Tietosuoja-asetuksen 39 artikla

Tehtävä	Toteutustapa	Aikataulutus
Organisaation neuvonta ja ohjaus kaikissa tietosuojakysymyksissä	Sisäisesti ja ulkoisesti (henkilötiedon käsittelijät, rekisteröidyt)	Jatkuva Aloita heti: riskin mukaan vaiheistettu Tehoisku ennen toukokuuta 2018
	Kokonaisvaltainen suunnitelma: tee roadmap	
	Ohjeistus, sparraus ja konsultointi	
	Koulutus (tarvittaessa ulkopuoliset)	
	Hanki myös itse koulutusta säännöllisesti	
	UKK-dokumentin tekeminen	
	Verkkokoulutusohjelma testeineen	
	Blogi/muu sisäinen viestintä	
Asetuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa (ml. vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset)	Jatkuva hallintamalli	Aloita heti, jatkuva toiminta
	Workshopit liiketoimintojen kanssa: teoriaa ja käytännön harjoituksia oikeilla caseilla	
	Huomioi myös muu lainsäädäntö kuin tietosuoja-asetus (sähköinen viestintä, työntekijöiden tietosuoja, kansallinen uusi tietosuojalaki)	
	Tietosuojalausekkeiden ja sopimusliitteiden läpikäynti (niin omat B2C/B2B kuin sopimukset käsittelijän kanssa)	
Vaikutustenarviointien tekemisen tukeminen ja valvonta	Osallistuu suunnitteluun ja toteutukseen	Jatkuva, 1-2 kertaa vuodessa kokonaisvaltainen arviointi
	Riskien tunnistaminen ja priorisointi	
	Projektimalli ja jatkuvuuden varmistaminen	
	Ulkopuolisen auditoijan käyttö mahdollista	
	Hyötyjen ja riskien identifiointi	
	Gap-analyysi	
Yhteistyö valvontaviranomaisen kanssa ja yhteyspisteenä toiminen	Alakohtaiset tapaamiset	Jatkuva
	Yhteistyö oman alan sisällä	
Dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta	Keskitetty tietokanta	Jatkuva Aloita heti: riskin mukaan vaiheistettu Tehoisku ennen toukokuuta 2018
	Aikataulutetusti (vuosikello)	
	Ohjeistus ja prosessien määrittely	
	Mallipohjien luominen	
	Varmista henkilötietojen käsittelyperuste	
	Datavirtojen kartoitus ja seuranta	

Ilmoitusvelvollisuuden toteutumisen seuranta (tietoturvaloukkaukset)	Pitää olla prosessi: sopimuksissa, dokumentointi, jälkitoimet ym.	Valmius: 72h havaitsemisesta ilmoitus
	Harjoittelu	
	Tietoisuus ja päätös	
	Koulutusta siitä, mikä on tietoturvaloukkaus	
	Mallipohjien luominen	
Osoitusvelvollisuuden toteutumisen seuranta	Jatkuva hallintamalli: varmista käsittelyn lainmukaisuus ja käsittelyn yleisten periaatteiden noudattaminen	Jatkuva
	Prosessien business owner	
	Organisaatiossa säännöllisesti testejä: tietosuoja-asioiden pysyttävä mielessä	
	Sisäinen auditointi, ”mystery shopping” -toiminta	
	Asiakkaiden palautteen kysyminen	
Tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle	Tietosuojatilinpäätöksen suunnittelu ja toteutus	Vuosikello Täsmäiskuja/sisäisiä tarkastuksia säännöllisesti
	Jatkuvuuden varmistaminen	
	Itseopiskelu mahdollisuuksia henkilöstölle ja verkkotestit	
	Ohjaus, koulutus ja täsmäiskut	
	Osaksi perehdytysohjelmaa	
	Tietosuojapolitiikan luominen organisaatioon	
	Johdon sitouttaminen	
Rekisteröityjen oikeuksien toteuttamisen tukeminen	Prosessien määritys	Heti järjestelmien osalta, kriittiset osat valmiina viimeistään toukokuussa 2018 Asiakasrajapinnan osalta jatkuva koulutus
	Järjestelmien automatisointi	
	Käy läpi tietojen suojaukset tavat organisaatiossa	
	Palvelullistaminen ja itsepalvelun lisääminen	
	Asiakaspalvelun koulutus ja asiakasrajapinnan riittävä ymmärrys	
	Rekisteriseloste (päivitettävä nykyinen)	

