LAPIN LIITTO

LAPIN LIITON JA LAPIN PELASTUSLAITOKSEN TIETOTILINPÄÄTÖS 2022

***Aikataulutus**: kerran vuodessa , muulloin pyydettäessä.*

***Tarkoitus**: Osoitusvelvollisuuden toteennäyttäminen, luottamuksen osoittamista sidosryhmiin nähden, johdon työväline tai sisäisen valvonnan työkalu.*

Päiväys ja laatija: 08.03.2023 Paulus Lohi , Tietosuojavastaava , Lapinliitto ja Lapin pelastuslaitos

SISÄLLYSLUETTELO

TIIVISTELMÄ VUODEN 2022 TAPAHTUMISTA

Lapin liiton ja Lapin Pelastuslaitoksen vuosi tietosuojan ja tietojärjestelmien tietoturvan osalta ollut hyvin rauhallinen. Tietopyyntöjä ei ole tullut ainoatakaan. Muutamia tietoturva/tietokalastelu viestejä on tullut . Ne on selvitetty yhdessä Lapit Oy (järjestelmien ylläpitäjä) kanssa ja kaikki ovat osoittautuneet vain epäilyiksi huijaus yrityksiksi ja niihin ei ole ohjeistuksen mukaan tarvinnut reagoida. Olemme eläneet Lapin liiton ja Lapin Pelastuslaitoksen viimeistä yhteistä vuotta. Vuosi 2023 tuo tulleessaan muutoksia. Lapin liitto jää omaksi toimijaksi ja Lapin pelastuslaitos siirtyy osaksi Lapin Hyvinvointialuetta. Nyt kun organisaatiot eroavat, toiminta tietosuojan ja tietoturvan kehittämiseksi on helpompaa ja selkeämpää.

1. JOHDANTO

Tietotilinpäätös tarjoaa ajantasaisen **tilannekuvan** organisaation henkilötietojen käsittelyn nykytilasta sekä arvion tietosuojan toteutumisesta. Tietotilinpäätöksessä kartoitetaan henkilötietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuojatyön tekemistä ja lisätä tekemisen vaikuttavuutta. Tietotilinpäätös toimii myös yhtenä **osoitusvelvollisuuden** osoittamisen välineenä **ja sisäisen ja ulkoisen valvonnan raporttina**. Osoitusvelvollisuuteen kuuluu mm. se, että organisaation **sopimuksissa ja alihankinnoissa** on huomioitu tietosuojan ja -turvan vaatimukset. Lisäksi rekisterinpitäjä tulee huomioida rekisteröidyn henkilötietojen käsittelyyn kohdistuvat **riskit.** Rekisterinpitäjän tulee huolehtia siitä, että henkilöstöllä ja ulkopuolisilla henkilötietojen käsittelijöillä on tarvittava **ohjeistus ja osaaminen**.

Rekisterinpitäjän tulee myös **seurata, raportoida ja valvoa** tietosuojaan ja -turvaan liittyviä asioita ja huolehtia siitä, että tietosuojaan koskeva sääntely toteutuu organisaatiolla. Osoitusvelvollisuuteen kuuluu myös **sisäänrakennetun tietosuojan** vaatimus, millä tarkoitetaan sitä, että tietosuojaperiaatteet toteutuvat kaikissa käsittelyn vaiheissa. Tietosuojaperiaatteet (5 art.) ovat 1. lainmukaisuuden, kohtuullisen ja läpinäkyvyyden periaate, 2. käyttötarkoitussidonnaisuuden periaate, 3. tietojen minimoinnin periaate 4. täsmällisyyden periaate, 5. säilytyksen rajoittamisen periaate ja 6. eheyden ja luottamuksellisuuden periaate.

Tietotilinpäätöksellä voidaan lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita ja käsitellään henkilötietoja sen mukaisesti. Hyvin hoidetulla tietosuojatyöllä vaikutetaan organisaation tehokkuuteen ja kilpailukykyyn. Tietosuojasääntely koostuu tietosuoja-asetuksesta, kansallisesta tietosuojalaista sekä erityislainsäädännöstä. Suomessa tietosuojavaltuutetun toimisto valvoo tietosuojalainsäädännön noudattamista.

