TIETOSUOJAN JA TIETOTURVAN OMAVALVONTASUUNNITELMA

Pro Lex Oy

Päivitetty 12.3.2025/tt

Hyväksyttävä johtoryhmältä huhtikuu/2025

Sisällys

1. Johdanto

Sosiaali- ja terveyspalvelujen tuottajien on laadittava tietoturvan ja tietosuojan omavalvontasuunnitelma. Omavalvonnan kautta huolehditaan siitä, että tietoturva- ja tietosuojakäytännöt arkaluonteisten asiakas- ja potilastietojen suojaamiseksi ovat asianmukaiset ja tuodaan esille, miten nämä toteutuvat käytännössä. Omavalvontaan sisältyy myös se, että tietojärjestelmien käyttöympäristössä huolehditaan tietoturvasta asianmukaisesti.

Omavalvontasuunnitelmassa viitataan aina kuin mahdollista olemassa oleviin erikseen ylläpidettäviin ohjeisiin ja dokumentteihin. Olennaista on, että suunnitelman linkkien tai tietojen avulla on selvää, mistä dokumentaatio on löydettävissä tai vaatimuksen täyttyminen on todennettavissa. Mikäli muuta valmista dokumentaatiota ei ole olemassa tai saatavissa, on mahdollista kuvata vaadittavat asiakokonaisuudet ja toimintatavat suoraan omavalvontasuunnitelmaan. Pääasiassa kaikki **Pro Lex Oy** tietosuojaan ja tietoturvaan liittyvät dokumentit ovat löydettävissä sähköisesti **Google driven palvelimelta** kohdasta Tietosuoja/-turva/GDPR. Rekisteriselosteet ovat saatavilla julkisesti verkkosivuilta www.prolex.fi

Pro Lex Oy:n käyttämät tietojärjestelmät ovat Accountor työvuoroVelho työvuorosuunnitteluohjelma sekä Fastroin Nappula -asiakastietojärjestelmä.

2. Tietosuojan toteuttaminen tietojärjestelmissä

Tietojärjestelmien hankinta, kehitys ja ylläpito

Tietosuoja ja –turva on huomioitu järjestelmien hankintaprojekteissa, kehitysprojekteissa ja järjestelmäylläpidossa.

Hankintavaiheessa varmistetaan sopimuksellisesti, että järjestelmäntoimittaja sitoutuu tarjoamaan SaaS (Software as a Service) - järjestelmää, joka täyttää voimassa olevien lakien ja asetusten velvoitteet. Järjestelmään toteutetaan vaikuttavuusarviointi, jossa käsitellään mm. järjestelmään tallennettavien tietojen laji, henkilötietojen käsittely ja säilytys järjestelmässä, käyttö- ja pääsyoikeuksien hallinta, tiedonsiirron suojaustapa, palomuuripolitiikka, tapahtumien jäljitettävyys, tekninen toimintaympäristö sekä sen valvonta ja ylläpito. Pääsynhallinnan osalta sovelletaan keskitettyä pääsynhallintaa, mikäli se järjestelmän osalta on mahdollista. Lisäksi on määritelty erillisiä sisäisiä prosesseja käyttö- ja pääsyoikeuksien hallintaa ja ylläpitoa varten.

Kaikilla käyttöjärjestelmillä on nimetyt vastuuhenkilöt/pääkäyttäjät, jotka huolehtivat siitä, että järjestelmässä olevat tiedot suojataan riittävällä tasolla. Ylläpito voidaan hoitaa sisäisesti tai ulkoisen toimittajan avulla. Ohjelmistojen asennus kuuluu ylläpidon tehtäviin.

Pro Lex Oy:n tietojärjestelmien käyttö on sallittua ainoastaan käyttäjän toimesta tämän omilla henkilökohtaisilla käyttäjätunnuksilla. Käyttäjätunnusten jakaminen ulkopuolisille on kiellettyä. Myös kaikenlainen yhteiskäyttö henkilöiden kanssa, joilla on itsellä pääsy ko. järjestelmään, on kielletty.

Käyttäjien pääsynhallinta

Järjestelmissä käytetään henkilökohtaisia tunnuksia ja yksilöllisiä salasanoja. Käyttäjähallintaa toteutetaan keskitetyllä käyttäjähallinnalla. Tämän lisäksi on määritelty prosesseja, joilla ylläpidetään ja tarkkaillaan

järjestelmien käyttö- ja pääsyoikeuksia.

