EU:n henkilötietosuoja-asetus (GDPR = General Data Protection Regulatio)

Astui voimaan 25.5.2016

Sanktiot astuivat voimaan 25.5.2018

eKirja
Holvin verkkokaupasta:

https://holvi.com/shop/TietoPaula/

1 EU:n tietosuoja-asetuksen (GDPR) tarkoitus pähkinänkuoressa
2 Peruskäsitteet
3 Rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet
4 Tietosuojaseloste
5 Kumppanisopimukset
6 Rekisterien käsittelykuvaukset
7 Henkilöstön ohjeistus
8 Tietovuodon sattuessa
9 Esimerkki omavalvontasuunnitelman sisällysluettelosta

Keskitymme näihin:

- EU:n henkilötietosuoja-asetuksen (GDPR) tarkoitus pähkinänkuoressa
- Peruskäsitteet
- Rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet
- Keskustelu

Ketä EU:n henkilötietosuoja-asetus koskee?

- Tämä koskee kaikkia EU:n alueella toimivia organisaatioita, jotka
  - keräävät
  - tallentavat
  - käyttävät henkilötietoja.

- B2C , ei koske B2B

Henkilötietoja (personal data) ovat

- Nimi
- Osoite
- Sähköpostiosoite
- Sijaintitiedot
- Verkkotunnistetiedot
- Terveystiedot
- Tulot ym. raha-asiat
- Kulttuurinen profiili

Miksi uudistus on tarpeen?

- Epäluottamus vanhoja tietosuojaa koskevia sääntöjä kohtaan oli este digitaalitalouden kehitykselle.

- Vain 15 % ihmisistä EU:ssa tehdyn tutkimuksen mukaan tuntee, että he voivat täysin hallita antamiaan tietoja verkossa.

Yritysten kasvun vauhdittaminen

- Samat säännöt kaikille yrityksille, jotka käsittelevät henkilötietoja EU:ssa.

- Liiketoiminta muuttuu helpommaksi ja reilummaksi.

Uusi järjestelmä pitää kustannukset alhaisina ja auttaa yrityksiä kasvamaan.

- 130 miljoonaa euroa ovat EU:ssa toimivien yritysten kustannukset tiedottamisesta 28:lle eri tietosuojaviranomaiselle vanhassa järjestelmässä.

- 2,3 miljardia euroa TÄMÄN yhden lain tuoma arvioitu taloudellinen hyöty. Harmonisoinnin hyöty.

Mitä yrityksen on tehtävä?

- Suojeltava niiden ihmisten oikeuksia, jotka luovuttavat tietojaan.
- ”Luotava tietojenkäsittelyn suojatiet.”

Rekisteröidyn oikeudet

- Oikeus **tarkastaa** omat tietonsa.
- Oikeus **pyytää korjausta** tietoihinsa.
- Oikeus **vaatia tietojensa poistamista** ts. vaatimus tulla unohdetuksi.
- Oikeus **kieltää suoramarkkinointi** tai rajoittaa kiistanalaisten tietojen käsittelyä kunnes asia saadaan ratkaistua.

Rekisteröidyn oikeudet

- Oikeus **siirtää tiedot** johonkin toiseen järjestelmään, silloin kun tiedot ovat rekisteröidyn itsensä toimittamia ja tietojen käsittely perustuu suostumukseen tai sopimukseen.
- Oikeus vastustaa henkilötietojensa käsittelyä, jos on sitä mieltä, että tietoja on käsitelty lain vastaisesti tai rekisterinpitäjällä ei ole oikeutta käsitellä niitä.
- Oikeus tehdä valitus henkilötietojensa käsittelystä valvontaviranomaiselle.

Peruskäsitteet

- **Rekisterinpitäjä** (controller) on organisaatio, joka yksin tai yhdessä toisen tahon kanssa määrää henkilötietojen käsittelyn tarkoitukset ja keinot.
- **Rekisteröity** (data subject) on luonnollinen henkilö
-
- **Käsittelijä** (processor) on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun (esimerkiksi atk-palvelun toimittaja, joka tuottaa rekisterin atk-käsittelyn).
-
- **Rekisteri** (filing system) on mikä tahansa jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein (voi olla hajautettu, keskitetty tai jaettu).
-
- **Suostumus** (consent) on mikä tahansa vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojen käsittelyn.

