VALTIOVARAINMINISTERIÖ

Julkisen hallinnon linjaukset tiedon sijainnista hallinnasta

Kuntamarkkinat 2018

13.9.2018 Tommi Kangasaho, valtioneuvoston kanslia

Tavoite 2025

Julkisen hallinnon ICT-palveluiden sijainti ja hallinta mahdollistavat kustannustehokkaat ja tiedon luottamuksellisuuden ja käytettävyyden varmistavat hallinnon omat ja kumppanoidut ratkaisut huomioiden organisaation erilaiset tiedonhallinnan tarpeet.

Työryhmän kokoonpano

- Tommi Kangasaho, VNK, puheenjohtaja (varalla Riku Sarlin)
- Pauli Kartano, VM, varapuheenjohtaja
- Eeva Lantto, VM
- Tero Latvakangas, Valtori (varalla Mikko Olli ja Mikko Määttä)
- Timo Kortesoja, Valtori (varalla Sonja Marjamäki)
- Tuula Seppo, Kuntaliitto
- Kimmo Rousku, Väestörekisterikeskus
- Eila Nummi, eduskunta (varalla Ari Apilo)
- Jukka Vesmanen, Vimana Oy
- Kalervo Koskimies, opetus- ja kulttuuriministeriö

Lisäksi mukaan kutsutaan asiantuntijoita työn eri vaiheisiin sekä julkisesta hallinnosta että elinkeinoelämän piiristä.

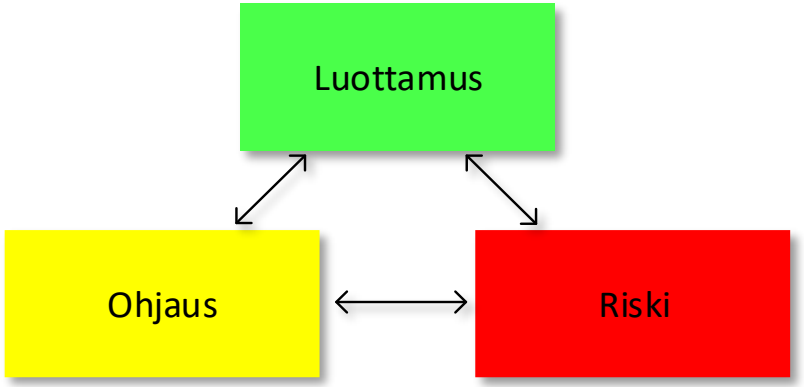
TIEDON JA PALVELUIDEN SIJAINTI, HALLINTA JA OHJAUS

Pilvipalvelut megatrendinä, ilmiönä ja mahdollisuutena

- Läpileikkaava ilmiö
- Jatkossa pääosa palveluista tulee olemaan väistämättä pilvipalveluita
- Palvelut laajasti käytössä
- Osaaminen pilvipalveluiden teknologiseen hyödyntämiseen sekä hankintaan vaihtelevaa
- Kyky huolehtia palveluiden vaatimuksenmukaisuudesta vaatii uusia kyvykkyyksiä

Ohjaus

- Palveluhyötyyn liittyvät riskit (muutokset sisältöön, ei voida hyödyntää uusinta teknologiaa)
- Palvelutakuuseen liittyvät riskit (kapasiteetti, saatavuus, jatkuvuus, tietoturva)
- Sopimusten tulkinta Suomen/ETA-alueen maissa
- Neuvotteluasema markkinoilla



Haasteet

- Luokiteltujen tietojen käsittely
- Toiminnan jatkuvuuteen liittyvät riskit tietojen sijaitessa ja/tai niiden hallinnan tapahtuessa Suomen ulkopuolella
- Tietoturvan ja tietosuojan toteutuminen tiedon sijainnista ja hallinnasta riippuen
    - Suomi, Euroopan Unioni (EU/ETA), muut maat
- Tietosuojan toteutuminen tiedon sijainnista ja hallinnasta riippuen
- Tiedon saatavuuteen ja omistajuuteen liittyvät riskit. Kuka omistaa tiedot? Mahdollistavatko palvelun käyttöehdot tiedon kaupallisen hyödyntämisen? Mikä vastuu palvelun tarjoajalla on, jos tietoa häviää? Mitä tapahtuu sopimuksen päättymisen jälkeen tiedolle?
- Usein yksipuoliset sopimusehdot