Henkilötietojen suojaaminen tietojärjestelmissä

Jokaisessa järjestelmässä on järjestelmäkohtainen varmuuskopiointikäytäntönsä. Järjestelmille on asetettu omat vaatimuksensa järjestelmän suojaamisen osalta.

Järjestelmien suojaus on toteutettu parhaiden käytäntöjen mukaisesti.

3. Omaisuuden ja tiedon hallinta

Suojausten hallinta

Päätelaitteiden virustentorjunta ja palomuurit ovat päällä ja verkkoliikenteessä käytetään oletuksena VPN-yhteyttä.

Päivitysten hallinta

Päätelaitteiden ohjelmistojen päivitykset ovat aina ajan tasalla. Päivitykset hoidetaan oman henkilökunnan tai ulkoisen palveluntarjoajan toimesta.

Fyysiset tilat ja asiakirjojen säilyttäminen

Yksiköt ja toimipaikat muodostavat pisteen, joissa paperille tulostettu, usein luottamuksellinen ja asiakassuhteen hoitoon tarvittava dokumentaatio säilytetään ja joissa usein liikkuu muitakin, kuin konsernin omaa henkilöstöä.

Tämä aiheuttaa sen, että aineiston säilytykseen ja tiloissa liikkumiseen kiinnitetään huomioita ja estetään luottamuksellisen tiedon pääsy ulkopuolisten henkilöiden käsiin.

Henkilötietoa sisältävien asiakirjojen säilyttäminen on sallittua vain asianmukaisesti suojatuissa tiloissa, lukituissa kaapeissa, jotka sijaitsevat lukituissa toimistotiloissa.

Tilaturvallisuudesta huolehtiminen

Pro Lex Oy:n toimipisteiden tilat, joissa säilytetään henkilötietoa sisältäviä asiakirjoja, pidetään lukittuina. Lukitus on järjestetty siten, että tiloihin eivät pääse ne, joilla ei ole sinne oikeutta. Työntekijät on velvoitettu huolehtimaan siitä, ettei toimipisteissä vierailevat henkilöt pääse näkemään mitään arkaluonteista materiaalia.

Toimipisteissä on määritellyt tilat, joita käytetään arkistotilana tai joissa säilytetään arkistomateriaalia (mm. lukittavat arkistokaapit).
Toimisto- ja arkistotiloihin on rajattu pääsy. Erillisiin arkistotiloihin pääsee vain henkilöstö, ei koskaan ulkopuoliset henkilöt.

Erilliset arkistotilat pidetään lukittuina ja mahdolliset erillisen arkistotilan avaimet säilytetään huolellisesti

ja poissa näkyviltä. Tila, jossa säilytetään arkistokaappia tai jossa arkistotila on, on erillisen lukituksen takana. Tarvittaessa hyödynnetään ns. turvallisuusvyöhykeperiaatetta: kriittisimpiin tiloihin on toteutettu ratkaisuja, kuten kulunvalvonta tai murtohälyttimet.

Tietovälineet, joilla henkilötietoja käsitellään

Pro Lex Oy:n koko henkilöstö on ohjeistettu ja velvoitettu noudattamaan huolellisuutta päätelaitteiden fyysisessä suojauksessa.

Päätelaitteet säilytetään ja kuljetetaan erityistä varovaisuutta noudattaen. Päätelaitteita ei jätetä lukitsemattomiin tai valvomattomiin tiloihin. Päätelaitetta ei saa jättää autoon näkyville. Päälaitetta ei käytetä muuhun kuin työnantajan ohjeistamaan toimintaan työvuoron aikana.

Tarpeetonta asiakirjojen ja paperien tulostamista, säilyttämistä ja arkistointia vältetään.

Toimipisteissä käytetään luottamuksellisen aineiston kierrättämiseen tarkoitettuja lukollisia tietoturvasäiliöitä. Kaikki luottamuksellinen aineisto kerätään ainoastaan lukittuun tietoturvasäiliöön tai tuhotaan ilman välivarastointia/välittömästi paperisilppurilla. Luottamuksellista aineistoa ei koskaan hävitetä keräämällä niitä paperikoreihin, paperi- tai lehtikeräyslaatikkoon.
Käytöstä poistetut tietovälineet hävitetään turvallisesti ja dokumentoidusti.

