Miten tietosuoja-asetusta toteutetaan Valtorin tuottamissa palveluissa

Aapo Immonen, Valtori

Valtori | Valtion tieto- ja viestintätekniikkakeskus

Sisältö

- Tietosuojavastaava ja tietosuojaorganisaatio
- Nykytilan kartoitus
- Rekisteröidyn oikeudet
- Rekisteripitäjän velvollisuudet
- Sopimukset (Rekisterinpitäjä-tietojenkäsittelijä Alihankkija)
- Osoitusvelvollisuus
- Riskiarvio
- Vuosikello
- Koulutus
- Poikkeamista ilmoittaminen, dokumentointi, raportointi

Tietosuojavastaava ja tietosuojan organisointi

- Toiminta osa tieto – ja kyberturvayksikön toimintaa
- Toimintaa ohjaa Tietosuojaryhmä, joka raportoi johdolle
- (TORI) tietosuojavastaava : Aapo Immonen , TUVE – yksikössä : Timo Kortesoja
- Tietosuojaresurssit : Maija Ronkainen, Raimo Hintikka, Markku Tihilä sekä 2 KPL KPMG:n konsultteja (toukokuuhun 2018 asti)
- Yhteydenotot: tietosuoja@valtori.fi tai suoraan tietosuojavastaavalle aapo.immonen@valtori.fi, tel: 0295 505 029

- Koko GDPR-asetus pohjautuu rekisteröityjen oikeuksien varmistamiseen
- Paljon vanhaa henkilötietolaista, vähän myös uutta
- Oleellista prosessikuvaukset ja niiden jalkauttaminen rekisteröidyn oikeuksien toteuttamiseksi

Rekisterinpitäjän tiedonantovelvoitteet

- Rekisterinpitäjällä velvollisuus tiedottaa avoimesti henkilötietojen käsittelystä:

Löytyy tietosuojaselosteesta:

- Rekisterinpitäjän ja tietosuojavastaavan yhteystiedot
- Henkilötietojen käyttötarkoitus ja käsittelyn oikeusperusta
- Säännönmukaiset tietolähteet
- Henkilötietojen luovutus kolmansille osapuolille
- Henkilötietojen luovutus kolmansiin maihin
- Henkilötietojen säilytysaika ja sen kriteerit
- Oikeus tehdä valitus valvontaviranomaiselle
- Automaattinen päätöksenteko ja profilointi
- Valtorilla tunnistettu n. 10 rekisteriä

Lähtökohtaisesti.

TIETOSUOJASELOSTE

1. Rekisterinpitäjä	**Nimi:** Valtion tieto- ja viestintätekniikkakeskus Valtori **Osoite:** Vapaudenkatu 58, 40100 Jyväskylä **Muut yhteystiedot:** puh. 0295 50 4000 (vaihde), kirjaamo@valtori.fi
2. Rekisterin yhteyshenkilö	**Nimi:** **Puhelin:** **Sähköposti:**
3. Valtorin tietosuojavastaavan yhteystiedot	**Nimi:** Aapo Immonen **Puhelin:** 0295 50 5029 **Sähköposti:** tietosuoja@valtori.fi
4. Rekisterin nimi	Anna henkilörekisterille nimi, joka ilmaisee rekisterin käyttötarkoituksen
5. Henkilötietojen käsittelyn tarkoitus	Kerro henkilötietojen käsittelyn tarkoitus, eli minkä rekisterinpitäjän tehtävän hoitamiseksi henkilörekisteri on perustettu (esim. asiakassuhteen, palvelussuhteen tai jäsenyyden hoitamiseksi). Jos henkilötietojen käsittely perustuu lainsäädäntöön, kerro se tässä.
6. Rekisterin tietosisältö	Merkitse ne tiedot tai tietotyypit, joita rekisteröidystä voidaan tallettaa. Henkilön yksilöintitiedot eritellään (esim. nimi, syntymäaika ja yhteystiedot). Muilta osin voi riittää tietotyyppien tai ryhmien kuvaus (esim. tiedot asiakkaan tilaamista palveluista, niiden toimittamisesta ja laskuttamisesta).
7. Säännönmukaiset tietolähteet	Kuvaus siitä, mistä rekisteriin talletettavat tiedot säännönmukaisesti saadaan. Tietoja voi kertyä rekisterinpitäjän omassa toiminnassa, niitä voidaan saada rekisteröidyltä itseltään tai luovutuksina muista henkilörekistereistä. Jos tietoja saadaan luovutuksena muualta, ilmoita millä perusteella luovutus tapahtuu (esim. rekisteröidyn suostumus tai lain säännös).
8. Tiedon säilytysaika	Kerro henkilötietojen säilytysaika ja kriteerit sen määräytymiselle (arkistonmuodostussuunnitelma, laki, asetus tms.)
9. Tietojen säännönmukaiset luovutukset	Jos tietoja luovutetaan säännönmukaisesti, kerro mitä tietoja luovutetaan ja kenelle, ja mihin luovuttaminen perustuu. Luovutuksen perusteena voi olla rekisteröidyn suostumus tai lain säännös.
10. Tietojen siirto EU:n tai ETA:n ulkopuolelle	Kerro, siirretäänkö tietoja EU:n tai ETA:n ulkopuolelle.

