UNA OY:N TIETOSUOJA- & TIETOTURVAPOLITIIKKA

1. JOHDANTO

Tietosuoja- ja tietoturvapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan UNA Oy:n ja sen alaisten ohjelmien ja tuottamien ICT-palveluiden tietosuojan ja tietoturvan toteuttamisessa ja kehittämisessä.

Tietosuoja ja tietoturvallisuus huomioidaan kaikessa tietojen käsittelyssä jo suunnitteluvaiheessa. UNA Oy:n hallitus tietosuoja- ja tietoturvaturvatoiminnan omistajana määrittelee tässä politiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuoja- ja tietoturvaperiaatteet, vastuut ja tavoitteet. Politiikka toimii perustana UNA Oy:n mahdollisille tietosuojaa ja tietoturvaa koskeville täsmentäville toimintaohjeille, joiden tehtävänä on tarkentaa politiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

UNA Oy:n hallituksen vahvistama tietosuoja- ja tietoturvapolitiikka kattaa UNA Oy:n kaikkeen toimintaan liittyvät tietojen käsittelyn tehtävät. Tietosuoja- ja tietoturvapolitiikka koskee koko organisaatiota ja sen henkilöstöä mukaan lukien ne UNA Oy:n sidosryhmien edustajat, jotka toimeksiantojensa puitteissa käsittelevät UNA Oy:n omistamaa tai hallinnoimaa tietoa. Politiikka kattaa UNA Oy:n omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

2. MÄÄRITELMÄT

Tietosuojalla tarkoitetaan henkilötietojen suojaamista ja rekisteröidyn oikeuksien tehokasta toteuttamista. Lainsäädännön perusteella henkilötietoja suojataan usein tarkemmin kuin organisaation käytössä olevia muita luottamuksellisia tietoja. Tietosuojalainsäädäntö edellyttää, että henkilötietojen käsittely on turvattava ja henkilötiedot on suojattava asiattomalta käsittelyltä. Henkilötietojen oikeellisuus on varmistettava, ne on pidettävä salassa ulkopuolisilta, niitä ei saa tuhota tai käsitellä asiattomasti ja niiden on oltava tarpeen mukaan käytettävissä.

Tietoturva tarkoittaa tietojen käsittelyn turvaamista. Tietoturva koostuu tietoturvaan liittyvistä vastuista ja käytännöistä, joilla pyritään varmistamaan

tietojen, tietojärjestelmien ja palvelujen turvaaminen siten, että niiden luottamuksellisuus, eheys ja saatavuus voidaan taata ja osoittaa toteutuneen. Tietoturvaan kuuluvat tietoturvaorganisaatio, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet

Tietosuojan ja -turvan muilla keskeisillä käsitteillä tarkoitetaan seuraavaa:

- **Eheys** eli tieto on oikeaa ja eheää, eikä muuttunut tahallisen tai tahattoman teknisen tai inhimillisen toiminnan seurauksena.
- **Kiistämättömyys** ilmentää sitä, että tiedon lähettäjä tai vastaanottaja tai tietoon liittyvä tapahtuma voidaan varmistaa luotettavasti myös jälkikäteen.
- **Luottamuksellisuus** eli tieto on vain siihen oikeutettujen saatavilla.
- **Saatavuus** eli tieto on saatavilla aina sitä tarvittaessa.

3. TIETOSUOJAN JA TIETOTURVAN TAVOITTEET JA PERIAATTEET

UNA Oy:n lähtökohtana tietosuojassa on riskilähtöisyys. UNA Oy rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa UNA Oy:n riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.

UNA Oy:n toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

UNA Oy:n tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:
- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää

- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

UNA Oy:n tietoturvatyön päämäärä on turvata UNA Oy:n toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Toimintalähtöisesti painottuvalla tietoturva- ja tietosuoja -asioiden hoidolla tuetaan organisaation toiminnalle asetettuja vaatimuksia. Lisäksi tietojen ja tietojärjestelmien huolellinen käsittely takaa osaltaan rekisteröidyn yksityisyyden suojaa.

Hyväksytyn tietosuoja- ja tietoturvapolitiikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa UNA Oy:n yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

4. TIETOSUOJAN JA TIETOTURVAN ORGANISOINTI JA VASTUUT

Tietosuojaa ja tietoturvaa johtaa ja valvoo **UNA Oy:n hallitus.** Tietosuoja- ja tietoturvapolitiikan hyväksyy ja toimeenpanee UNA Oy:n hallitus ja siitä vastaa UNA Oy:n toimitusjohtaja.

Toimitusjohtaja päättää rekisterinpidon ja tietosuojan kokonaisuudesta antamalla tietosuojaa ja rekisterinpitoa koskevat periaateohjeet sekä nimeämällä tietosuoja- ja tietoturvavastaavat.

UNA Oy:n lakiasiainjohtaja yhdessä johtoryhmän jäsenten kanssa vastaavat tietosuojan ja tietoturvallisuuden operatiivisesta toteuttamisesta.