LINJAUKSET

1. linjaus

Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta

- Pilvipalveluita hankittaessa täytyy huomioida samat asiat kuin missä tahansa ICT-palvelun hankinnassa
- Pilvipalveluissa korostuu erityisesti hankintatoimen ja sopimustekniikan osaaminen sekä markkinatuntemus
- Pilvipalvelun hyödyntäminen perustuu riittävään tiedonomistajan tekemään riskiarvioon ja käyttöönottopäätökseen

2. linjaus

Tiedon sijaitessa Suomen rajojen ulkopuolella erityistä on kiinnitettävä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

- Sopimuksissa huomioitava millä ehdoille tietoa palvelussa käsitellään ja miten ja missä mahdolliset ristiriitatilanteet hoidetaan.
- Palvelun jatkuvuuden osalta on huomioitava palvelun toiminta päästä päähän, eikä keskittyä vain palveluntarjoajan toiminnan jatkuvuuteen.
- Palvelun hankkijan on kiinnitettävä varmistettava tiedon saatavuus erilaisissa tilanteissa sekä palveluntarjoajaa vaihdettaessa.
- On huomioitava oman organisaationsa ulkopuoliset käyttäjät ja niiden tarpeet ja vaatimukset.

3. linjaus

Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuu vaatimukset

- Palvelun arvo muodostuu palveluhyödystä ja -takuusta, joiden molempien täytyy toteutua
- Hyödyt ovat yleensä kiistämättömiä, mutta palvelutakuun sopiminen saattaa olla haasteellista varsinkin globaalien pilvipalveluiden luonteen vuoksi

4.linjaus

Mikäli pilvipalvelut tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita

- Valitaan aina parhaiten sopiva vaihtoehto
- Lähtökohtana pilvipalveluiden hyödyntäminen

5. linjaus

Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti vähintään kerran vuodessa ja oleellisten sopimusehtojen muuttuessa

- Varsinkin julkiset pilvipalvelut kehittyvät jatkuvasti, josta syystä niitä on arvioitava säännöllisesti ja oleellisten sopimusehtojen muuttuessa
- Palvelun tilanteen arviointi myös muista näkökulmista

6. linjaus

Viranomainen ylläpitää listaa hyväksytyistä palveluntarjoajista

- Viranomainen määrittelee millä keinoin ja/tai asetuksin tiedon käsittely on sallittua.
- Viranomainen ylläpitää listaa vaatimukset todennetusti täyttävistä palveluntarjoajista, joissa muun kuin julkisen tiedon käsittely on sallittua. Listalla olo ei ole ennakkovaatimus hankintoihin osallistumiselle, mutta ennen kuin palvelu voidaan ottaa käyttöön, sen on täytettävä määritellyt vaatimukset.

7. linjaus

Julkisen tiedon käsittelyä ei rajoiteta

- Julkista, tai sellaiseksi tarkoitettua, tietoa voidaan käsitellä vapaasti pilvipalveluissa
- Varautumisvaatimukset ja tietoturva (eheys, kiistämättömyys, saatavuus) huomioitava

8. linjaus

Henkilötietoa suojaustason IV tietoa voi käsitellä julkisessa pilvessä, kun tietoturva ja -suoja on asianmukaisesti toteutettu

- Kun tieto on esimerkiksi salattu ja suojattu asianmukaisesti viranomaisen hyväksymällä tavalla, voidaan sitä käsitellä julkisessa pilvipalvelussa
- Henkilötietojen käsittelyn ja hallinnan osalta tulee lisäksi varmistua muista EU/ETA-alueen ulkopuolella vaadittavista edellytyksistä.