Viestintä rekisteröidylle

- Käytä selkeää kieltä.
- Kerro **kuka** olet, kun pyydät tietoja.
- Kerro **miksi** käsittelet heidän tietojaan,
- **kuinka kauan** niitä säilytetään ja
- **kenelle** ne luovutetaan.

Varoitus

- Tiedota ihmisille tietoturvaloukkauksista, jos heihin kohdistuu vakava uhka.

- Tämä on laissa määritelty velvollisuus

Suostumus

- Pyydä ihmisiltä selkeä suostumus tietojen käsittelyyn.

- Keräätkö tietoja lapsilta sosiaalista mediaa varten?
  - Tarkista ikäraja, joka määrittää, tarvitaanko vanhemman suostumus

Tietojen tarkastelu ja siirto

- Anna ihmisille mahdollisuus tarkastella tietojaan ja siirtää ne toiselle yritykselle.

Arkaluonteisten tietojen turvaaminen

- Toteuta ylimääräisiä suojatoimia terveyttä, rotua, sukupuolista suuntautuneisuutta, uskontoa ja poliittisia näkemyksiä koskevien tietojen turvaamiseksi.

Pyyhi tiedot pois

- Anna ihmisille ”oikeus tulla unohdetuksi”. Pyyhi heidän henkilötietonsa, jos he sitä pyytävät, mutta vain, jos se ei rajoita ilmaisunvapautta tai mahdollisuutta tehdä tutkimusta.

Markkinointi

- Anna ihmisille oikeus kieltäytyä suoramarkkinoinnista, johon käytetään heidän antamiaan tietoja.

Tekoäly

- Jos käytät profilointia oikeudellisesti velvoittavien sopimusten (esim. lainat) hakemusten käsittelyyn, sinun on
- **kerrottava s**iitä asiakkaillesi;
- **varmistettava, että prosessin tarkistaa ihminen eikä kone, jos hakemukseen vastataan kielteisesti.**
- **tarjottava hakijalle oikeus riitauttaa päätös**

Tietojen siirto EU:n ulkopuolelle

- Tee oikeudellisia järjestelyjä siirtäessäsi tietoja maihin, joita EU:n viranomaiset eivät ole hyväksyneet.

Tuotekehitys, kehitystyö

- Sisällytä tietosuoja suunnitteluun
- Tarkista, tarvitsetko tietosuojasta vastaavan henkilön Mitä yrityksesi on tehtävä?
- Noudattamatta jättämisen hinta
- Ota tietoturva huomioon tuotteidesi mahdollisimman varhaisessa kehitysvaiheessa.

Tietosuojavastaava

-
- Tarkista, tarvitsetko tietosuojasta vastaavan henkilön.
- Se ei ole aina pakollista. Tarve riippuu siitä, minkä tyyppisiä tietoja keräät ja kuinka paljon, onko tietojen käsittely pääasiallista liiketoimintaasi ja teetkö sitä suuressa mittakaavassa.

Käsitteletkö tietoja toiselle yritykselle?

- Varmista, että sinulla on aukoton sopimus, jossa luetellaan kummankin osapuolen velvollisuudet.

Noudattamatta jättämisen hinta

- Paikalliset tietosuojaviranomaiset valvovat lain noudattamista. Heidän työtään koordinoidaan EU:n tasolla. Sanktio voi olla
  - Varoitus
  - Huomautus
  - Tietojenkäsittelyn keskeyttäminen
  - Sakko, jopa 20 milj. euroa tai 4 % liikevaihdosta. Sääntöjen rikkomisen hinta voi olla korkea.

Pk-yritysten on pidettävä rekisteriä ainoastaan, jos tietojen käsittely

- On säännöllistä
- Uhkaa ihmisten oikeuksia ja vapauksia
- Koskee arkaluonteisia tietoja tai rikosrekisteritietoja.