11. Rekisterin suojauksen periaatteet	**A. Manuaalinen aineisto** Jos rekisterissä syntyy manuaalista aineistoa, sen suojausta voidaan kuvata maininnalla säilytyksestä lukitussa tilassa. **B. ATK:lla käsiteltävät tiedot** ATK:lla käsiteltävien tietojen osalta ilmoitetaan, miten tiedot on suojattu organisaation ulkopuolisilta sekä miten niiden käyttöoikeudet on rajattu organisaation sisällä. Kerro yleisistä periaatteista, älä ilmoita tietoturvaa vaarantavia yksityiskohtia. Mainitse tässä, jos rekisteriin talletetut henkilötiedot on säädetty salassa pidettäviksi.
12. Rekisteröidyn oikeudet	**A. Oikeus saada pääsy tietoihin** EU 2016/679:n 15. artiklan mukaan rekisteröidyllä on oikeus saada pääsy häntä koskeviin henkilötietoihin. Pyyntö osoitetaan kohdassa 2 olevalle taholle. **B. Oikeus tehdä valitus valvontaviranomaiselle** EU 2016/679:n 77. artiklan mukaan rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle tietosuojavaltuutetun toimistoon jos hän katsoo, että henkilötietojen käsittelyssä rikotaan asetusta. **C. Oikeus vaatia tiedon korjaamista** EU 2016/679:n 16. artiklan mukaan rekisteröidyllä on oikeus vaatia rekisterissä olevan itseään koskevan virheellisen tiedon korjausta. Pyyntö osoitetaan kohdassa 2 olevalle taholle. **D. Oikeus poistaa tiedot** EU 2016/679:n 17. artiklan mukaan rekisteröidyllä on oikeus saada rekisterinpitäjä poistamaan rekisteröityä koskevat henkilötiedot ilman aiheetonta viivytystä. Pyyntö osoitetaan kohdassa 2 olevalle taholle. Oikeutta poistaa tiedot ei sovelleta lakisääteisissä rekistereissä. **E. Oikeus siirtää tiedot järjestelmästä toiseen** EU 2016/679:n 20. artiklan mukaan rekisteröidyllä on oikeus siirtää henkilötietonsa järjestelmästä toiseen, edellyttäen että käsittely perustuu suostumukseen tai sopimukseen, ja että se tehdään automaattisesti. Rekisteröidyllä on myös oikeus saada siirrettyä tietonsa suoraan rekisterinpitäjältä toiselle, mikäli se on teknisesti mahdollista. Pyyntö osoitetaan kohdassa 2 olevalle taholle. Oikeutta siirtää tiedot järjestelmästä toiseen ei sovelleta lakisääteisissä rekistereissä.

Rekisteröidyn oikeudet

Tietojenkäsittely on Valtorissa merkittävältä osin lakisääteistä. Valtorissa on luotu / luodaan prosessit

Miten rekisteröidyn tietoihin päästään

Miten rekisteröidyn tiedot oikaistaan

Miten rekisteröidyn tiedot siirretään järjestelmästä toiseen

Sekä huolehditaan rekisteröidyn oikeudesta vastustaa käsittelyä, automaattista päätöksentekoa ja profilointia

Oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta

- Rekisterinpitäjän on ilmoitettava rekisteröidylle hänen henkilötietoihinsa kohdistuneesta tietoturvaloukkauksesta jos loukkaus aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille
- Ilmoitus voidaan tehdä median välityksellä, jos yksittäisten ilmoitusten lähettäminen aiheuttaisi kohtuutonta vaivaa
- Ilmoitukseen on tulossa pohja:
  - Selkeä ja yksinkertainen kuvaus tapahtuneesta
  - Tietosuojavastaavan yhteystiedot, josta rekisteröity saa lisätietoja
  - Loukkauksen todennäköiset vaikutukset rekisteröidylle
  - Kuvaus toimenpiteistä, joilla haittavaikutuksia lievennetään ja tilanne ratkaistaan

Tärkeää

- Väärinkäytösten välttämiseksi rekisteröidyn henkilöllisyys on tunnistettava, kun hänen pyyntöjä toteutetaan
- Rekisteröidyn oikeuksiin liittyvät pyynnöt on toteutettava kuukauden sisällä niiden saapumisesta (mahdollisuutena kahden kuukauden jatkoaika)
- Tiedot toimitettava rekisteröidylle sähköisesti ja maksutta

