VAHTI / Sihteeristö

3.5.2021

Tietosuoja-asetuksen itsearviointi

Digiturvan hyvät käytännöt tukimateriaali

3.5.2021

Dokumentinhallinta

Omistaja	Digi- ja väestötietovirasto – Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI)
Laatinut	VAHTI-työryhmä 4 Tietosuojan kehittäminen
Tarkastanut	VAHTI-sihteeristö
Hyväksynyt	VAHTI-sihteeristö

Version hallinta

versionro	mitä tehty	pvm/henkilö
0.80	Luonnosversio	25.1.2021 TS
0.90	Luonnosversio	19.4.2021 KR
1.0	Julkaisuversio	3.5.2021 KR

Sisällysluettelo

Yleistä

Tämä asiakirja on tarkoitettu vapaasti hyödynnettäväksi ja sovellettavaksi tietosuojan itsearviointia edistävänä tukimateriaalina. Jokaisen organisaation tulee tarkistaa ja sovittaa tämä sen omaan toimintaan, sitä ei tule ottaa käyttöön sellaisenaan.

Toivomme, että annat palautetta tästä tukimateriaalista:

https://response.questback.com/dvv/digiturvahyvatkaytannotpalaute

Muut yhteydenotot koskien tätä tukimateriaalia:
digiturva@dvv.fi

1 Itsearviointi

1	**Onko tiedossa, millaisia henkilötietoja organisaatiosi käsittelee?**	**(arviointi)**
Tarkempi kuvaus	• Nimi, osoite, sähköpostiosoite, puhelinnumero jne. • Hetu (TsL 29 §) • Erityiset henkilötietoryhmät (TsA 9 art. TsL 6 §) • Rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot (TsA 10 art., TsL 7 §) • Turvakiellon alaiset henkilötiedot • Henkilöstön (TtsL), asiakkaiden, vierailijoiden, sidosryhmien henkilötiedot	
Miten osoitetaan	(Kerro, millä asiakirjoilla tai muulla dokumentaatiolla osoitat vaatimuksen toteutumisen. Jos mahdollista, lisää viittaus dokumentaatioon.)	
Vaatimuksen perusteet	• TsA 4 (1) art.	
Suunnitelma	(Tarvittavat toimenpiteet sekä niihin liittyvät vastuut, tehtävät ja aikataulut tai mistä ne löytyvät)	
2	**Onko henkilötietojen käsittelyn oikeusperusteet tunnistettu?**	

Tarkempi kuvaus	• TSA:n mukaiset perusteet
	  ○ suostumus
	  ○ sopimus
	  ○ lakisääteinen velvoite (edellyttää säännöksen yksilöintiä)
	  ○ elintärkeä etu
	  ○ yleinen etu ja julkinen valta (edellyttää säännösten yksilöintiä, yleisen edun yksilöintiä ja julkisen vallan säädösperustaa)
	  ○ oikeutettu etu
	• Onko käsittelyn erityisedellytykset huomioitu mm. seuraavissa tapauksissa?
	  ○ erityisiin henkilötietoryhmiin kuuluvien tietoen käsittelyperusteet
	  ○ rikostuomioihin ja rikkomuksiin liittyvä käsittely
	  ○ henkilötunnuksen käsittely
	  ○ henkilötietojen käsittely työsuhteen yhteydessä	

Miten osoitetaan		
Vaatimuksen perusteet	• TsA 6, 9 ja 10 art. • TsL 6 ja 29 § • TtsL 2, 3, 5 ja 6 luku	
Suunnitelma		