LAPIN LIITON JA LAPIN PELASTUSLAITOKSEN henkilötietojen käsittelyä ja tietoturvaa on ohjeistettu henkilökunnalle erilaisin ohjein. Ohjeet löytyvät Sharepointista. Vuonna 2019 on tehty Tietoturva- ja tietosuoja käsikirja, lisäksi on useita muita ohjeita, joissa on käytännön ohjeita tietoturvaan ja tietosuojaan liittyen. Tietotilinpäätös tehdään ensimmäisen kerran vuodesta 2022 ja jatkossa se tehdään vuosittain. Tietotilinpäätös on lähtökohtaisesti julkinen ja voidaan julkaista johdon määrittelemän ohjeistuksen mukaan. Sen laatii tietosuojavastaava. Tilinpäätöksen sisältöä pyritään joka vuosi kehittämään ja laajentamaan. Jatkossa pyritään myös lisäämään tilastoja eri vuosilta, jotta tietosuojan ja tietoturvan osalta tapahtumien määriä/vuosi voidaan seurata ja vertailla.

2. TIETOSUOJAN JA TIETOTURVALLISUUDEN TOTEUTTAMINEN

Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä on vastuussa siitä, että se toteuttaa tarvittavat **tekniset ja organisatoriset toimenpiteet**, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Rekisterinpitäjän on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudelta vaihtelevat riskit ja suhteuttava toimenpiteet näiden mukaisesti. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tila- ja käytönvalvontaa, pääsynhallinta, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytännesääntöjen sekä sertifikaattien käyttöä. Tässä kappaleessa annetaan kuva siitä, miten tiedon eheys, saatavuus ja luottamuksellisuus taataan sekä myös tiedon läpinäkyvyys (5 art.).

Lapin liiton ja Lapin pelastuslaitoksen käyttämät tietokoneet ja järjestelmät tulevat IT-sopimuskumppanin kautta. (Lapit Oy)

He vastaavat myös koneiden ja ohjelmistojen tietosuojasta ja tietoturvasta yhdessä organisaatiomme ylimmän johdon kanssa.

Lapin Liitolla ja Lapin pelastuslaitoksella on yhteinen **tietosuojavastaava.** Vuoden 2023 alusta lähtien organisaatiot eriävät toisistaan ja jatkavat omilla tietosuojavastaavilla. Tietosuojavastaavan tehtävä on valvoa, että organisaatioiden tietoturva- ja tietosuoja-asiat hoidetaan lain vaatimalla tavalla ja kehittää ja kouluttaa henkilöstön osaamista näiden a osalta. Näiden asioiden hoitamisen vastuu lain vaatimusten mukaisesti on kuitenkin organisaatioiden johdolla(Lapin liitto ja Lapin pelastuslaitos), ei tietosuojavastaavalla

Lapin pelastuslaitos tekee suppean turvallisuusselvityksen henkilöstä hänen aloittaessa työt organisaatiossa. Kulunvalvontajärjestelmää rakennetaan parhaillaan eri toimipaikoille, sillä koko maan kattava Tuve (Turvallisuusverkko) otetaan pian käyttöön.

Lapin pelastuslaitoksella on olemassa etätyön tietoturva ohjeistus. Lisäksi on tehty ohje tietosuojaloukkauksen varalta (tietokone, massamuisti, puhelin jne. katoaa). Ohjeet löytyvät Sharepointista.

3. TIEDONHALLINTA, TIETOVARANNOT JA TIETOVIRRAT

Organisaation tulee suunnitella ja kuvata tiedonhallinnan, tietovarantojen ja tietovirtojen kokonaistilanteensa. Tämä tapahtuu esimerkiksi **kokonaisarkkitehtuurin, tietojärjestelmäarkkitehtuurin, tietovarantokuvausten, tiedonohjaussuunnitelmien ja erilaisten prosessikuvausten** avulla. Tarkoituksena on selventää sitä, miten tietoa hallintaa sen koko **elinkaaren** ajan, tiedon vireille tulosta hävittämiseen tai arkistointiin saakka. Lisäksi kuvaukset toimivat ja toteuttavat julkisuusperiaatetta sekä toimivat omien tietojen pyyntöön liittyvinä apuvälineitä. Tiedonohjaussuunnitelmilla voidaan todentaa esimerkiksi sitä, että tietojen säilytysajat on määritelty asianmukaisesti ja että niiden hävittäminen on suunnitelmallista. Tietovarantoja ja tietojenkäsittelyä saatetaan hoitaa myös organisaation ulkopuolella, esim. palkanlaskenta. Organisaatiolla on olemassa ohjeistus ja sopimukset näihin ulkoisiin tietojenkäsittelytilanteisiin. Organisaatio voi myös käsitellä tietoja käyttäen omia palvelinsalejaan tai ulkoisista pilvipalveluista.