4. Toimittajien ja sopimusten hallinta

Tietoturva- ja tietosuojavaatimusten määrittely sopimuksen/hankinnan kohteelle ja alihankkijoille
Rekisterinpitäjä on ulkoistanut valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Tietosuoja-asetus selkiyttää rekisterinpitäjän ja käsittelijän välistä sääntelyä sekä on osoittanut velvollisuuksia myös suoraan käsittelijälle.

Rekisterinpitäjän velvollisuuksiin kuuluu valita vain sellaisia henkilötietojen käsittelijöitä, jotka:
- noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen

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

Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksissa on määritelty henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sovittu käsiteltävät henkilötiedot. Lisäksi sopimuksissa on varmistettu, että henkilötietojen käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti. Tämä pitää sisällään myös henkilötietojen käsittelyyn liittyvät sallitut tietojen siirrot ja sijainnit.

Tietoturvan ja tietosuojan hallinnan menettelyt

- velvollisuus noudattaa salassapitovelvollisuutta
- tietosuojapolitiikka, tietosuojaorganisaatio, -roolit ja –vastuut, tietosuojaselosteet, rekisterien tietovirta/vuokuvaukset
- kuvaukset rekisteröityjen oikeuksien takaamiseksi määritellyistä prosesseista
- tehdyt tietosuojan riski- ja vaikutustenarvioinnit hallintakeinoineen
- tietosuojaa ja tietoturvaa käsittelevien foorumeiden ja ohjausryhmien pöytäkirjat
- riskirekisterit ja kirjanpito riskien hyväksymisestä ja omistajuudesta
- tietoturvatestauksen tulokset
- kuvaukset prosesseista, joilla taataan sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen
- henkilötietoja käsittelevälle henkilöstölle suunnattavat ohjeet
- dokumentaatio mahdollisista henkilötietojen käsittelyssä tapahtuneista loukkauksista
- tietotilinpäätös (keinona toteuttaa osoitusvelvollisuus)
- ei ulkoista henkilötietojen käsittelyn tehtäviä ilman rekisterinpitäjän kirjallista ennakkosuostumusta
- auttaa rekisterinpitäjää rekisteröidyn oikeuksien toteuttamisessa
- auttaa rekisterinpitäjää käsittelyn tietoturvallisuuden toteuttamisessa, henkilötietojen tietoturvaloukkausten havaitsemisessa ja niistä ilmoittamisessa sekä vahinkojen minimoinnissa, vaikutustenarviointien tekemisessä ja valvontaviranomaisen ennakkokuulemisessa tietosuojaasetuksen mukaisesti
- joko poistaa tai palauttaa henkilötiedot rekisterinpitäjälle käsittelypalvelujen päättyessä.
- sallii rekisterinpitäjän suorittaa auditoinnit ja osallistuu niihin itse
- työasemien viruksilta ja haittaohjelmilta suojautuminen, valvonta ja seuranta

Henkilötietojen käsittelijän tulee myös saattaa rekisterinpitäjän saataville kaikki sellaiset tiedot, jotka ovat tarpeen asetuksen velvollisuuksien noudattamisen osoittamista varten. Lisäksi on syytä erikseen miettiä

ja sopia eli ilmoittaa rekisterinpitäjälle, mikäli sen ohjeistus rikkoo asetuksen säännöksiä.

Lisäksi organisaatio sitoutuu siihen, että henkilötietojen käsittelyä suorittavat vain sellaiset henkilöt, jotka ovat saaneet hyväksyttävän tuloksen turvallisuusselvityksessä, jos rekisterinpitäjällä on lainmukainen oikeus teettää turvallisuusselvityksiä ja jos rekisterinpitäjä selvitysten teettämistä käsittelijältä vaatii.