9. linjaus

Suojaustason III tietoa voi käsitellä viranomaisen hyväksymissä pilvipalveluissa

- Luottamuksellisen tiedon käsittelyyn käytettävän pilvipalvelun täytyy sijaita fyysisesti Suomen tai EU:n alueella ja sen täytyy olla Suomessa tai EU alueella sijaitsevan toimijan hallinnassa
- Palvelusta on viranomaisen hyväksyntä
- Valinta perustuu tiedonomistajan riskiarvioon

Suosituksia jatkotoimenpiteiksi 1/2

- Luodaan prosessit, joilla pystytään välttämään päällekkäisiä arviointeja ja auditointeja yhteisille palveluille
- Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI) luo arviointipankin, jossa on saatavilla tietoja tehdyistä arvioinneista helpottamaan uusien hankintojen ja palveluiden suunnittelua ja määrittelyä
- Luodaan hallinnolle ylätason pilviohje, jossa yleisimpien palvelujen soveltuvuutta on tuotu esiin ja jossa huomioidaan myös hankinta-asiat (esimerkkinä vastaavasta https://wiki.eduuni.fi/display/pilviohje/Pilviohje)
- Tarkastellaan linjaukset uuden tiedonhallintalain tultua voimaan ja päivitetään linjaukset ja termistö vastaamaan uutta lakia.

Suosituksia jatkotoimenpiteiksi 2/2

- Neuvotellaan yhteiset sopimus- ja hinnoitteluehdot tärkeimpien palveluntarjoajien kanssa koko julkiselle hallinnolle
- Luodaan riskianalyysipohja ja toteutusmallin valintatyökalu tukemaan palvelujen ja niiden vaatimusten arviointia
- Luodaan ylätason pilviarkkitehtuuri
  - Osana pilviarkkitehtuuria luodaan käyttötapausesi-merkkejä helpottamaan hankintojen ja palveluiden suunnittelua ja määrittelyä

Jatkotyössä selvitetään vastuulliset toteuttajat sekä tarkempi sisältö, aikataulu ja seuranta kullekin toimenpiteelle.

Henkilötietojen tietoturvaloukkaukset ja TAISTO18 harjoitus

Kuntamarkkinat 13.9.2018 Kimmo Rousku

Väestörekisterikeskus

@kimmo

- Kimmo Rousku, VAHTI-pääsihteeri, Väestörekisterikeskus.
- Kimmo Rousku on toiminut valtionhallinnossa ICT- ja turvallisuuden asiantuntija ja johtamistehtävissä vuodesta 1995 saakka, viimeisen kymmenen vuoden ajan hän on keskittynyt valtion ja julkisen hallinnon turvallisuuden eri osa-alueiden kehittämiseen.
- Kimmo toimii VAHTI-pääsihteerinä ja johtavana erityisasiantuntijana Väestörekisterikeskuksessa.

Tule mukaan verkostoihini!

Väestörekisterikeskus

- Yhteiskunnan digitalisaatio etenee kovaa vauhtia. Väestörekisterikeskuksen Digiturvapalvelut tukevat koko julkista hallintoa turvallisten palvelujen ja toimintaympäristön kehittämisessä.
- Väestörekisterikeskus vastaa VAHTIn operatiivisesta toiminnasta.
- Väestörekisterikeskus tuottaa digitaalisen turvallisuuden asiantuntijapalveluita koko valtionhallinnolle.
- **#digiturva**