Organisaatio voi johtaa tiedolla ja hyödyntää omaa tietopääomaansa vain, jos johdolla on tarpeeksi tietoa muun muassa omasta toiminnasta, toimintaympäristöstään, prosessien toimivuudesta, henkilökunnan osaamisesta, tietovirroista ja tietovarannoista. Tässä luvussa kuvataan muun muassa sitä, miten organisaatio toteuttaa tietosuojaperiaatteina tietojen minimointia, käyttötarkoitussidonnaisuutta ja säilytyksen rajoittamista ja tiedon läpinäkyvyyttä.

Lapin liitto ja Lapin pelastuslaitos ylläpitävät eri **henkilörekistereitä**. Nämä ovat omien lakisääteisten toimintojemme kannaltamme välttämättömiä.

Lakiperusteet. EU:n yleisen tietosuoja-asetuksen 6 artiklan

1c kohta: Käsittely on tarpeen rekisterinpitäjän lakisääteisten velvoitteiden noudattamiseksi.

1e kohta: Käsittely on tarpeen rekisterinkäyttäjälle kuuluvan julkisen vallan käyttämiseksi.

Tietoja voidaan käyttää myös rekisterinpitäjän oman toiminnan suunnittelu-, kehittämis- ja tilastointitarpeisiin

Lapin liiton ja Lapin pelastuslaitoksen ylläpitämät rekisterit voivat sisältää tietoja henkilöistä, yrityksistä tai yhdistyksistä. Rekistereissä on mm. seuraavia tietoja:

Henkilötiedot: henkilötunnus, nimi, osoite, puhelinnumero, sähköpostiosoite, kiinteistötunnus, kuva ja auton rekisteritunnus.

Yrityksen- tai yhdistyksen tiedot: Y-tunnus, nimi, osoite, puhelinnumero, sähköpostisoite, yhteishenkilön nimi ja sähköpostiosoite, kiinteistötunnus. Rekisteriin kirjatut tiedot ovat salassa pidettäviä.

Lapin pelastuslaitos saa tietoja ilmoittajan itsensä antamana, Hätäkeskuslaitokselta, Liikenne-ja viestintävirasto Traficomilta, Digi- ja väestövirastolta sekä muilta viranomaisilta. Rekisterinpitäjä ei luovuta rekisteriin kirjattuja henkilötietoja ulkopuolisille. Tietoja voidaan luovuttaa vain, jos rekisterinpitäjällä on velvollisuus lain, viranomaismääräysten tai muun pakottavan syyn vuoksi. Mikäli rekisteröidyn tietojen luovuttaminen Lapin pelastuslaitoksen ulkopuolelle on muutoin tarpeellista, tietoja voidaan luovuttaa vain rekisteröidyn nimenomaisella suostumuksella.

Tietoja säilytetään lain määrittelemän ajan. Tietoja säilytetään niin, pitkään kuin asiakkuus, palvelun tarve, tai laskutusperuste on olemassa. Käsittelyn perusteena oleva lainsäädäntö, kirjanpitosäännökset tai mahdolliset oikaisuprosessit saattavat pidentää **säilytysaikoja**. Mikäli rekisterinpitäjä ei tarvitse sälytettävän tiedon sisältämää henkilötietoa, ne voidaan poistaa jossakin tapauksissa jo aiemmin säilytettävästä materiaalista. Tiedot hävitetään, kun ne eivät ole rekisterinpitäjän kannalta tarpeellisia.

Asiakasta koskevia tietoja käsittelevillä työntekijöillä on lakisääteinen **vaitiolovelvollisuus**. Salassapito- ja vaitiolovelvollisuus jatkuu palvelussuhteen päättymisen jälkeenkin. Rekisterin tietoturvallisuus sekä henkilötietojen luottamuksellisuus, eheys ja käytettävyys varmistetaan asianmukaisin teknisin ja organisatorisin toimenpitein.

