöer (krypterad grupparbetsmiljö), lagringsmedier eller arbetsstationer på upphöjd skyddsnivå.

6. Dataskyddets organisation och ansvar

”Dataskyddets ansvar och förpliktelser är fastställda.”

Östra Nylands välfärdsområdes viktigaste aktörer med tanke på datasäkerhet och deras roller med ansvar fastställs nedan.

Välfärdsområdesstyrelsen är välfärdsområdets högsta organ som beslutar om den övergripande säkerheten. Välfärdsområdesstyrelsen godkänner de ändringar som föreslagits till dataskyddspolicyn.

Välfärdsområdesdirektören fungerar som ägare av datasäkerhet och -skydd inom välfärdsområdet och skapar således förutsättningar för ändamålsenligt förverkligande av dessa.

Välfärdsområdets datasäkerhetsansvarige ansvarar för att förverkliga och integrera välfärdsområdets dataskydd i den övergripande säkerhetens delområden. I ansvaret ingår nödvändig planering, anvisning, uppföljning och utveckling samt koordinering av hantering av datasäkerhetsrisker och -avvikelser. Datasäkerhetsansvarige rapporterar till välfärdsområdets ledning.

Sektorernas ledning ansvarar för genomförandet av datasäkerheten och dataskyddet i sin underordnade verksamhet. Därutöver godkänner sektorernas ledning de dataskyddsplaner och -anvisningar som tas i bruk inom respektive sektor.

Sektorernas datasäkerhetsansvariga ansvarar för att sektorns dataskydd förverkligas och integreras i välfärdsområdets dataskyddshelhet. I ansvaret ingår nödvändig planering, anvisning, uppföljning och utveckling samt koordinering av hantering av datasäkerhetsrisker och -avvikelser.

Chefen ansvarar för genomförandet av datasäkerheten och dataskyddet i sin underordnade verksamhet.
Användaren av uppgifter och informationssystem ansvarar för egen del för iakttagandet av föreskrifterna och anvisningarna. Dessutom är alla användare ansvariga för att utan dröjsmål meddela om avvikelser, hot eller risker som gäller datasäkerhet och dataskydd i enlighet med separata anvisningar.

Ägaren av informationen, informationssystemet eller tjänsten ansvarar för följande i anslutning till sitt ägande:

- Fastställande, godkännande och tillsyn av användarna och användningsrättigheterna
- Förverkligande av riskhantering
- Säkerställande av informationens integritet
- Klassificering av information (fastställande av offentlighet och sekretess samt arkivbildning).

Producenten för välfärdsområdets IT-tjänster ansvarar för förverkligandet av dataskyddet och den tekniska tillsynen i informationssystemmiljön med metoder som lagen tillåter och samarbetsförfaranden auktoriserar.

Administratörerna övervakar förverkligandet av dataskydd i sina egna ansvarsområden. Administratörerna sköter applikationens underhållsåtgärder och säkerställer att systemet används i enlighet med lagar, författningar och anvisningar.

Dataskyddsombudet har i uppgift att ge experthjälp både till organisationens personal och till ledningen i dataskyddsfrågor. Dataskyddsombudet rapporterar till välfärdsområdets ledning.

Arbetstagaren är förpliktigad till att följa givna anvisningar och föreskrifter. Därutöver är alla arbetstagare förpliktigade till att anmäla datasäkerhetsavvikelser.

7. Datasäker användning av information och informationssystem

”Man säkerställer informationens konfidentialitet, integritet och tillgänglighet.”

Information som är i välfärdsområdets bruk samt informationssystem, utrustning och programvaror är avsedda för att sköta arbetsuppgifter. I välfärdsområdets informationssystemmiljö får man endast använda informationssystem, utrustning och programvaror som är godkända av IT-tjänsterna. Installationsarbete får endast utföras av aktör som välfärdsområdet har gett befogenheter till detta.

7.1. Hantering av användningsrättigheter

Användningsrättigheter till välfärdsområdets information och informationssystem beviljas för att sköta arbetsuppgifter utifrån arbetsroll och i den omfattning som arbetsuppgifterna kräver. Användningsrättigheterna godkänns utifrån ansökan av informationssystemets ägare eller en av denne befullmäktigad aktör. Grundläggande användningsrättigheter skapas automatiskt baserat på personalsystemets uppgifter.

Ansvaret om användningsrättigheterna ligger alltid hos den sektor som beviljar dem. Chefen ska se till att hens underordnade har ändamålsenliga och uppdaterade användningsrättigheter.

7.2. Insamling av logguppgifter

Logguppgifter innebär dokument (händelseloggning) om en viss händelse vid en viss tidpunkt. När informations- och kommunikationssystemets verksamhet eller en autentiserad användares aktiviteter obestridligen ska visas, ska nödvändig händelseloggning utföras med tekniska resultat (loggsystem) som bevarar informationens integritet.

Försummelser och missbruk leder till omedelbart ingripande med välfärdsområdets normala disciplinära metoder eller på det sätt som lagstiftningen förutsätter. Säkra sätt för att behandla information och hantering av datasäkerhetsavvikelser beskrivs i separata anvisningar.

8. Upprätthållande av dataskyddskompetens och -kännedom

”Utbildning av personalen är en förutsättning för att kunna skapa och upprätthålla en dataskyddskultur.”

