Punainen Risti

Dataskyddsdokumentation
Skapad: 27.4.2018
Uppdaterad: 14.1.2020

RIKTLINJER FÖR DATASKYDD

---

1 FINLANDS RÖDA KORS SYFTE OCH GRUNDLÄGGANDE PRINCIPER

Syftet för Finlands Röda Kors är enligt 2 § i organisationens regler att under alla förhållanden skydda liv och hälsa, samt försvara människovärdet och mänskliga rättigheter, främja samarbete och fred mellan folken, rädda människoliv i hemlandet och utomlands, hjälpa de mest utsatta genom att förebygga och lindra mänskligt lidande, stödja och hjälpa landets myndigheter att göra humanitära insatser såväl i fredstid som under krig och väpnade konflikter för att främja människornas välfärd, skapa en positiv inställning till gemensamt ansvar och biståndsarbete bland medborgarna, öka förståelsen för Röda Korsets arbete och allmänt humanitära strävanden samt stärka organisationens beredskap och verksamhetsförutsättningar.

Röda Korsets verksamhet styrs av sju grundläggande principer: humanitet, opartiskhet, neutralitet, självständighet, frivillighet, universalitet och enhet.

2 GRUNDLÄGGANDE RIKTLINJER FÖR DATASKYDD FÖR FINLANDS RÖDA KORS

All verksamhet inom Finlands Röda Kors utgår från att hjälpbehövande, de som deltar i frivilligverksamheten, samarbetspartner och bidragsgivare litar på organisationens arbete. Dataskyddet är mycket viktigt för Finlands Röda Kors och hela organisationen ska förbinda sig till det. Behandlingen av personuppgifter är nödvändig för organisationens verksamhet och behörig behandling viktig för att upprätthålla tillförlitligheten.

Det förutsätts att alla som arbetar och verkar inom organisationen agerar i enlighet med lagstiftningen, värdena och principerna samt är medvetna om sitt eget ansvar för att upprätthålla organisationens tillförlitlighet när behandling av personuppgifter ingår i arbetsuppgifterna.

Med dataskydd avses integritetsskydd vid behandling av personuppgifter. Enligt Finlands grundlag och Europeiska unionens stadga om de grundläggande rättigheterna är integritetsskydd en grundläggande rättighet för alla fysiska personer, och behandling av personuppgifter ska alltid grunda sig på lagen.

Finlands Röda Kors verksamhet innefattar omfattande behandling av personuppgifter om bland annat frivilliga, medlemmar, bidragsgivare, hjälpmottagare, klienter, samarbetspartners samt skolors kontaktpersoner och anställda. Finlands Röda Kors får personuppgifterna i regel av personerna själva när de deltar i verksamheten eller stödjer den. Personuppgifter är upplysningar om en fysisk person (= registrerad) med vilka personen direkt eller indirekt kan identifieras genom att man kombinerar uppgifter. Personuppgifter är till exempel namn, personbeteckning, foto, lokaliseringsuppgift, onlineidentifikatorer eller en eller flera faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med behandling av personuppgifter avses alla åtgärder beträffande personuppgifter, som insamling, registrering, organisering, lagring, bearbetning, sökning, användning, utlämning, spridning, sammanförande, begränsning, radering eller förstöring.

Med personregister avses en datamängd som innehåller personuppgifter och som är tillgänglig enligt särskilda kriterier. Registret kan bestå av flera datalager och en del av uppgifterna kan även vara till exempel i pappersform. Dataskyddet regleras av EU:s allmänna dataskyddsförordning (2016/679, General Data Protection Regulation, GDPR) och Finlands dataskyddslag (1050/2018), lagen om integritetsskydd i arbetslivet (347/2019) samt, alltefter verksamhet, även av speciallagstiftning.