1)Manuaalinen aineisto säilytetään lukitussa, kulunvalvonnan piirissä olevassa tilassa/ kameravalvonnan piirissä olevassa tilassa

2)Tietojärjestelmissä käsiteltävien tietojen suojauksessa on käytössä henkilökohtaiset käyttäjätunnukset ja salasanat, sekä kullakin henkilöllä on vain tehtävän hoitamiseksi tarpeelliset käyttöoikeudet, jotka määräajoin tarkistetaan.

4. LAINSÄÄDÄNTÖ JA MUU OHJEISTUS

Julkishallinnon organisaatiot noudattavat **Suomen ja EU:n lainsäädäntöä**. Kuntia ohjaavat mm. kuntalaki, hallintolaki, julkisuuslaki, tietosuoja-asetus, tietosuojalaki, arkistolaki sekä lukuiset muut yleis- ja erityislait. Lisäksi sisäiset ja ulkoiset **rahoittajat** (projektit, hankkeet) on omat ohjeistukset henkilötietojen käsittelystä, säilyttämisestä ja arkistoinnista. Sen lisäksi organisaatioilla on omia **käytännesääntöjä ja ohjeistuksia** sekä **kansallisia tai kansainvälisiä sertifikaatteja**. Organisaatioissa on myös omavalvontaa sekä virallisempia auditointeja. Tässä luvussa tehtävänä on käydä läpi lainsäädännöllistä ja omien ohjeistuksiin ja politiikkoihin liittyviä taustoja tietojenkäsittelyn osalta.

Lapinliitto ja lapin pelastuslaitos noudattavat tietoturva ja tietosuoja-asioissa seuraavia lakeja ja ohjeistuksia:

- EU:n tietosuoja-asetus (2016/679)
- Suomen perustuslaki (731) 2.luku 10 §: Yksityiselämän suoja ja luottamuksellisen viestin salaisuus 12 §: Viranomaisten hallussa olevien asiakirjojen ja tallenteiden julkisuus
- Laki viranomaisten toiminnan julkisuudesta (621/1999) 1 §: Julkisuusperiaate 3 §: Velvoite hyvään tiedonhallintatapaan 10 §: Tiedonsaanti salassa pidettävästä asiakirjasta 5 luku: Viranomaisen velvollisuudet edistää tiedonsaantia ja hyvää tiedonhallintatapaa 6 luku: Salassapitovelvoitteet 7 luku: Salassapidosta poikkeaminen
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Arkistolaki (821/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Tietosuojalaki (5.12.2018/1050): Henkilötietojen käsittelyä koskevat yleiset periaatteet
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003): Tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa
- Laki sähköisistä allekirjoituksista (14/2003)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Laki yksityisyyden suojasta työelämässä (759/2004): Työntekijää koskevien henkilötietojen käsittely
- Rikoslaki (39/1889) 34. luku 9a §: Vaaran aiheuttaminen tietojenkäsittelylle 38. luku 3 §: Viestintäsalaisuuden loukkaus 38. luku 8 §: Tietomurto 38. luku 9 § 1. kohta: Henkilörekisteririkos
- Henkilötietolaki (523/1999) 48 §: Henkilörekisteririkkomus
- Vahingonkorvauslaki (41/1974)
- Uudistuvat säädökset löytyvät ajantasaisina mm. Valtion säädöstietopankki – sivustolta (www.finlex.fi)
- Lapinliiton henkilöstön tietoturva- ja tietosuoja käsikirja (3.6.2019)
  Sharepoint: Ohjeita henkilöstölle tietoturvaan ja tietosuojaan liittyen.