3	**Tunnistetaanko, milloin organisaatiosi toimii rekisterinpitäjänä ja milloin se toimii käsittelijänä?**	
Tarkempi kuvaus	• Onko olemassa prosessi tai ohjeistus roolin tunnistamiseksi?	
Miten osoitetaan		
Vaatimuksen perusteet	• TsA 4 art. 7-8 kohta	
Suunnitelma		
4	**Onko sopimukset henkilötietojen käsittelystä tehty ja sopimusten hallinta kunnossa?**	
Tarkempi kuvaus	• Onko tietosuoja sisäänrakennettu hankintaprosessiin? • Onko henkilötietojen käsittelyn vaatimukset ja ehdot huomioitu henkilötietojen käsittelijöiden kanssa tehdyissä sopimuksissa? • Onko sopimusten hallintamalli laadittu? • Onko siirrot 3. maihin otettu huomioon?	
Miten osoitetaan		
Vaatimuksen perusteet	• TsA 28 art.	
Suunnitelma		
5	**Tunnistetaanko yhteisrekisterinpitäjyystilanteet ja onko yhteisrekisterinpitäjyyttä koskevista vastuista sovittu?**	
Tarkempi kuvaus	• Tunnistetaanko tilanteet, joissa on kyse yhteisrekisterinpitäjyydestä? • Onko yhteisrekisterinpitäjien vastuunjaosta sovittu tiedon keräämisestä sen hävittämiseen/arkistointiin? • Ovatko roolit ja vastuut selkeitä ja läpinäkyviä rekisteröidyille?	
Miten osoitetaan	• ohje tai prosessi, joka auttaa tunnistamaan yhteisrekisterinpitäjyyden ja siihen liittyvät roolit • sopimukset • viestintä rooleista ja vastuunjaosta rekisteröidylle	
Vaatimuksen perusteet	• TsA 26 art. • huom. myös EDPB:n ohje	
Suunnitelma		
6	**Onko henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu?**	
Tarkempi kuvaus	• rekisterien omistajat / vastuuhenkilöt • johdon vastuut • esimiehet	

	• henkilöstö • valvonta • tietosuojavastaava • muut roolit (tiedonhallinta, tietosuoja, tietoturva, riskienhallinta, tilaturvallisuus)	
Miten osoitetaan		
Vaatimuksen perusteet	• TihL 4.2 § • TsA 37 art.	
Suunnitelma		
7	**Onko tietosuojavastaavan asema ja rooli määritelty?**	
Tarkempi kuvaus	• tarve tietosuojavastaavan nimeämiseen on selvitetty • Tietosuojavastaavan sijaisjärjestelyt kunnossa, yhteydenotot poissaolon aikana • tietosuojavastaavan tehtävät ja asema ovat laissa säädetyn mukaiset	
Miten osoitetaan	• päätös tietosuojavastaavan nimeämisestä • esim. asema määritelty hallintosäännössä, työjärjestyksessä tms. • tehtävänkuvaus	
Vaatimuksen perusteet	• TsA 37 – 39 art.	
Suunnitelma		
8	**Onko seloste käsittelytoimista laadittu?**	
Tarkempi kuvaus	• Sisältääkö vaaditut tiedot?	
Miten osoitetaan		
Vaatimuksen perusteet	• TsA 30 art.	
Suunnitelma		
9	**Toteutuvatko tietosuojaperiaatteet organisaatiosi toiminnassa?**	
Tarkempi kuvaus	• lainmukaisuus, kohtuullisuus, läpinäkyvyys • käyttötarkoitussidonnaisuus • tietojen minimointi • täsmällisyys • säilytyksen rajoittaminen • eheys ja luottamuksellisuus	
Miten osoitetaan		

Vaatimuksen perusteet	• TsA 5 art.	
Suunnitelma		
10	**Onko tiedossa, missä tietojärjestelmissä käsittelette henkilötietoja?**	
Tarkempi kuvaus	• tietojärjestelmäsalkku/rekisteri • tietovirtakuvaukset • aputiedostot/listaukset	
Miten osoitetaan		
Vaatimuksen perusteet		
Suunnitelma		
11	**Tunnistetaanko rakenteeton tieto ja miten sitä hallitaan?**	
Tarkempi kuvaus	• satunnaisten, ei-jäsenneltyjen sähköisten tietojen tunnistaminen ja hallinta • Tietoa käsitellään sellaisissa ympäristöissä, joissa tiedon elinkaarta ei pystytä metatietojen avulla hallitsemaan. • esim. sähköpostiviestit, verkkolevyllä olevat tiedostot, Teams-tiimien tiedostot, Skype-/Teams-keskusteluhistoria	
Miten osoitetaan		
Vaatimuksen perusteet		
Suunnitelma		
12	**Onko informointikäytännöt määritelty ja noudatetaanko niitä?**	
Tarkempi kuvaus	• Otetaan huomioon informoinnin kohderyhmä sekä käsittelyn laajuus ja luonne valittaessa informointikäytäntöä. • Pystyttävä osoittamaan, että rekisteröity on saanut informaation • Onko informaatio ymmärrettävää ja saavutettavaa?	
Miten osoitetaan		
Vaatimuksen perusteet	• TsA 12 – 14 art. • Digipalvelulaki	
Suunnitelma		
13	**Onko olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi?**	
Tarkempi kuvaus	• Onko tunnistettu, milloin tullee suorittaa vaikutustenarviointi tai ennakkokuuleminen?	