Väestörekisterikeskus

Aloitetaan terminologiasta

#Digiturva

- **Riskienhallinta**
  - *kaiken* toiminnan kulmakivi, myös vapaa-aikana
- **Tietoturvallisuus**
  - Tietojen tai muun suojattavan kohteen saatavuus, eheys
    - Lisäksi luottamuksellisuus, ***vain*** jos kyseessä on salassa pidettävä tieto
- **Kyberturvallisuus**
  - Digitaalisen toimintaympäristön kokonaisvaltainen turvaaminen, sisältää myös infrastruktuurin ja muut tarvittavat rakenteet
- **Jatkuvuuden hallinta ja varautuminen**
  - Ei jos vaan ***KUN*** kaikesta huolimatta jotain tapahtuu, miten organisaatio palautuu takaisin sen toiminnalta edellytettävään tilaan – toteuttamalla jatkuvuus | valmius | toipumissuunnitelmia sovitusti
- **Tietosuoja**
  - Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.

Väestörekisterikeskus

Ja tästä lisätietoa – ajankohtaista digiturvasta videoblogit

Ajankohtaista digiturvallisuudesta 1/2018 (koko soittolista)

Ajankohtaista digiturvallisuudesta avaus
VAHTIn varapuheenjohtaja Aku Hilve, valtiovarainministeriö

Henkilöstö:

Miten selviät turvallisuuden terminologiaviidakossa?
VAHTI-pääsihteeri Kimmo Rousku, Väestörekisterikeskus

MMKT – toimintamalli turvalliseen työskentelyyn
VAHTI-pääsihteeri Kimmo Rousku, Väestörekisterikeskus

Kybersää
Tilannekuvapalveluiden päällikkö Jarna Hartikainen, Viestintävirasto, Kyberturvallisuuskeskus

ICT-, tietoturva- ja tietosuojahenkilöt:

Suojaudu kyberuhalta
Tilannekuvapalveluiden päällikkö Jarna Hartikainen, Viestintävirasto, Kyberturvallisuuskeskus

Johto:

Riskienhallinta on organisaation toiminnan mahdollistaja
VAHTI-pääsihteeri Kimmo Rousku, Väestörekisterikeskus

Kyberturvallisuuden johtaminen
Johtaja Jarkko Saarimäki, Viestintäviraston, Kyberturvallisuuskeskus

Ajankohtaista tietosuojasta johdolle ja esimiehille
Erityisasiantuntija Tuula Seppo, Kuntaliitto sekä VAHTI-pääsihteeri Kimmo Rousku, Väestörekisterikeskus

Ajankohtaista digiturvallisuudesta 2/2018 (koko soittolista)

Henkilöstö:

Tietosuoja-asetuksen soveltaminen on alkanut 25.5.2018
Tietosuojavaltuutettu Reijo Aarnio, tietosuojavaltuutetun toimisto sekä VAHTI-pääsihteeri Kimmo Rousku, Väestörekisterikeskus

Mitkä perusasiat jokaisen pitää muistaa tietosuojasta?
Ylitarkastaja Anna Hänninen, tietosuojavaltuutetun toimisto

Vain vahva salasana suojaa tietosi
Asiantuntija Johanna Rautio | Tietoturva-asiantuntija Perttu Halonen, Viestintävirasto, Kyberturvallisuuskeskus

Varo huijareita verkossa
Asiantuntija Johanna Rautio | Tietoturva-asiantuntija Perttu Halonen, Viestintävirasto, Kyberturvallisuuskeskus

Kesän #kybersää
Tilannekuvapalveluiden päällikkö Jarna Hartikainen, Viestintävirasto, Kyberturvallisuuskeskus

ICT-, tietoturva- ja tietosuojahenkilöt:

Väestörekisterikeskus tuottaa valtiohallinnon digitaalisen turvallisuuden asiantuntijapalveluita, mihin palveluita voi käyttää ja kuinka ne saa käyttöön?
Tietoturva-asiantuntija Hanna Heikkinen, Väestörekisterikeskus

Miksi ja miten organisaatio voi osallistua henkilötietojen tietoturvaloukkausten hallintaa edistävään TAISTO18-harjoitukseen?
VAHTI-pääsihteeri Kimmo Rousku, Väestörekisterikeskus

Johto ja esimiehet:

Tietosuojavaltuutetun terveiset johdolle koskien tietosuojan kehittämistä
Tietosuojavaltuutettu Reijo Aarnio, tietosuojavaltuutetun toimisto

Väestörekisterikeskus

VALTIOVARAINMINISTERIÖ

"Nouda passi
Ärrältä kulkematta
poliisilaitoksen kautta!"
Riskienhallinta mahdollistaa uudenlaisia toimintamalleja.