5.REKISTERÖIDYN OIKEUKSIEN TOTEUTUMINEN

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, jonka tarkoituksena on turvata **rekisteröidyn oikeuksien ja vapauksien** toteutuminen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Rekisterinpitäjän velvollisuus on huolehtia rekisteröidyn oikeuksien toteutumisesta. Näitä ovat muun muassa rekisteröidyn oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada pääsy tietoihin ja oikeus oikaista virheellisiä tietoja. Lisäksi rekisteröidyillä on oikeus tietyillä rajauksilla saada tieto sosiaali- ja terveydenhuollon käyttö ja -luovutustiedoista. Rekisterinpitäjän tulee **informoida** rekisteröityjä henkilötietojen käytöstä avoimesti ja selkeästi. Rekisterinpitäjän tulee myös varautua mahdollisiin henkilötietojen tietoturvaloukkauksiin ja harjoitella niihin varautumista käytännössä. **Henkilötietojen tietoturvaloukkauksia** ovat mm., että tiedot lähetetty väärälle vastaanottajalle, suojaamaton tiedonsiirtoväline on hävinnyt esim. USB-tikku, haittaohjelmatartunta, kyberhyökkäys ja hakkerointi. Rekisterinpitäjän tulee tilastoida henkilötietojen tietoturvaloukkaukset ja ilmoittaa niistä tietosuojavaltuutetun toimistolle ja tietyn edellytyksin myös rekisteröidyille. Henkilötietojen käsittelijöillä on velvollisuus puolestaan ilmoittaa henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle. Tässä luvussa kuvataan tietosuojaperiaatteina erityisesti läpinäkyvyyttä ja kohtuullisuutta.

Lapin liitto ja Lapin pelastuslaitos käsittelee hyvin vähän toiminnassa henkilötietoja. Pyrimme siihen, että meillä olisi rekistereissämme mahdollisimman vähän henkilöiden tietoja ja varsinkin arkaluontoisia tietoja. Tarkoitus on, että emme rekisteröi turhaan mitään henkilötietoja ja poistamme meille tarpeettomat tiedot heti kun se on mahdollista. Omien työntekijöiden henkilötietoja käsitellään sisäisissä toimissa ja palkkakirjanpidossa. Säilytysajoista löytyy ohje Sharepointista.

Lapin liiton ja Lapin pelastuslaitoksen henkilötietoja käsittelevistä ohjelmista on tehty tietosuojaselosteet.

Ne löytyvät Sharepointista ja vuoden 2023 ne tullaan lisäämään Lapin pelastuslaitoksen internet sivuille. Sisäisesti on tehty ohjeet miten toimitaan, jos tulee henkilötietokysely, tietosuoja/tietoturvaloukkaus tai huijausviesti. Lisäksi on laadittu erilaisia ohjeita mm. etätyön tietoturvaan. Ne löytyvät Sharepointista.

6.ARVIOINTI, KEHITTÄMINEN JA TIEDON HYÖDYNTÄMINEN

Organisaation tulee arvioida tietosuojan ja -turvan tilanne toimintapolitiikan, mittareiden, kokonaisarkkitehtuuri ja muiden kuvausten avulla sekä mahdollisten asiakas- ja henkilöstön palautteiden näkökulmasta ja verrata kehitystä aiempiin vuosiin. Henkilöstön osaamisen, tietovirtojen ja toimintaprosessien arviointi ja kehittäminen ovat keskiössä. Organisaation johto voi johtaa tiedolla vain, jos sillä on riittävä ymmärrys omasta toiminnasta ja toimintaympäristöstään. Tavoitteena on päästä kohti tiedon hyödyntämistä. Tarkoituksena on tuoda esille myös keskeiset kehittämistavoitteet. Samalla on myös arvioitava asetettujen kehittämistavoitteiden toteutumista.

Lapin liiton ja Lapin pelastuslaitoksen tietosuoja-asiat ovat hoidettu lain vaatimusten mukaan. Tietosuoja ja tietoturva käsikirja on laadittu hyväksi pohjaksi. Lisäksi on laadittu useita muita ohjeita, mutta niiden laajuutta, saatavuutta ja kiinnostavuutta on parannettava. Pelastuslaitoksen puolella tietoturvatentti on ollut hyvä askel parempaan. Jatkossa se pitää tehdä kahden vuoden välein. Sen tekeminen tulee olla kaikille pakollinen ja sen suorittamisen määrää on seurattava.

Jatkossa on myös hyvä pyrkiä lisäämään koulutuksia ja lyhyitä tietoiskuja tietosuoja-asioista, jotta ne eivät pääsisi unohtumaan ja tiedon päivittäminen olisi jatkuvaa. Tulemme jatkossa tekemään paljon yhteistyötä Lapin hyvinvointi-alueen muiden tietosuojavastaavien kanssa.