	• Onko vakioitu prosessi kriteerien tunnistamiseksi olemassa?	
Miten osoitetaan	• kuvaus prosessista	
Vaatimuksen perusteet	• TsA 35 (1) art.	
Suunnitelma		
14	**Onko olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi?**	

Tarkempi kuvaus	• Onko olemassa vakioitu prosessi loukkausten käsittelemiseksi ja dokumentoimiseksi?
	  ○ ilmoituskanavan määrittäminen ja vastuuhenkilöt ilmoitusten käsittelyyn
	  ○ viranomaisilmoitusten tekeminen, päätöksentekovastuu ilmoituksista
	  ○ rekisteröidyille ilmoittaminen
	• Miten varmistetaan henkilöstön kyvykkyys tunnistaa tietoturvaloukkauksia?	

Miten osoitetaan	• kuvaus prosessista	
Vaatimuksen perusteet	• TsA 33 ja 34 art.	
Suunnitelma		
15	**Jos henkilötietoja siirretään kolmansiin maihin, onko siirron edellytykset selvitetty?**	
Tarkempi kuvaus	• Onko ymmärretty, mitä tarkoitetaan siirrolla kolmansiin maihin (esim. pääsy tietoihin kolmannesta maasta)? • Onko tunnistettu ne tilanteet, joissa tapahtuu siirtoja kolmansiin maihin? • Onko vaatimusmäärittelyssä huomioitu ne tilanteet, joissa siirrot kolmansiin maihin eivät ole mahdollisia? • Onko huomioitu siirrot kolmansiin maihin koko alihankintaketjussa?	
Miten osoitetaan	• sopimusten kolmansiin maihin siirtoja koskevat ehdot	
Vaatimuksen perusteet	• TsA 5 luku	
Suunnitelma		
16	**Onko olemassa tarvittavat sisäiset ja ulkoiset ohjeet koskien tietosuojaa ja tietoturvallisuutta?**	
Tarkempi kuvaus	• toimitilojen tietoturvallisuutta koskevat ohjeet (esimerkiksi henkilöstön ja vieraiden liikkuminen toimitiloissa)	

	• tietoaineistojen käsittelyohjeet sisältäen esimerkiksi ohjeet henkilötietojen ja salassa pidettävien tietojen käsittelystä eri palveluissa
	• Onko tarvittava ohjeistus olemassa? Esimerkiksi:
	  ○ rekisteröityjen oikeuksien toteuttaminen
	  ○ tietosuojaperiaatteet
	• Onko ohjeistus ja prosessit jalkautettu ja miten se pystytään osoittamaan?	

Miten osoitetaan	• hyväksytyt, kirjalliset ohjeet • prosessikuvaukset	
Vaatimuksen perusteet	• TsA 32 art. • TihL 4.2 § 2 k	
Suunnitelma		
17	**Onko huolehdittu henkilöstön osaamisen ylläpitämisestä tietosuojan ja tietoturvallisuuden osalta?**	
Tarkempi kuvaus	• Onko tietosuoja huomioitu henkilöstön kouluttamisessa ja perehdytyksessä järjestetty? • Onko otettu huomioon eri rooleihin ja työtehtäviin liittyvät erityistarpeet? • Onko osaamisen ylläpitäminen säännönmukaista toimintaa?	
Miten osoitetaan	• koulutussuunnitelma • koulutus- ja perehdytysmateriaalit	
Vaatimuksen perusteet	• TsA 32 (4) art. • TihL 4.2 § 3 k	
Suunnitelma		
18	**Ovatko edellä olevat kohdat muuttuneet toiminnaksi, kulttuuriksi ja asenteeksi organisaatiossasi?**	
Tarkempi kuvaus	• Mieti, miten kykenet arvioimaan toiminnan, kulttuuri ja asenteen muuttumista organisaatiossasi. • esim. johdolle ja henkilöstölle kohdennetut kyselytutkimukset	
Miten osoitetaan	• palvelulupaus tietosuojan huomioonottamisesta organisaation toiminnassa • tietosuojapolitiikka • vuosikello • osaamisen mittaaminen	
Vaatimuksen perusteet	• TsA 5 (2) art.	
Suunnitelma		