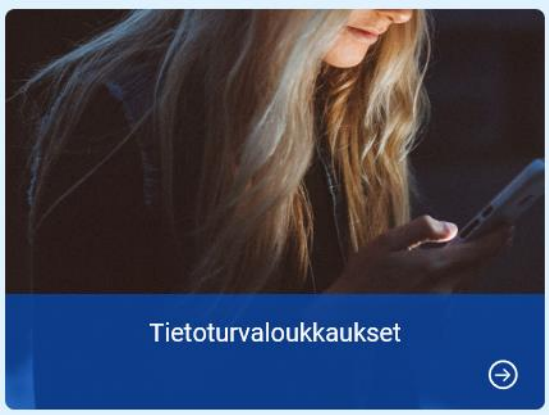
Johda myös riskejä

Mahdollista onnistuminen ja menestys

Väestörekisterikeskus

Henkilötietojen tietoturvaloukkaus?

- Tietosuojavaltuutetun toimistolla loistavat, uudet toukokuussa päivitetyt sivut



Väestörekisterikeskus

Tietoturvaloukkaukset

Mikä on henkilötietojen tietoturvaloukkaus?

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa
- tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen.

Väestörekisterikeskus

2 Jakso

Henkilötietojen turvallisuus

32 artikla

Käsittelyn turvallisuus

1. Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten

a) henkilötietojen pseudonymisointi ja salaus;

b) kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;

c) kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;

d) menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

2. Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi.

Dokumentoi kaikki henkilötietojen tietoturvaloukkaukset

Sekä rekisterinpitäjän että henkilötietojen käsittelijän on suojattava henkilötiedot niin, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvää riskiä. Lisäksi rekisterinpitäjän on varauduttava mahdollisiin tietoturvaloukkauksiin laatimalla toimintaohjeet tietoturvaloukkaustilanteita varten. Tietoturvaloukkauksiin on pystyttävä reagoimaan mahdollisimman nopeasti.

Rekisterinpitäjän täytyy arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena olleille henkilöille, esimerkiksi

- ei aiheudu riskiä
- aiheutuu riski
- aiheutuu korkea riski.

Riskin taso määrittää ne toimenpiteet, joihin rekisterinpitäjän on ryhdyttävä. Toimenpiteitä ovat esimerkiksi

- tietoturvaloukkauksen dokumentointi
- ilmoitus valvontaviranomaiselle
- ilmoitus rekisteröidylle.

Dokumentoi kaikki henkilötietojen tietoturvaloukkaukset sekä niiden vaikutukset ja toteutetut korjaavat toimet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta lopulta seuraa. Dokumentointivelvollisuuden tai ilmoituksen tekemisen laiminlyöminen on tietosuoja-asetuksen vastaista. Se voi johtaa tietosuoja-asetuksessa määritettyihin seuraamuksiin.

Esimerkkejä henkilötietojen tietoturvaloukkauksista ja siitä, kenelle niistä ilmoitetaan

Seuraavien esimerkkien tarkoituksena on auttaa rekisterinpitäjiä määrittämään, onko niiden tehtävä ilmoitus erilaisissa henkilötietojen tietoturvaloukkaustilanteissa. Nämä esimerkit voivat myös olla avuksi määritettäessä, kohdistuuko henkilöiden oikeuksiin ja vapauksiin riski vai korkea riski.