Edellä esitettyjen sopimusvaatimusten ohella organisaatiossa on määritelty, miten henkilötietojen käsittelijän palvelun laatua seurataan. Tietosuojan vuosikellossa on määritelty tietosuojan ja tietoturvan säännöllisen raportoinnin käytännöt ja tarvittaessa sekä pyydettäessä järjestetään säännöllinen rekisterinpitäjän ja käsittelijän välinen palaveri, jossa seurataan tietosuojan ja tietoturvan toteutumista henkilötietojen käsittelyssä. Rekisterinpitäjän tulee pitää kirjaa kaikista henkilötietojen käsittelytoimista. Tähän velvollisuuteen kuuluu olennaisena osana tieto kaikista henkilötietojen käsittelijöistä, joille käsittelytoimia on ulkoistettu sekä inventaario kyseisten käsittelijöiden kanssa tehdyistä sopimuksista. Sopimusvaatimuksia tulee hallita ja tarvittaessa tehdä niihin tarkennuksia tai muutoksia esimerkiksi henkilötietojen käsittelyn riskiarvion muuttuessa.

Tietoturvaraportointi

Pro Lex Oy:n yksiköiden vastuuhenkilöt raportoivat säännöllisesti

tietoturvaan liittyvistä asioista toimitusjohtaja ja tietosuojavastaava Tapani Turpeiselle.

Tietoturvapoikkeamien hallinta

Tietoturvapoikkeamien hallinnassa varaudutaan ja ennakoidaan häiriötilanteita, turvataan toiminnan jatkuvuus minimoimalla häiriötilanteiden aiheuttamat vahingot ja pyritään estämään häiriötilanteiden muodostuminen jatkossa (https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf).

Havainnointikyky koostuu teknisten kontrollien lisäksi myös henkilöstön ja sidosryhmien havainnoista.

Tietoturvapoikkeaman hallintaprosessi on jaettu Suomen Valtionvarainministeriön Tietoturvapoikkeamatilanteiden Hallinta-ohjeen mukaisesti neljään päävaiheeseen:

1. tietoturvapoikkeamien käsittelykyvyn muodostaminen

- Riittävä dokumentointi

- Päätöksenteko

- riippuvuuksien tunnistaminen

- henkilöstöresurssien ylläpito

- tilannekuvan ylläpito

- tiedon jakaminen yrityksen sisällä

- haittaohjelmien ja poikkeavan toiminnan havainnointi ja havainnointikyvyn kehittäminen

- sopimusmenettelyt

- harjoittelu

2. tietoturvapoikkeaman havaitseminen ja analysointi

- Normaalista poikkeavan toiminnan havaitsemisen jälkeen analysointi, minkä tavoitteena on selvittää, mitä on tapahtunut ja miksi. Tuloksena voidaan todeta, onko kyseessä tietoturvapoikkeama.

- Työtekijöitä kannustetaan ja koulutetaan havaitsemaan mahdollisia poikkeamia ja ilmoittamaan niistä Työnantajalle.

- Työnantaja käsittelee kaikki havainnot

3. tietoturvapoikkeamaan reagointi

- Toimenpiteet vastuutetaan ja aikataulutetaan, jotta minimoidaan mahdolliset vahingot. Poikkeamista informoidaan muita viranomaisia ja sidosryhmiä sekä käynnistetään toimenpiteet poikkeaman korjaamiseksi.

4. tietoturvapoikkeamasta toipuminen eli paluu normaaliin toimintaan

- Toipumisvaiheessa palataan normaalitilaan, poikkeamasta laaditaan raportti, jonka havaintojen perusteella kehitetään toimintoja, kehitetään käsittelykykyä ja varautumista, jotta poikkeaman toistuminen voidaan jatkossa estää.

5. Toiminnan jatkuvuuden hallinta (Tarvittavat suunnitelmat epäsuotuisiin tilanteisiin ja niistä toipumiseen, jotta voidaan taata henkilötietojen saatavuus esimerkiksi teknisen vian sattuessa)

Tietojen luottamuksellisuus

Tarkemmat kuvaukset on määritelty kunkin järjestelmän osalta järjestelmäkohtaisessa tietosuojaa koskevassa vaikutusten arvioinnissa (DPIA:ssa).

Tietojen eheys, muuttumattomuus

Tarkemmat kuvaukset on määritelty kunkin järjestelmän osalta järjestelmäkohtaisessa tietosuojaa koskevassa vaikutusten arvioinnissa (DPIA:ssa).

Tietojen saatavuus

Tarkemmat kuvaukset on määritelty kunkin järjestelmän osalta järjestelmäkohtaisessa tietosuojaa koskevassa vaikutusten arvioinnissa (DPIA:ssa).