Ett av de centrala kraven i dataskyddslagstiftningen är ansvarsskyldighet, med andra ord ska Finlands Röda Kors kunna visa att personuppgifterna behandlas på ett behörigt sätt och enligt bestämmelserna i lagstiftningen. Dessutom är Finlands Röda Kors skyldigt att informera de registrerade om konfidentialiteten hos deras personuppgifter har äventyrats. Detta förutsätter tillräcklig dokumentering av åtgärderna och de interna processerna i anknytning till behandlingen av personuppgifter.

I dessa riktlinjer beskrivs principerna för dataskydd inom Finlands Röda Kors. Rinktlinjerna för dataskydd gäller all behandling av personuppgifter inom Finlands Röda Kors och för Finlands Röda Kors räkning, oavsett uppgifternas ursprung, innehåll eller användningsändamål. Riktlinjerna för dataskydd är offentliga.

Riktlinjerna för dataskydd kompletteras med mer detaljerade anvisningar om bland annat upprätthållande av personregister, tillgodoseende av de registrerades rättigheter och hantering av dataskyddsavvikelser. De mer detaljerade anvisningarna får dock inte strida mot de principer som beskrivs i riktlinjerna för dataskydd.

En förutsättning för att dataskyddet ska kunna genomföras är tillräcklig datasäkerhet, vars principer beskrivs i Finlands Röda Kors riktlinjer för datasäkerhet.

Genomförandet av och effektiviteten hos riktlinjerna för dataskydd och datasäkerhet utvärderas regelbundet som en del av revisionen av den övriga verksamheten och rapporteras i ett databokslut.

3 FINLANDS RÖDA KORS PRINCIPER FÖR DATASKYDD

- Vi samlar endast in personuppgifter som är nödvändiga för verksamheten.

- Vi behandlar personuppgifterna endast för de ändamål för vilka de har samlats in.
- Vi behandlar personuppgifterna konfidentiellt och omsorgsfullt.
- Vi lagrar inte personuppgifter i onödan.
- Vi är öppna om vår behandling av personuppgifter.
- Vi lämnar inte ut personuppgifter utanför organisationen. Inom organisationen lämnar vi ut uppgifter mellan centralbyrån, distriktsbyråerna, avdelningarna, institutionerna och bolaget för första hjälpen.
- Uppgifter om registrerade i utsatt ställning (till exempel äldre, minderåriga och offer för förföljelse) behandlas med särskild omsorgsfullhet.
- Uppgifterna lämnas ut till myndigheter i situationer där lagen kräver det, exempelvis för att utreda och förhindra missbruk.