Esimerkki	**Ilmoitetaanko valvontaviran-omaiselle?**	**Ilmoitetaanko rekisteröi-dylle?**	**Huomautukset/ suositukset**
i. Rekisterinpitäjä on tallentanut salatun varmuuskopion henkilö-tietoja sisältävästä arkistosta USB-muistitikulle. Muistitikku varastetaan tiloihin tehdyn murron yhteydessä.	Ei.	Ei.	Mikäli tiedot on salattu uusimman tekniikan mukaisella algoritmilla, tiedoista on varmuuskopioita, yksilöllinen salaus-avain ei vaarannu ja tiedot voidaan palauttaa ajoissa, tästä tietoturva-loukkauksesta ei välttämättä tarvitse ilmoittaa. Jos tiedot kuitenkin myöhem-min vaarantuvat, ilmoittaminen on tarpeen.

- Mihin tämä pohjautuu?
- Riskienhallintaan

Väestörekisterikeskus

Mitä riskien arvioinnissa on otettava huomioon?

Rekisterinpitäjän on arvioitava, millainen riski tietoturvaloukkauksesta on aiheutunut vuodon kohteena olevalle henkilölle. Arvio määrittää tarvittavia tietoturvaloukkauksesta seuraavia toimenpiteitä.

Huomioi arviossa seuraavat asiat:

1. Tietoturvarikkomuksen tyyppi
2. Henkilötietojen luonne, arkaluonteisuus ja määrä
3. Tunnistamisen helppous
4. Rekisteröidyn ominaisuudet
5. Rekisterinpitäjän ominaisuudet
6. Tietovuodon seurauksien vakavuus

Väestörekisterikeskus

Ilmoita valvontaviranomaiselle 72 tunnin kuluessa

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. Henkilötietojen käsittelijän tulee ilmoittaa tietoturvaloukkauksesta ensin rekisterinpitäjälle, jollei ole erikseen sovittu, että käsittelijä voi ilmoittaa tietoturvaloukkauksista suoraan tietosuojavaltuutetun toimistolle. Vastuu ilmoituksen tekemisestä säilyy kuitenkin rekisterinpitäjällä.

Ilmoituksen voi tehdä sähköisellä lomakkeella. Jos ilmoitusta ei tehdä 72 tunnin kuluessa, rekisterinpitäjän on toimitettava tietosuojavaltuutetun toimistolle perusteltu selitys.

Koska henkilötietojen tietoturvaloukkauksesta ilmoitetaan rekisteröidylle?

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Rekisterinpitäjän on tällöin ilmoitettava asiasta ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua esimerkiksi sulkemalla luottokorttinsa.

Sisällytä ilmoitukseen nämä tiedot:

- selkeä kuvaus henkilötietojen tietoturvaloukkauksesta
- tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa
- henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset
- toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on jo toteuttanut; tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

Ilmoitusta ei vaadita, jos

- rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja niitä on sovellettu henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin (erityisesti niitä, joiden avulla henkilötiedot muutetaan ulkopuolisille mahdottomiksi ymmärtää, kuten salausta)
- rekisterinpitäjä on tehnyt jatkotoimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu
- se vaatisi kohtuutonta vaivaa, koska ei esimerkiksi tiedetä, keitä rekisteröidyt ovat. Asiaa arvioidaan riskien mukaan. Jos rekisteröityihin ei voida ottaa yhteyttä henkilökohtaisesti, on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröityjä informoidaan yhtä tehokkaalla tavalla.

Jos rekisterinpitäjä ei ole vielä ilmoittanut henkilötietojen tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia ilmoituksen tekemistä.

Miten pienennät riskiä henkilötietojen tietoturvaloukkauksen osalta?