	Suostumusten keruu	
	Suostumuksen perumisen prosessi	
	Säilytysaikojen kartoitus ja määrittely	
	Sertifikaatit ja logot: hankkiminen ja viestintä niistä asiakkaille	
	Eri tasoja: eri käyttäjillä eri toiveet - palvele kaikkia	
	Ulkoinen viestintä	
	(Laajemmin yhteiskunnallinen kysymys: esimerkiksi informaatio-oikeutta osaksi yleistä koulutusta)	
Käsittelytoimiin liittyvän riskin asianmukainen huomiointi tehtävien suorittamisessa	Ml. kumppanisopimukset ja alihankkijat. Käy läpi sopimukset ja sopimusliitteet	Jatkuva
	Rekisteripitäjän ja käsittelijän väliset sopimukset kuntoon	
	Riskikartoitukset ja riskilähtöinen arviointi	
	Katastrofisuunnitelma	
	Liiketoiminnan ymmärtäminen tarpeellista	
Lainsäädännön ja käytännön seuranta	Itse	Jatkuva
	Yhteistyötä oman alan sisällä	
	Viranomaisten sivut ja tilaisuudet	
Sisäinen raportointi johdolle	Tietosuojatilinpäätös	Jatkuva seuranta Raportointi johdolle kvartaaleittain
	”Datatase”: jatkuvasti päivittyvä	
Toimiminen organisaation oikean tietosuoja-asenteen rakentajana sekä toimiminen tietosuojan kasvoina organisaatiossa	Näkyvyys	Jatkuva
	Jatkuvuuden hallinta	
	Saavutettavuus	
	Palvelualttius	
Lokipyynnöt ja käytönvalvonta	Eri tietosuoja- ja tietoturvalokit	Jatkuva

Digitaalisen liiketoiminnan tietosuojafoorumi 6.10.2017, osallistujien työpajavastausten koonti

Mitä ei tulisi kuulua tietosuojavastaavan tehtäviin?

- Päätöksenteko riskipäätöksissä
- Syntipukkina toiminen: johto ei voi ulkoistaa rekisterinpitäjän vastuutaan
- Toiminen yksin
- Laajasti muita tehtäviä: jätettävä aikaa toimia tietosuojavastaavana
- Muut tehtävät eivät saa aiheuttaa eturistiriitoja

Mistä tunnistan hyvän tietosuojavastaavan tai -palvelun?

- Asiantunteva niin lainsäädännön, yrityksen liiketoiminnan kuin teknologian (privacy by design) osalta
- Innostava, ratkaisukeskeinen ja osaa antaa vaihtoehtoja. ”Sisäinen myyjä”: ½ konsultti, ½ myyjä. Psykologi: antaa myös tukea
- Pitkäjänteinen, sosiaalinen, näkyvä. Periksiantamaton: jaksaa selittää, kunnes kaikki ymmärtävät
- Riippumaton, auktoriteetti. Toisaalta nöyryys oppia uutta
- Käytännönläheinen ja vastuullinen. Ei asettele vastakkain: kyky keskustella ja tuoda yhteen pöytään
- Kyky kuunnella ja vuorovaikutustaidot: pystyy kommunikoimaan kaikkien toimintojen kanssa
- Aktiivinen rooli: huolehtii ohjeistuksen viemisestä teoriasta käytäntöön
- Tervettä järkeä ja systematisuutta. Strategisti. Liiketoiminnan mahdollistaja. Osaa arvioida riskejä
- Hallitsee projektien johtamisen
- Verkostoituu sisäisesti ja ulkoisesti

Jos ostopalvelu:

- Ymmärtää toimialan
- Osaa kouluttaa ja kartoittaa tietovirtoja
- Kansainvälisyys jos on kansainvälinen organisaatio
- Asiakaslähtöisyys
- Skaalautuvuus
- Sertifikaatit

Mitä tietosuojavastaava tarvitsee onnistuakseen työssään?

- Organisaation ja erityisesti johdon selkeä tuki: ilmapiiri, jossa häntä kuunnellaan. Oltava valtaa.
- Jatkuva dialogi johdon kanssa ja johdon sitoutuneisuus

Digitaalisen liiketoiminnan tietosuojafoorumi 6.10.2017, osallistujien työpajavastausten koonti

- Riippumattomuus. Selkeät vastuut organisaatiossa

- Yrityksellä oltava datastrategia
- Säännöllinen koulutus
- Aikaa ja riittävät resurssit: tiimi suhteutettava työn määrään
- Työkalut ja riittävät toimivaltuudet. Tuki teknisissä kysymyksissä
- Sisäinen ja ulkoinen verkosto
- Palkitsemisohjelma