Rekisterin kirjattavat tiedot

- Yrityksen nimi ja yhteystiedot
- Tietojen käsittelyn syy
- Rekisteröityjen ryhmien ja henkilötietojen kuvaus
- Tietoja vastaanottavien organisaatioiden ryhmät
- Tietojen siirtäminen toiseen maahan tai organisaatioon
- Tietojen poistamisen määräaika, jos mahdollista
- Kuvaus käsittelyn yhteydessä käytettävistä turvatoimista, jos mahdollista

Valmistaudu vaikutustenarviointiin

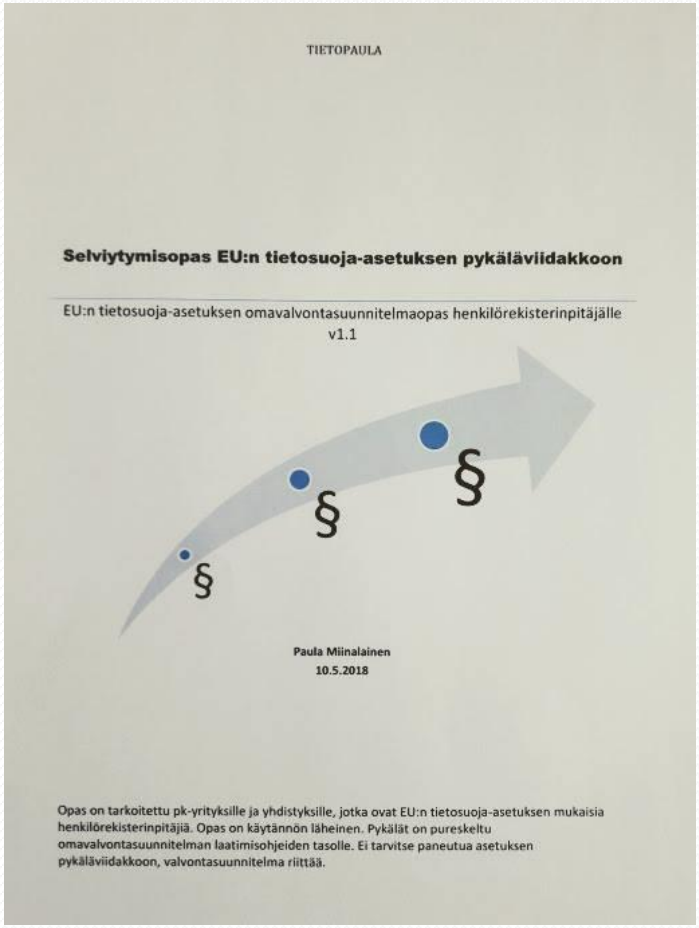
- Vaikutustenarviointia saatetaan edellyttää korkean riskin tietojenkäsittelyssä.
  - Uudet teknologiat
  - Henkilötietojen automaattinen, systemaattinen käsittely ja arviointi
  - Julkisen alueen laaja-alainen valvonta (esim. videovalvonta)
  - Arkaluonteisten tietojen laaja-alainen käsittely, kuten biometria

Kuvat

- Julkisen alueen laaja-alainen valvonta (esim. videovalvonta)

eKirja Holvissa saatavissa

https://holvi.com/shop/TietoPaula/



Tietosuojaoppaita

Oikeusministeriön opas

Artikkeli TIVI-lehdessä

Paula Miinalainen
Paula on pitkän linjan ICT-ammattilainen. Hänellä on vuosikymmenten aikana kertynyt ammattitaito järjestelmien rakentamisesta erityisesti taloushallinnon ja vakuutustenhoidon alueella. Paulasta on tärkeää se, että nyt yhdenmukaistetaan EU:n direktiivien määräämänä vastaavia järjestelmiä EU:n alueella.

