Pro Tietosuojan tarkistuslista

Tarkistakaa tämän listan avulla, oletteko tehneet tietosuoja-asetuksen edellyttämät toimet organisaatiossanne!

1. Rekisteri- tai tietosuojaseloste tehty ☐

2. Käyty läpi käytetyt palvelut ja järjestelmät sekä tiedusteltu niiden toimittajilta, toimivatko ne ja toimittajat itse GDPR:n mukaisesti. ☐

3. Kartoitettu käsiteltävät henkilötiedot, jotta tiedetään missä kaikkialla ja missä muodossa niitä on. Organisaation oman henkilöstön sekä ulkopuolisten tietoja on yllättävän monessa paikassa - niin sähköisessä muodossa kuin perinteisesti paperilla. ☐

4. Tuhottu kaikki vanhat ja tarpeettomat henkilötiedot asetuksen edellyttämällä tavalla. ☐

5. Arvioitu, kuinka asetuksen tarkoittamalla tavalla kriittisiä käsiteltävät tiedot ovat, sekä selvitetty voidaanko niitä käsitellä laillisesti. ☐

6. Mietitty käyttö- ja pääsyoikeuksien, niin fyysisen kuin digitaalisen, myöntämisen rutiinit ja ohjeistus. ☐

7. Mietitty oletteko henkilörekisterin (tai sen osan) osalta rekisterinpitäjiä vai käsittelijöitä. ☐

8. Tehty kartoitusten, selvitysten ja mietinnän jälkeen asetuksen velvoittama konkreettinen, teidän oma dokumentaationne siitä, että henkilötietoja käsitellään ja tallennetaan asetuksen mukaisesti (osoitusvelvollisuus). Jo alkumetreillä on syytä muistaa, että tätä dokumentaatiota on päivitettävä myös tulevaisuudessa (käytännössä jatkuvasti). ☐

9. Tarkistettu henkilötietojen tietoturvallinen käsittely (ml. säilytys) sekä sen koulutus ja ohjeistus henkilöstölle. Henkilötiedot tulee turvata sekä tietomurron, varkauden kuin myös tahattoman tuhoutumisen estämiseksi! ☐

10. Tehty henkilötietojen käsittelyn riskien arviointi (sekä tietosuoja että tietoturva). ☐

11. Huolehdittu koko henkilöstön asianmukaisesta koulutuksesta heti ja myös jatkossa, jotta he voivat toimia asetuksen vaatimusten ja teidän omien ohjeidenne mukaisesti. Vastuu on työnantajalla! ☐

12. Varauduttu tietojen näyttämiseen ja tuhoamiseen niitä pyydettäessä sekä todentamaan rekisteröidyn henkilöllisyys ennen pyyntöjen toteuttamista. ☐

13. Varauduttu myös asiattomiin henkilötietojen kyselyihin ja ilkivaltaan. ☐

14. Huolehdittu asianmukaisesta ohjeistuksesta henkilötietoja siirrettäessä. Esimerkiksi sähköpostin tai rekisteritulosteiden käyttöä on syytä harkita tarkasti, sillä ne eivät ole ongelmattomia. ☐

15. Valmistauduttu ongelmatilanteisiin hyvissä ajoin, koska kiireessä ja ns. ”tilanne päällä” se voi olla vaikeaa, merkittävästi kalliimpaa tai jopa mahdotonta. Tehkää hyvä ohjeistus toimenpiteistä valmiiksi. ☐

16. Tarjottu hyvä tapa poikkeamailmoituksen tekemiseksi koko henkilöstölle tietoturvaloukkauksen tapahtuessa tai sitä epäiltäessä. Poikkeamailmoitus voi olla myös positiivinen tai muuten merkittävä havainto. ☐

17. Tarkistettu olemassa olevien sopimusten ja käytänteiden asetuksenmukaisuus kumppaneiden ja pää-/aliurakoitsijoiden sekä esim. tilitoimiston, mainostoimiston tai muun palveluntarjoajan kanssa. ☐

pro tietosuoja