Väestörekisterikeskus

MMKT-toimintamalli turvalliseen työskentelyyn

- Me kaikki teemme virheitä – tällä pienennät niiden todennäköisyyttä
- 95% tieto- ja kyberturvallisuuteen liittyvistä poikkeamista aiheutuu ihmisten toiminnasta, tietoisesta tai yleensä tiedostamattomasta
- Ja ennen kaikkea ***kiireestä*** tai muusta huolimattomuudesta
- https://www.youtube.com/watch?v=yPpZXvjAMjI&list=PLl-Miv8NOLJnfk9diD-4UrbcO8oeMxRzL&index=3

Henkilöstölle: MMTK toimintamalli turvalliseen työskentelyyn

Väestörekisterikeskus

MMKT-toimintamalli turvalliseen työskentelyyn

Väestörekisterikeskus

MMKT-toimintamalli turvalliseen työskentelyyn

Väestörekisterikeskus

Suosittelemme tutustumaan ja hyödyntämään

- VAHTI-ohjeet ja materiaalit
- www.vahtiohje.fi
- Ajankohtaisvideoblogit (joista mm. edellä olevat on poimittu)
- www.vm.fi/digiturva
- VAHTI-tilaisuuksien materiaalit, mm lokakuun julkisen hallinnon digiturvallisuuden teemakuukausi
- https://vm.fi/vahti-materiaalit-ja-tilaisuudet
- Tietosuojan ja tietoturvan yhteishankkeet
- https://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit
  - 24.9 työpaja #15 ja loppuvuodesta vielä kaksi työpajatilaisuutta
- Arjen tietosuoja-verkkokoulutukset ja testi [yhteensä jo **yli 240 000** katselukertaa]
- http://www.arjentietosuoja.fi

Väestörekisterikeskus

Väestörekisterikeskus

Miksi? Miten? Kenelle? Miten mukaan?

- **Miksi?**
  - Tietosuoja-asetus edellyttää uusia prosesseja, esimerkiksi henkilötietojen tietoturvaloukkausten osalta
  - Näitä prosesseja tulee harjoitella, tosin osa joutuu harjoittelemaan näitä ns. livenä eli arjen tapahtumissa – harjoitus tekee mestarin, mutta mestaritkin harjoittelevat
- **Miten?**
  - Valtiovarainministeriö toteuttaa TAISTO18-harjoituskuukauden marraskuussa, jossa julkisen hallinnon organisaatiot voivat harjoitella (henkilötietojen) tietoturvaloukkausten hallintaa hyvin suunnitellun ja johdetun harjoituksen avulla omassa organisaatiossaan

Väestörekisterikeskus

Miksi? Miten? Kenelle? Miten mukaan?

- **Kenelle?**
  - Julkisen hallinnon organisaatiot tai sellaisten omistamat organisaatiot (laajasti tulkittuna)
  - Entäs me yritykset – saatte joulukuussa kaiken tarvittavan materiaalin, ohjeet ja tiedot sellaisen toteuttamiseksi itsenäisesti
- **Miten mukaan?**
  - Kutsukirje
  - Linkki ilmoittautumiseen

Yhteishankkeiden materiaalit

Tälle sivulle kootaan tietosuojan yhteishankkeiden työpajatilaisuuksien verkkolähetyslinkit, materiaalit, työkalut, ryhmä- sekä kotitehtävät. Sivulla on listattu myös tulevat työpajatilaisuudet.

Kutsu julkisen hallinnon organisaatioille osallistua TAISTO18-harjoitukseen:

- Kutsu Taisto18-harjoitukseen PDF 130kB
- Inbjudan till Taisto18-övningen PDF 135kB
- Ilmoittautumislinkki Taisto18-harjoitukseen
  Suomeksi: http://www.webropolsurveys.com/S/49348605CF4890E2.par
  Ruotsiksi: http://www.webropolsurveys.com/S/2CF949F09B81EDA5.par

https://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit

Väestörekisterikeskus

Digiturvallista syksyä!

Kimmo Rousku
VAHTI-pääsihteeri | Johtava erityisasiantuntija
kimmo.rousku@vrk.fi – puh. 029553 5120

Väestörekisterikeskus