Suojele henkilötietoja - suojele organisaatiotasi

nisaatioihin, jotka käsittelevät EU-kansalaisten henkilötietoja oman toimintansa vuoksi tai käsittelevät niitä toisen organisaation puolesta. Henkilötietoja ovat: nimi, osoite, sijaintipaikka, verkontunnistetiedot,

tamiseksi on määrätty joukko sääntöjä, joita on pakko noudattaa. Noudattamatta jättäminen on sanktioitu. Sanktio voi olla: varoitus, huomautus, tietojenkäsittelyn keskeyttäminen tai sakko. Sakko voi olla jopa 20

miten asetuksen määräyksiä on organisaatiossa noudatettu. Asetus antaa jonkin verran kansallista liikkumavaraa. Se aiheuttaa lukuisia muutoksia Suomen lainsäädäntöön. Muutokset ovat parhaillaan lausuntokierroksella oikeusministeriössä.

Artkkkeli TIVi-lehdessä

Selviytymisopas
EU:n tietosuoja-asetuksen pykäläviidakkoon

Teksti: Paula Miinala ja Minna Oksanen

► EU:n tietosuoja-asetus (GDPR = General Data Protection Regulation) vaikuttaa liiketoimintaprosesseihin ja tulevaan lainsäädäntöön. Se koskee jokaista organisaatiota, joka käsittelee eurooppalaisen henkilötietoja. Viisas johto näkee vahvan tietosuojan lisäävän organisaation luotettavuutta ja panostaa asetuksen toteuttamiseen. Hyvä tietosuoja kannattaa tuoda esiin osana yrityskuvaa, sitä ei kannata jättää vain juristien ja tietohallinnon asiaksi vaan se on koko organisaation asia. Organisaation johto on tarvittavien toimenpiteiden mahdollistaja sekä jalkauttaja koko organisaatiossa.

Organisaatiolla on näyttövelvollisuus asetuksen noudattamisesta. Tätä varten on hyvä laatia omavalvontasuunnitelma. Tässä artikkelissa esitämme yksinkertaisen perusrungon siitä, millainen tämä omavalvontasuunnitelma voisi olla.

Paula Miinalainen *on pitkän linjan ICT-ammattilainen, jolla on vuosikymmenien aikana kertynyt ammattitaito järjestelmien rakentamisesta erityisesti taloushallinnon ja vakuutusten hoidon alueilla. Nyt Paulan mielestä on tärkeää yhdenmukaistaa vastaavia järjestelmiä ja tietosuojaa EU:n alueella.*

Minna Oksanen *on tiedon hallinnan ammattilainen Talent Basesta, jolla on kokemusta sekä BI-alueesta että master datan jalkauttamisesta ja liiketoiminnan käsite- ja tietomallinnuksesta. Hän on ollut asiantuntijana useassa regulaatiohankkeessa mm. viimeisimpänä ison organisaation GDPR-hankkeesta. Minna on TIVIAn hallituksen jäsen ja vastuussa viestintätoimikunnasta.*

TEE NÄMÄ:

1. Mieti tietosuojalupaus
Tietosuojalupaus: Pidämme henkilötietojen turvallisuudesta huolta
tietosuojalainsäädännön mukaisesti. Järjestelmämme ovat suojattuja, emmekä anna tietoja kolmannelle osapuolelle ilman henkilön lupaa.

4. Tee kustakin rekisteristä henkilötietojen käsittelyn prosessikuvaus, jossa kuvaat, kuka tekee, mitä tekee, miksi tekee ja missä tekee. Kuvaa millaiset oikeudet tekijällä on henkilötietojen käsittelyyn.

5. Käy läpi kumppanit, jotka ovat henkilötietojen käsittelijöitä.
It-palvelujen toimittajat, it-tuki, rekrytointikumppanit, arkistojen

MARKKINOINTIREKISTERI

Firma oy
rekisterinpitäjä

Asiakasrekisteriin liittyvä

Postittaja oy:n ohjelmistos
henkilökohtaiset käyttäjätu

Muutos asiakastietoih

Tietojen katseluoike

Asiakkaan poisto
- Poistosääntö
- Asiakkaan pyy
- Erityinen poisto

1. Firma Oy:
pääsee v
markkino

Rekisterinp
yksin tai yh
tietojen käs

Käsittelijä
lötietoja re