ICT –toipumissuunnitelma

Palautussuunnitelmat on luotu järjestelmäkohtaisesti.

6. Käsittelyn valvonta ja seuranta, lokitietojen auditointi

Järjestelmistä kerätään lokitietoja järjestelmän mahdollistamalla tavalla. Tarkemmat kuvaukset on määritelty kunkin järjestelmän osalta järjestelmäkohtaisessa tietosuojaa koskevassa vaikutusten arvioinnissa (DPIA:ssa).

Tietojen käsittelyn seuranta- ja valvontatehtävät ovat selkeästi vastuutettu ja riittävästi resursoidut.

Mikäli työntekijä käsittelee ilman asiakkaan tai potilaan suostumusta tai ilman lainsäädännön tuomaa oikeutta asiakkaan tietoja, kyseessä on tietosuojarikkomus tai tietosuojarikos, joista voi seurata rangaistus. Vaikka teko ei täyttäisikään tietosuojarikkomuksen tai - rikoksen tunnusmerkistöä, voi seurauksena tietosuojasäännösten rikkomisesta olla palvelussuhteeseen liittyviä kurinpitotoimenpiteitä. Rekisterinpitäjä on velvollinen korvaamaan vahingon, joka on aiheutunut henkilötietolain vastaisesta henkilötietojen käsittelystä.

Seurantaa on mahdollisuuksien mukaan hyvä suorittaa automatisoidusti, sillä lokia muodostuu tyypillisesti hyvin paljon.

7. Tietoturva-organisaation määrittäminen, roolit ja vastuut sisältäen henkilöstölle määriteltävät tietoturvavastuut

Pro Lex Oy:n johto on keskeisessä asemassa tietoturvallisuuden ylläpitämisessä ja kehittämisessä. Johto huolehtii siitä, että tietoturva on organisoitu ja vastuutettu erityisesti riskienhallintatoimissa, tietohallintatoimissa, sopimus- ja hankintatoimissa sekä lainmukaisuuden valvonnassa.

Pro Lex Oy:ssa tietoturvatyön vastuuhenkilönä, tietoturvavastaavana, toimii tietosuoja-asetuksen mukainen tietosuojavastaava (DPO), jolle on osoitettu riittävät resurssit hoitaa ja toteuttaa organisaation tietoturvavelvoitteita organisaation toimintaympäristön ja ulkoisten vaatimusten edellyttämällä tavalla. Tietosuojavastaavana toimii organisaation **tietohallintopäällikkö Taneli Turpeinen**. Tietosuojavastaavan lisäksi **Pro Lex Oy**:n johtoryhmä toimii myös tietosuojatiiminä, joka käsittelee säännöllisesti kaikki konsernissa esille tulevat tietosuojaan liittyvät asiat mukaan lukien tietosuojapoikkeamat ja tietosuojarikkomukset.

Tietoturvavastaavan vastuulle kuuluu huolehtia siitä, että **Pro Lex Oy**:ssä on ajantasainen tietoturvapolitiikka ja, että sitä myös noudatetaan päivittäisessä liiketoiminnassa.

Tietoturvavastaavan ja Tietosuojatiimin tehtävät:

- Tietoturvahallinnointi
- Tietoturvapolitiikan rakentaminen ja kehittäminen
- Tietoturvakoulutuksen ja osaamisen kehittäminen sekä kouluttaminen
- Huolehtiminen siitä, että henkilöstö on perehtynyt tietoturvapolitiikkojen sekä ohjeistusten sisältöön ja sitoutuu noudattamaan niitä.
- Toimiminen viestintäkanavana johdon ja henkilökunnan välillä
- Tiedottaminen poikkeamatilanteista kolmansille osapuolille - esimerkiksi viranomaiset, lehdistö ja

rekisteröidyt asiakkaat

Kaikki, **Pro Lex Oy**:n henkilöstö sekä ulkoiset yhteistyötahot, jotka käyttävät tai joilla on pääsy **Pro Lex Oy**:n materiaaleihin sekä tietojärjestelmiin, joita **Pro Lex Oy** toiminnassaan hyödyntää ovat velvollisia noudattamaan **Pro Lex Oy**:n tietoturvapolitiikkoja ja ohjeita. Jokainen työntekijä on vastuullinen käsittelemään tietoja ja materiaaleja niiden arkaluonteisuuden mukaisesti. He ovat vastuullisia myös raportoimaan välittömästi **Pro Lex Oy**:n johtoryhmälle kaikki havaitsemansa luottamuksellisen tiedon ja järjestelmien väärinkäytökset, tietoturvaheikkoudet tai mahdolliset tietoonsa tulleet yrityksen toimintaa koskevat uhat.