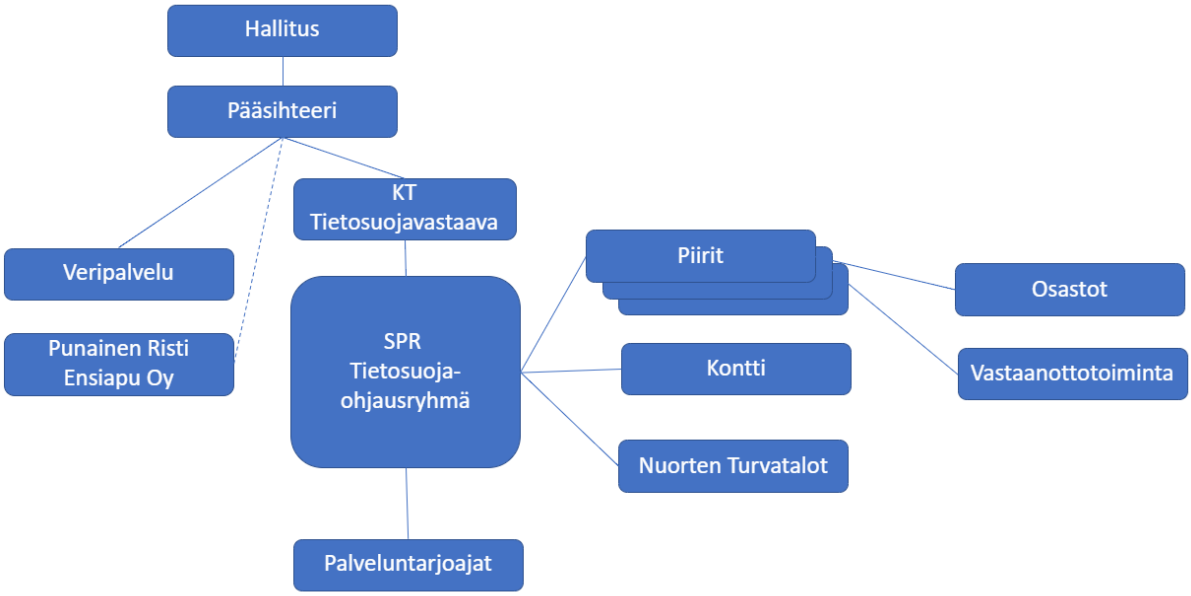
4 PERSONREGISTER

Personuppgifter som behandlas för ett visst användningsändamål bildar ett personregister. Det ska finnas en ansvarig enhet/institution och en kontaktperson för varje personregister. Varje personregisters funktion beskrivs i en sekretesspolicy som ska vara uppdaterad och lätt att förstå. Sekretesspolicyerna är offentliga och finns tillgängliga på Finlands Röda Kors webbplats, med undantag för de sekretesspolicyer som gäller personalen och som finns tillgängliga på intranätet för Finlands Röda Kors anställda.

Den ansvariga personen för varje register ansvarar för registret, tillräcklig och uppdaterad dokumentering av det samt för instruktioner för behandling av uppgifterna i registret för de personer som behöver dem. Den ansvariga personen för registret svarar dessutom för att årligen förstöra onödiga och överflödiga uppgifter i enlighet med lagringstiderna i sekretesspolicyn.

5 DATASKYDDSORGANISATION OCH ANSVAR

Finlands Röda Kors dataskyddsorganisation har följande uppbyggnad:



I regel har Röda Korset rollen som personuppgiftsansvarig i all behandling av personuppgifter. Detta gäller alla personuppgifter om medlemmarna, de frivilliga, hjälpmottagarna, de som utbildas och personalen. Finlands Röda Kors distrikt har rollen som personuppgiftsansvarig vid behandlingen av sina anställdas personuppgifter samt vid annan behandling av personuppgifter för sin egen räkning. Ansvaren för dataskyddet mellan centralbyrån, distrikten och avdelningarna beskrivs i trepartsavtalet som finns i bilagorna.

Blodtjänst och Suomen Punainen Risti Ensiapu Oy är självständiga personuppgiftsansvariga, vars verksamhet, system samt grunder för och skyldigheter i behandlingen av personuppgifter skiljer sig märkbart från Finlands Röda Kors övriga verksamhet. Blodtjänst och Suomen Punainen Risti Ensiapu Oy har separata riktlinjer för dataskydd, praktiska anvisningar och ett dataskyddsombud som stödjer denna riktlinje. Detta har ansetts nödvändigt för att tillräcklig kompetens och ett tillräckligt dataskydd ska kunna garanteras inom hela Finlands Röda Kors organisation.

Dataskyddsombudet inom Finlands Röda Kors

- är expert inom dataskydd
- samordnar dataskyddsgruppens verksamhet
- är kontaktperson till den övervakande myndigheten

- följer upp och övervakar behandlingen av personuppgifter och huruvida den stämmer överens med de uppställda kraven
- rapporterar om dataskyddets status till Finlands Röda Kors ledning enligt i förväg fastställda mätare
- rapporterar om utvecklingsbehov i dataskyddsfrågor till Finlands Röda Kors ledning
- stödjer hela organisationens dataskyddsarbete
- utbildar och ansvarar för utbildningsmaterial och instruktioner
- ansvarar för dataskyddswebbplatser och dokumentering av dataskyddsprocesserna på organisationsnivå
- utreder frågor, fattar inte beslut
- stödjer och utbildar registrens ägare
- ansvarar för utbildningen av och stödet till distriktens och institutionernas kontaktpersoner i dataskyddsfrågor
- ansvarar för upprättandet av databokslutet
- ansvarar för kommunikationen om dataskyddsarbetet inom organisationen
- håller sig uppdaterad, utbildar sig, bildar nätverk
- kommunicerar med Röda Korsets internationella organisation i dataskyddsfrågor.