UNA Oy:n tietosuojavastaava valvoo tietosuojalainsäädännön noudattamista organisaatiossa sekä vastaa neuvonnasta ja kouluttamisesta tietosuoja-asioissa. Tietosuojavastaava raportoi organisaation johdolle tietosuojan toteutumisesta. Tietosuojavastaava raportoi UNA Oy:n hallitukselle ja toimitusjohtajalle viivytyksettä havaitsemistaan tietosuojaan liittyvistä virheistä ja vakavista puutteista. Tietosuojavastaavan asema organisaatiossa on riippumaton.

UNA Oy:n tietoturvavastaava vastaa tietoturvan kehittämisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta UNA Oy:ssä ja sen ostamissa palveluissa. Tietoturvavastaava raportoi organisaation johdolle tietoturvan toteutumisesta. Tietoturvavastaava vastaa myös tietoturva-asioista tiedottamisesta UNA Oy:n ulkopuolelle ja UNA Oy:n sisällä yleisellä tasolla. Tietoturvavastaava raportoi tietoturvaan liittyvistä virheistä ja vakavista puutteista viivytyksettä UNA Oy:n hallitukselle ja toimitusjohtajalle.

UNA Oy:n tietosuoja- ja tietoturvavastaavat voivat perustaa tietosuojatyöryhmän tietosuojan ja tietoturvan kehittämisen suunnittelua ja toimeenpanon valmistelua varten.

Tietoturva- ja tietosuojavastaava antavat tietotilinpäätöksen raporttina UNA Oy:n hallitukselle kerran vuodessa.

Kunkin henkilörekisterin vastuuhenkilön on huolehdittava siitä, että tietosuojalainsäädännön edellyttämät velvoitteet ko. rekisterinpidon osalta tulevat hoidettua.

Henkilöstöhallinnolliset esimiehet vastaavat tietosuoja- ja tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omien alaistensa osalta.

Jokainen UNA Oy:ssä tietoja käsittelevä, tietojärjestelmien ylläpitäjä ja käyttäjä on vastuussa tietoturvan ja tietosuojan toteuttamisesta sekä tietoturva- ja tietosuojaohjeiden noudattamisesta omalta osaltaan. Jokaisella UNA Oy:n työntekijällä on tietosuoja- ja tietoturva-asioihin liittyvä valvontavastuu. Jokainen UNA Oy:n tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä eteenpäin annettujen ohjeiden mukaisesti. Henkilötietojen käsittelyyn ja tietoturvaan liittyvät poikkeamat raportoidaan välittömästi sisäisen ohjeistuksen mukaisesti.

5. TIETOSUOJAN JA TIETOTURVAN TOTEUTTAMINEN

UNA Oy:n tietoturva- ja tietosuoja perustuvat tietoturvaa, tietosuojaa, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin kansallisiin ja kansainvälisiin säädöksiin, velvoitteisiin, määräyksiin ja ohjeisiin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon UNA Oy:n tietoturvan ja -suojan kehittämisessä.

Lainsäädännön lisäksi tulee noudattaa muita UNA Oy:ssä hyväksyttyjä tietoturvaan ja tietosuojaan liittyviä ohjeita ja määräyksiä. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa tämän tietoturvapolitiikan tai organisaation ylemmän tason määräysten kanssa siten, että tietoturva tai tietosuojan taso heikkenee.

Henkilökunnan toimintaa ohjaavat lainsäädännön ja määräysten mukaiset velvollisuudet ja oikeudet sekä työntekijän lojaliteettivelvoite.

5.1. Tietosuojan toteuttaminen

UNA Oy toteuttaa *sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta* ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Näin varmistetaan, että käsittely vastaa tietosuoja-asetuksen vaatimuksia. Tietosuojan toteuttamisessa UNA Oy varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.

UNA Oy toteuttaa *riskilähtöisen toimintaperiaatteen* varmistamiseksi tietosuojan vaikutustenarviointeja sellaisten henkilötietojen käsittelytoimille, joiden suunnitteluvaiheessa on todennäköistä, että käsittelytoimiin liittyy yksilöiden oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa. Samalla varmistetaan tietosuoja-asetuksen vaatimusten toteutuminen.

UNA Oy:n valvontaa täydentää rekisteröidyn mahdollisuus itse valvoa ja määrätä henkilötietojensa käytöstä käyttäen *rekisteröidylle kuuluvia oikeuksiaan*. UNA Oy:ssä on määritetty toimintaprosessi ja ohje liittyen toimintaan rekisteröityjen käyttäessä oikeuttaan saada pääsy henkilötietoihinsa. Prosessin mukaista toimintatapaa noudatetaan niissä tapauksissa, joissa rekisteröidyt haluavat saada nähtäväkseen omia rekistereissä olevia henkilötietojaan.

Kolmannet osapuolet

UNA Oy voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. UNA Oy valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja

organisatoristen toimenpiteiden avulla sekä täyttävät tietosuoja-asetuksen vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta.

Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä. UNA Oy:n ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti. Yhteishankintayksikkönä toimiessaan UNA Oy toimii UNA Oy:n asiakkaiden tietosuoja- ja tietoturvamäärittelyjä kunnioittaen.

5.2. Tietoturvan toteuttaminen

Tietoturvallisuustoiminnan tarkoituksena on suojata data ja tietoaineistot sekä niiden käytettävyys, eheys ja luottamuksellisuus kaikissa olomuodoissa. Toiminnan tietoturvallisuuden kannalta tärkeimmät turvattavat kohteet ovat henkilöt, tilat, laitteet, tietoliikenne, tietojärjestelmät, ohjelmistot, palvelut sekä toiminnan jatkuvuus ja palautettavuus.

Näiden kohteiden turvaamisen tavoitteena on operatiivisten järjestelmien ja sisäisen tietojenkäsittelytoiminnan ja tietosuojan turvaaminen sekä palvelujen tuottaminen normaalioloissa ja normaaliolojen häiriötilanteissa sekä poikkeusoloissa.

Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuus- ja kriittisyysluokitus asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille.

Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määritteleminen tapahtuu säännöllisesti suoritettavilla turvallisuusanalyyseillä.

Toiminnan jatkuvuuden kannalta on tärkeää, että yhtiön hallinto ja palveluntuottajat ovat varautuneet erilaisiin tietoturvaloukkaustilanteisiin, esimerkiksi tunnistamalla kriittiset toiminnot ja palvelut. Toiminnan jatkuvuus turvataan toipumissuunnittelulla, joka sisältää häiriöiden ennalta ehkäisemisen ja mahdollistaa niistä nopean toipumisen. Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla.

Tilanteissa, joissa joudutaan toteuttamaan priorisointia, turvatoimien järjestys on seuraava:

- henkilön hengen tai terveyden turvaaminen
- arkaluonteisen tai muuten erittäin merkittävän tiedon luottamuksellisuuden turvaaminen
- tietojärjestelmien ja rekistereiden eheyden turvaaminen
- käyttö- ja toimintaympäristön käytettävyyden turvaaminen

5.3. Tietojärjestelmien hankinta ja omistaminen

Jokaisella tietojärjestelmällä on omistaja ja pääkäyttäjä. Laajemmilla järjestelmillä voi olla myös erikseen vastuukäyttäjiä. Omistaja on mukana järjestelmien hankintavaiheesta alkaen koko elinkaaren ajan.

Tietojärjestelmien toimintaa ja käyttöä tulee valvoa. Sisäisten tietojärjestelmien tietojen käyttö tulee pääsääntöisesti sallia vain työtehtävien tai niihin rinnastettavien tehtävien hoitamiseen sekä yhteistyökumppaneilla vastaavasti sopimusten ja lupien mukaisten tehtävien hoitamiseen.

Uusien tietojärjestelmien, prosessien sekä tilojen tietoturva- ja tietosuoja-asiat tulee huomioida ja testata hankintavaiheessa. Organisaatiosta tulee aina olla tietoturvan asiantuntijuuden edustus hankintaprosessissa, silloin kun kyseessä on tietotekninen tai tietoverkkoon kytkettävä laite tai järjestelmä.

UNA Oy:n järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan tietosuojaa- ja tietoturvaa koskevat vaatimukset. Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

6. TOIMINTA TIETOTURVA- JA TIETOSUOJAPOIKKEAMATILANTEISSA SEKÄ ILMOITUSVELVOLLISUUS

UNA Oy:ssä on määritetty toimintaprosessi tietoturva- ja tietosuojapoikkeamatilanteisiin. Tietoturva- ja tietosuojapoikkeamat ilmoitetaan, käsitellään ja rekisteröidään toimintaohjeen mukaisesti.

Henkilötietojen tietoturvaloukkauksen sattuessa UNA Oy:llä on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan.

- Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturva-loukkaus on tullut ilmi, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.
- Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, ilmoitetaan rekisteröidylle loukkauksesta ilman aiheetonta viivytystä.

7. RIKKOMUKSET JA SEURAAMUKSET

UNA Oy:n henkilöstön ja järjestelmien käyttäjien toimintaa ohjataan henkilökohtaisella ja riittävällä perehdytyksellä, saatavilla olevilla toimintaohjeilla sekä koulutuksella. Tietojärjestelmien käyttäjiltä edellytetään käyttö- ja salassapitositoumuksen hyväksyminen. Jokainen käyttäjä sitoutuu noudattamaan tietoturva- ja tietosuojaohjeita saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

Tietosuojasitoumuksen ja toimintaohjeiden sekä lainsäädännön vastainen toiminta käsitellään tapauskohtaisesti.

Tietosuojarikkomukset raportoidaan UNA Oy:n toimitusjohtajalle, lakiasiainjohtajalle ja tietosuojavastaavalle.