Kaikkien niiden tahojen, jotka luovat tai pitävät omistuksessaan **Pro Lex Oy**:n hyödyntämiä tietoja tai tietojärjestelmiä, vastuulla on huolehtia omien tietojärjestelmiensä turvallisuudesta sekä suojata teknisten ja käytännön ratkaisujen avulla tietojen luotettavuus.

8. Tietoturvan ja tietosuojan säännöllinen mittaaminen, todentaminen ja kehittäminen

Pro Lex Oy:n omistamille työasemille on asennettu haittaohjelmasuojaus-ohjelmisto, joka huolehtii myös ohjelmien päivitysten pitämisestä ajan tasalla. Tekninen testaus henkilötietoa sisältävien järjestelmien osalta tehdään yhteistyössä ko. järjestelmiä tuottavien palveluntuottajien kanssa.

Tietojen käsittelyyn liittyviä säännöllisesti tehtäviä prosesseja auditoidaan vuosittain tietosuojan vuosikellon mukaisesti.

Tietosuojaa todennetaan ylläpitämällä tilastoa tietosuojapoikkeamien ja tietosuojaloukkausten lukumäärästä ja näihin liittyvistä muista tiedoista tapauskohtaisesti:

- tietosuojailmoitusten (viranomaiselle/rekisterinpitäjälle) lukumäärät (kpl)

- tietosuojapoikkeamien lukumäärät (kpl)

9. Viranomaisyhteistyö

Rekisterinpitäjällä on velvollisuus tehdä yhteistyötä valvontaviranomaisen kanssa valvontaviranomaisen niin pyytäessä. Yhteistyö kuuluu nimitetyn tietosuojavastaavan vastuulle.

Rekisterinpitäjällä on myös ilmoitusvelvollisuus valvontaviranomaiselle henkilötietojen tietoturvaloukkaustilanteissa.

10. Tietosuoja- ja tietoturvapolitiikat, ohjeet

Ohjeiden päivittäminen toteutetaan vuosittain tietosuojan vuosikellon mukaisesti. Kaikki ohjeistukset tietoturva-asioihin liittyen löytyvät yksiköiden toimistoista.

11. Henkilöstön tietoturvatietoisuuden ja osaamisen varmistaminen

Pyritään varmistamaan alla mainituin keinoin:

- Henkilöstön sitoutuminen noudattamaan voimassa olevia tietosuoja- ja tietoturvapolitiikkaan, tämä todennetaan henkilöstöhallintojärjestelmässä olevan sitoutumismerkinnän avulla
- Koulutusmateriaalin ajantasaisuuden ylläpitäminen
- Koulutussuunnitelmien, perehdyttämismateriaalien ja –suunnitelmien ylläpitäminen ja päivittäminen
- Julkaisu- ja viestintätapojen ohjeistus, konsernin virallisten viestintäkanavien hyödyntäminen
- Vaitiolovelvollisuus ja salassapitosopimukset
- Järjestelmien käyttöohjeiden hallinnointi ja saatavuus

12. Henkilötietoihin kohdistuvien tietoturvaloukkausten hallinta

Pro Lex Oy:llä on voimassa oleva ohjeistus poikkeustilanteiden varalle. Henkilöstöä on koulutettu sekä ohjeistettu tunnistamaan yrityksen tietoturvaa uhkaavat tilanteet. Ohjeistus on luettavissa toimipisteiden toimistoissa.

Henkilöstö on velvoitettu välittömästi ilmoittamaan tietosuojaan liittyvien riskitilanteiden kaltaisista tapahtumat tietosuojavastaavalle mahdollisten lisävahinkojen välttämiseksi. Tietoturvaloukkausten osalta noudatetaan konsernissa laadittuja tietosuoja- tai tietoturvatoimintaohjeita poikkeamatilanteissa. Lisäksi lainsäädäntöä ja sen myötä tulevia muutostarpeita ohjeeseen seurataan. Ohje tarkistetaan 1krt/kalenterivuosi.