Finlands Röda Kors dataskyddsgrupp

- bereder det strategiska beslutsfattandet
- har inget operativt ansvar, är ett styrande hjälporgan
- gör prioriteringar på organisationsnivå
- behandlar aktuella frågor som gäller dataskydd, såsom bedömningar av dataskyddets effekter
- utvecklar förfaringssätt och principer som gäller dataskydd
- sammanträder minst två gånger per år
- går igenom databokslutet, skillnader mellan riktlinjerna och det praktiska genomförandet
- behandlar avvikelser
- utvecklingsorienterad
- ansvarar för uppdateringen av riktlinjerna.

Distriktets/institutionens kontaktperson för dataskydd

- ansvarar för dataskyddspraxis inom sitt distrikt/sin institution och för utbildningen av personalen
- distriktets kontaktperson är även den primära kontaktpersonen gentemot asylförläggningarna och avdelningarna samt ansvarar för den praktiska tillämpningen av dataskyddsanvisningarna vid asylförläggningarna och inom distrikten
- upprätthåller distriktets/institutionens dataskyddsdokumentation för de registers del där distriktet/institutionen har rollen som personuppgiftsansvarig eller när behandlingen avviker från den vid centralbyrån
- förstår den personuppgiftsansvariges och personuppgiftsbiträdets ansvar samt förstår när distriktet är personuppgiftsansvarig och när personuppgiftsbiträdet är det

- ansvarar för distriktets/institutionens andel i databokslutet
- förstår dataskyddets roll i verksamhetsrevisionen på avdelningen
- stödjer introduktionen till dataskydd på avdelningen.

Avdelningens kontaktperson för dataskydd

- är kontaktperson till distriktet och centralförvaltningen i dataskyddsfrågor som gäller avdelningen
- ansvarar för dataskyddspraxis i avdelningens verksamhet
- upprätthåller avdelningens dataskyddsdokumentation
- ansvarar för avdelningens interna dataskyddsanvisningar och utbildningar i dataskydd
- förstår den personuppgiftsansvariges och personuppgiftsbiträdets ansvar samt förstår när avdelningen är personuppgiftsansvarig och när personuppgiftsbiträdet är det
- upprätthåller avdelningens dataskyddsdokumentation
- ansvarar för utbildningen i och anvisningarna för dataskydd för avdelningens aktiva medlemmar och frivilliga.

Centralbyråns dataskyddambassadör

- den egna enhetens/linjens stödperson inom dataskydd som påminner om dataskyddspraxis och att den ska beaktas
- insatt i ämnet, intresserad
- deltar i arbetsgruppens möten och är aktiv
- lyfter fram den egna enhetens frågor/utmaningar i arbetsgruppen
- bistår vid upprättandet av databokslutet.

Cheferna ansvarar för att riktlinjerna för dataskydd iakttas inom deras respektive ansvarsområden och att de nödvändiga instruktionerna är tillräckliga och uppdaterade.

Varje anställd följer principerna för dataskyddet och rapporterar om de dataskyddsavvikelser som hen upptäcker till organisationens dataskyddsombud, tietosuoja@redcross.fi.

6 DE REGISTRERADES RÄTTIGHETER

De registrerade har rätt att få information om hur deras personuppgifter behandlas och används. Varje registrerad har rätt att

- få tillgång till sina uppgifter

- begära korrigering av uppgifter
- begära radering av uppgifter
- begära begränsning av behandling
- begära överföring av uppgifter mellan system.

Finlands Röda Kors bedömer alltid från fall till fall innehållet i förfrågningar från registrerade och genomförandet av förfrågningarna. Finlands Röda Kors kan nödvändigtvis inte tillmötesgå de registrerades förfrågningar i alla situationer. De registrerades rättigheter för varje enskilt personregister antecknas i sekretesspolicyn.