Rekisterinpitäjän velvollisuudet

Yksityishenkilöt

Yhteistyökumppanit

Asiakkaat

Oma henkilöstö

Rekisterinpitäjän velvollisuudet 1/3

Käsittelyn oikeusperusta:
- Suostumus
- Sopimus
- Laki
- Etujen suojaaminen
- Julkinen valta

Tietosuojariskienhallinta:
- Riskilähtöinen lähestymistapa
- Riskiarvion kautta tietoturvakontrollit
- Tarvittaessa vaikutustenarvioinnit

Tietosuojan hallinnointi, roolit ja vastuut:
- Tietosuojavastaava
- Tietosuojaorganisaatio
- Tietosuojan vuosikello

Tietoturvallisuus:
- Henkilötiedot suojattava riskiarvion edellyttämin keinoin
- Luokittelupäätös
- Tiedon elinkaari

Rekisterinpitäjän velvollisuudet 2/3

Poikkeamien hallinta ja ilmoitusvelvollisuus:

- Koskee sekä rekisteröityjä että valvontaviranomaista
- 72h kuluessa havaitsemisesta
- Prosessimäärittely

Dokumentaatio, ohjeistukset ja politiikat:

- Tietosuojapolitiikka
- Ohjeistus sekä henkilöstölle että tietojenkäsittelijöille
- Dokumentoidaan kaikki

Sopimukset:

- Asiakkaat ja alihankkijat
- Valtori rekisterinpitäjänä sekä tietojen käsittelijänä
- Alihankkija tietojenkäsittelijänä tai asiakkaan alikäsittelijänä

Yhteistyövelvoite:

- Velvollisuus tehdä yhteistyötä valvontaviranomaisen kanssa
- Pyynnöstä, ennakkokuulemiset, tietoturvaloukkaukset

Rekisterinpitäjän velvollisuudet 3/3

Sisäänrakennettu ja oletusarvoinen tietosuoja:

- Tietosuojan huomioiminen mahdollisimman aikaisessa vaiheessa
- Järjestelmissä, sovelluksissa, hankinnoissa, projekteissa
- Tiedon elinkaaren huomiointi

Hallinnolliset sakot ja seuraamukset:

- Valvontaviranomaisella oikeus määrätä 20milj.€/ 4% liikevaihdosta
- Ei tule todennäköisesti koskemaan julkishallintoa

OSOITUSVELVOLLISUUS

- Rekisterinpitäjän pystyttävä osoittamaan, miten se on varmistanut velvollisuuksien toteutumisen teknisen, hallinnollisin ja organisatorisin keinoin

Tietojenkäsittelysopimus (TKS)

Valtori | Valtion tieto- ja viestintätekniikkakeskus

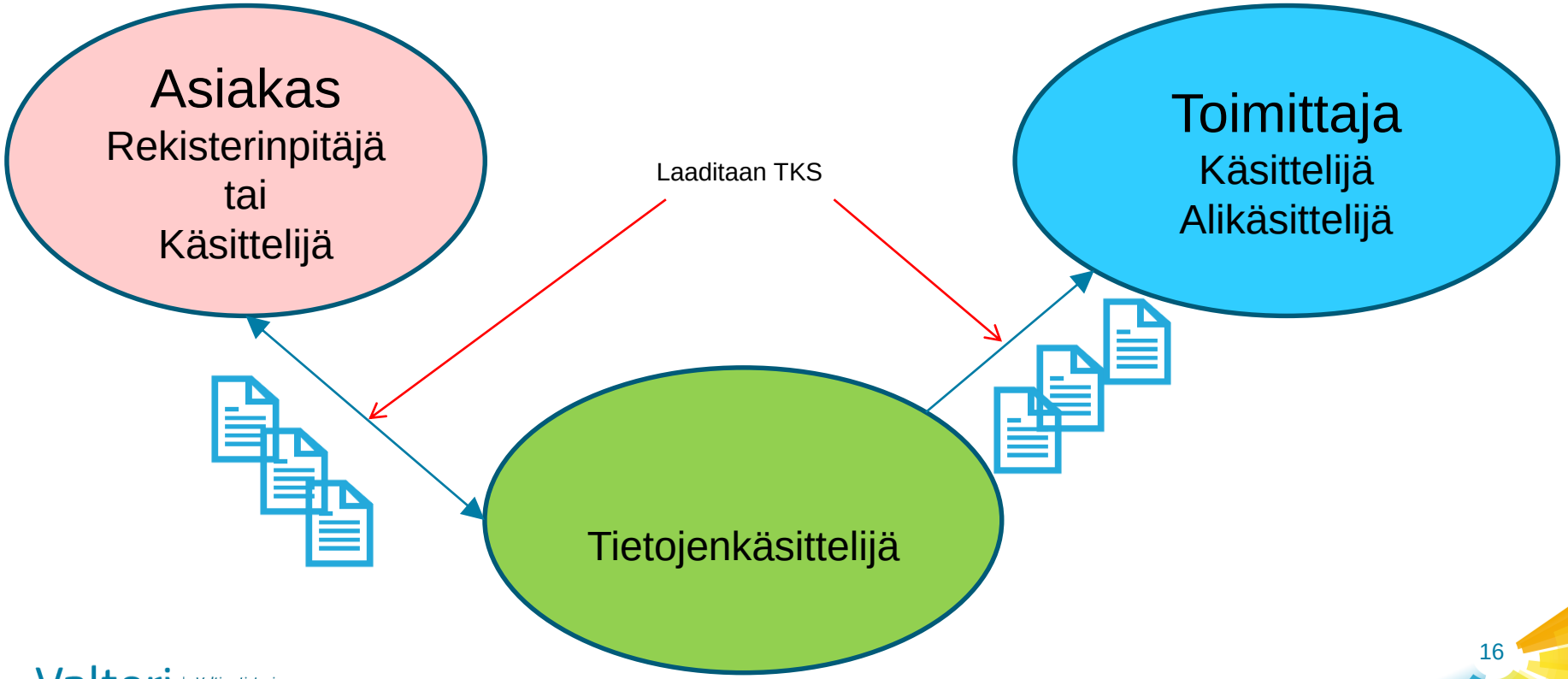
Kuka tekee sopimuksen ja kenen kanssa?