Varje arbetstagare som börjar med ett nytt uppdrag instrueras i enlighet med välfärdsområdets introduktionspraxis i datasäkerhetens grunder och förverkligandet av datasäkerhet i de egna arbetsuppgifterna. Den nya arbetstagaren ska genomgå välfärdsområdets dataskyddsutbildning så snart som möjligt efter att hen börjat sitt uppdrag, så att hen ska kunna beviljas användningsrättigheter till välfärdsområdets informationssystem och -tjänster. Därutöver har alla arbetstagare tillgång till uppdaterade dataskyddsanvisningar och det anordnas regelbundet fortbildning i datasäkerhet.

Upprätthållande av dataskyddskompetens beskrivs mer detaljerat i de sektorspecifika dataskyddsplanerna och -anvisningarna. Ansvariga för underhåll, utveckling och ledarskap i datasäkerhet och dataskydd erbjuds tillräcklig administrativ och teknisk utbildning.

9. Uppföljning, underhåll och utveckling av datasäkerhet

”Människor, processer och teknologi.”

Denna Östra Nylands välfärdsområdes dataskyddspolicy gås igenom årligen och uppdateras av välfärdsområdets datasäkerhetsansvarig vid behov.

Dataskyddsplanerna och -anvisningarna för Östra Nylands välfärdsområdes sektorer gås igenom årligen och uppdateras av respektive sektors datasäkerhetsansvarig vid behov.

Östra Nylands välfärdsområdes dataskyddsarbete baseras på människors, processers och teknologiers ständiga utveckling enligt följande skeden:

- **Planering**; man producerar planer och anvisningar på basis av analyser och utvärderingar.
- **Genomförande**; planeringsskedets resultat tas i bruk i välfärdsområdets verksamhet.
- **Uppföljning**; man utför teknisk tillsyn samt administrativ uppföljning.
- **Förändringshantering**; baserat på det som man har lärt sig i uppföljningsskedet utför man förändringshantering i enlighet med välfärdsområdets förändringshanteringsprocess.

10. Upphandlingar och avtal

”Datasäkerhet tas i beaktande vid upphandlingar och avtal.”

Vid upphandlingar ska man följa upphandlingslagstiftningen, välfärdsområdets upphandlingsanvisningar samt den offentliga förvaltningens allmänna rekommendationer om att beakta datasäkerheten hos ICT-upphandlingarna och upphandlingens objekt.

Man ska fästa särskild uppmärksamhet vid att informations- och kommunikationstekniska upphandlingar passar välfärdsområdets helhetsarkitektur. Vid informations- och kommunikationstekniska upphandlingar ska man inom ramen för upphandlingslagstiftningen sträva efter så enhetliga upphandlingar som möjligt som drar nytta av existerande kompetens med beaktande av ekonomi och risker.

Redan när man planerar upphandlingen ska man definiera vilken dataskyddsnivå man vill uppnå, vilka de ändamålsenliga dataskyddsarrangemangen är och hur man övervakar förverkligandet av datasäkerheten.

För dataskyddets del förutsätter dataskyddsförordningen att välfärdsområdet endast får använda sådana tjänsteleverantörer eller andra behandlare av personuppgifter som tillämpar tillräckliga tekniska och organisatoriska skyddsåtgärder. Behandlingen ska uppfylla dataskyddsförordningens krav och säkerställa skyddandet av den registrerades rättigheter.

Bilaga 1 Välfärdsområdets dataskyddsanvisningar

I den här bilagan har man samlat ihop anvisningar om välfärdsområdets dataskydd. Förutom anvisningarna nedan kan sektorerna ha egna preciserande anvisningar.

- Dataskyddsanvisningar för chefer
- Personalens dataskyddsanvisningar
- IT-personalens dataskyddsanvisningar
- Dataskyddsanvisningar för informationssystemets ägare
- Anvisningar för hantering av datasäkerhetsavvikelser
- Anvisningar om lösenord

Bilaga 2 Mer information

Centrala lagar för datasäkerhet:

- Lagen om informationshantering inom den offentliga förvaltningen 906/2019
- Lagen om tillhandahållande av digitala tjänster 306/2019
- Lagen om tjänster inom elektronisk kommunikation 917/2014
- Lagen om offentlighet i myndigheternas verksamhet 621/1999

Informationshanteringsnämndens anvisningar och rekommendationer, till exempel följande:

- Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet

Centrala allmänna dataskyddsanvisningar som ges till den offentliga förvaltningen (Vahti-anvisningarna) är de nyaste
anvisningarna, till exempel följande:

- Vahti 22/2017 Ohje riskienhallintaan
- Vahti 8/2017 Tietoturvapoikkeamatilanteiden hallinta
- Vahti 2/2016 Toiminnan jatkuvuuden hallinta
- Vahti 2/2014 Tietoturvallisuuden arviointiohje
- Vahti 2/2012 ICT-varautumisen vaatimukset
- Vahti 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (behandlingskrav beskrivs i bilagorna)

Följande är centrala för den offentliga förvaltningens dataskydd:

- Katakri: Verktyg för informationssäkerhetsauditering för myndigheter
- Pitukri: Säkerhetskriterier för molntjänster

Andra anvisningar från den offentliga förvaltningen:

- Turvallisen sovelluskehityksen käsikirja, Befolkningsregistercentralen

- Handboken Säker utveckling, Cybersäkerhetscentret, Transport- och kommunikationsverket Traficom