Alla förfrågningar om användning av de registrerades rättigheter styrs till dataskyddsombudet på adressen tietosuoja@redcross.fi.

7 ÖVERFÖRINGAR OCH UTLÄMNANDEN AV PERSONUPPGIFTER TILL TREDJE LÄNDER UTANFÖR EU OCH EES

Vid överföringar och utlämnanden av personuppgifter till tredje länder ska särskild noggrannhet iakttas. Vid systematiska överföringar ska man som en förutsättning för systemfunktionerna säkerställa att mottagaren har vidtagit nödvändiga skyddsåtgärder.

Vid enskilda överföringar ska man i första hand försäkra sig om att den registrerade är införstådd med principerna för överföringen och den mottagande aktören samt godkänner överföringen. Uppgifter kan även överföras om det är nödvändigt för att verkställa ett avtal eller skydda personen.

8 INBYGGT DATASKYDD OCH KONSEKVENSBEDÖMNING

Kraven på dataskydd ska beaktas i ett så tidigt skede som möjligt när ändringar i verksamheten, verksamhetssätten eller systemen planeras. När ändringar i behandlingen av personuppgifter och nya behandlingsmetoder planeras ska riskerna för individens rättigheter och friheter alltid bedömas. Om risken bedöms vara stor ska en separat konsekvensbedömning göras, där riskerna till följd av behandlingen bedöms. Vid bedömning av risker är det skäl att även beakta eventuella risker för den offentliga bilden av Finlands Röda Kors och eventuella andra risker för Finlands Röda Kors verksamhet.

9 RADERING, ANONYMISERING OCH PSEUDONYMISERING AV PERSONUPPGIFTER

Personuppgifter ska inte lagras i onödan eller för säkerhets skull. Man fastställer behovet av att lagra personuppgifter separat i varje enskild sekretesspolicy och handlar därefter. Anonymisering av personuppgifter innebär att uppgifterna görs oigenkännliga så att de inte längre kan kopplas till de registrerade. Anonymiserade uppgifter kan inte kopplas till en person och omfattas inte heller av dataskyddsföreskrifterna. Pseudonymisering innebär att personuppgifterna behandlas så att de inte längre kan tillskrivas en specifik registrerad utan att tilläggsuppgifter som upplöser pseudonymiseringen används. Uppgifterna som behövs för att upplösa pseudonymiseringen förvaras separat och skyddas. Pseudonymiserade personuppgifter ska behandlas på det sätt som dataskyddsförordningen och övrig

tillämplig lagstiftning förutsätter. Personuppgifter anonymiseras och pseudonymiseras när det är möjligt med tanke på uppgifternas användningsändamål.

10 DATASKYDDET I AVTAL

Även externa aktörer, såsom underleverantörer, ska följa Röda Korsets dataskyddsprinciper. När avtal ingås och uppdateras ska man se till att dataskyddsperspektiven beaktas i avtalen i tillräcklig grad och på ett entydigt sätt. I synnerhet ska observeras att dataskyddspraxis och anknytande lagstiftning i hög grad varierar utanför Europeiska unionen. Med varje personuppgiftsbiträde ska ett avtal om behandling av uppgifter som dataskyddsförordningen förutsätter upprättas.

11 PERSONUPPGIFTSINCIDENTER

Personuppgiftsincident avser ett dataintrång till följd av vilket överförda, lagrade eller på annat sätt behandlade personuppgifter av misstag eller på ett lagstridigt sätt förstörs, försvinner, förändras, olovligen överlåts eller blir tillgängliga.

Misstänkta eller observerade personuppgiftsincidenter ska omedelbart meddelas till den ansvariga personen för det aktuella registret, den ansvariga personen för verksamheten samt dataskyddsombudet. Dessutom ska nödvändiga motåtgärder vidtas.

Det ges separata och mer detaljerade anvisningar om hur personuppgiftsincidenter behandlas och om nödvändiga meddelanden till de registrerade och tillsynsmyndigheterna.

Bilagor: Organisationens behandling av personuppgifter – trepartsavtal