- Artiklan 28 mukaan ”Henkilötietojen käsittelijän suorittamaa käsittelyä on määritettävä sopimuksella”
  - Saa käyttää vain sellaista käsittelijää, joka toteuttaa riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi

- Vastaavasti Käsittelijän tulee tehdä TKS nk. Alikäsittelijän (=alihankkija, joka osin tai kokonaan vastaa Käsittelijän tehtävistä) kanssa
  - Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa

- Aloite sopimuksen tekemiselle pitäisi olla Rekisterinpitäjällä, mutta Valtorin kohdalla lienee parempi edetä joustavassa järjestyksessä

Sopiminen – ketkä, milloin, miksi



Mitä TKS:ssä sovitaan?

- Sopimuksessa vahvistetaan käsittelyn
  - kohde ja kesto,
  - käsittelyn luonne ja tarkoitus,
  - henkilötietojen tyyppi ja
  - rekisteröityjen ryhmät,
  - rekisterinpitäjän velvollisuudet ja oikeudet

Erityisesti tulee myös sopia, että Käsittelijät

- käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti
- ovat sitoutuneet noudattamaan salassapitovelvollisuutta
- auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata pyyntöihin

Riskiarvio

- Uuden asetuksen yksi keskeinen tavoite on proaktiivinen riskienarviointi, jolla korvataan jatkossa rekisteri- ja toimintailmoitukset tietosuojaviranomaisille.
- Valtorilla olemassa valmis lomakepohja.
- Käytetään arvioitaessa toimintaa sekä rekisterinpitäjän että tietojenkäsittelijän näkökulmista

Poikkeamista ilmoittaminen

- Tietosuojapoikkeamista ilmoittaminen
- Rekisterinpitäjä on yhteydessä tietosuojaviranomaiseen tarvittaessa.
- Tietojenkäsittelijä on yhteydessä tietosuojavastaavaan, joka on yhteydessä rekisterinpitäjään. Alihankkija on yhteydessä Valtorin tietosuojavastaavaan.
- Valtorissa kuvattu prosessina poikkeamien käsittely sekä rekisteröidyn että reksiterinpitäjän esittämät tietopyynnöt.

Dokumentointi, raportointi

- Dokumentoikaa kaikki mahdollinen alkaen sopimuksista prosesseihin.
- Raportointi tapahtuu esim. tietotilinpäätösraporteilla. Tietotilinpäätös:
    - antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta
    - kuvaa mitä tietovarantoja organisaation hallussa on
    - kuvaa organisaation toimintaan liittyvät tietovirrat
    - kuvaa organisaation tietovirtojen yhteentoimivuuden tietojenkäsittelyn kanssa
    - kuvaa miten tietosuoja ja -turva toteutuvat organisaation toiminnassa
    - kuvaa miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu
    - toimii suunnittelun ja toiminnan ohjauksen tukena organisaatiossa
    - toimii raportoinnin ja johtamisen tukena organisaatiossa
    - toimii kehittämistoimenpiteiden seurannan apuvälineenä
    - toimii organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä
    - varmistaa sovellettavan lainsäädännön noudattamisen