B 5.1 TIETOTURVAOHJE (24.01.2019, muut. 16.1.2020)

Suomen Asianajajaliiton valtuuskunta on 24.1.2019 antanut asianajotoimintaan liittyvästä tietoturvasta seuraavan ohjeen, joka tulee voimaan 1.6.2019. Valtuuskunnan 16.1.2020 hyväksymät muutokset tulevat voimaan 1.2.2020.

Asianajajan on huolehdittava, että

1. Hänen oma ja toimiston henkilökunnan tietoturvaa koskeva osaaminen on riittävän korkealla tasolla siten, että tätä ohjetta ja tietoturvaopasta (B 5.2) voidaan soveltaa toiminnan järjestämisessä. Vähintään 10 työntekijän asianajotoimiston on järjestettävä ulkoinen tietoturva-auditointi säännöllisin väliajoin.

2. Asianajotoimistoon tai asianajotoimintaan ei toteuteta sellaisia tarkastuksia tai tietopyyntöjä, joihin sisältyy asianajotoiminnan järjestämistä, asiakkuuksia tai toimeksiantoja koskevien tietojen keräämistä tai luovuttamista asiakkaille, palveluntarjoajille tai muille ulkopuolisille osapuolille. (16.1.2020, voimaan 1.2.2020)

3. Käytössä olevat fyysiset toimitilat ovat lukitut ja muutoinkin suojatut. Kaikki asianajajasalaisuuden piirin kuuluva aineisto, riippumatta siitä, miten tieto on tallennettu tai säilytetty, on suojattu.

4. Asianajotoiminnassa käytettävien laitteiden ja välineiden tiedot on salattu (kryptattu). Näitä laitteita ja välineitä ei saa antaa ulkopuolisten käyttöön. Asianajosalaisuuden säilyttämiseksi tulee välttää vieraiden laitteiden käyttöä tai niiden kytkemistä omiin laitteisiin. Laitteiden elinkaarista on huolehdittava siten, että laitteet, joihin ei enää tarjota päivityksiä, poistetaan käytöstä ja vaihdetaan uusiin.

5. Toimiston tai asianajajan laitteissaan käyttämät langattomat verkot on suojattu. Toimiston vierailijoilla ei tule olla pääsyä toimiston sisäiseen verkkoon (vieraille on järjestetty esimerkiksi oma langaton verkko). Käytettäessä julkisia verkkoja on käytettävä salattua yhteyttä (vpn tai vastaava).

6. Käytettävät salasanat ovat riittävän monimutkaisia, ne vaihdetaan tarpeeksi usein ja huolehditaan, etteivät muut pääse niihin käsiksi. Lisätunnistautumismenetelmiä käytetään mahdollisuuksien mukaan korkeamman tietoturvatason saavuttamiseksi.

7. Tietoturvaohjelmistot ja palomuuri ovat kunnossa. Laitteiden, käyttöjärjestelmien, ohjelmien ja sovellusten päivitykset asennetaan ilman aiheetonta viivästystä.

8. Asiakirjoihin tulee olla pääsy vain niillä henkilöillä, jotka tarvitsevat tai saattavat tarvita salassa pidettäviä tietoja tai ainakin pääsyä kyseisiin tiedostoihin työtehtäviensä hoitamiseksi.

9. Varmuuskopiointi tehdään säännöllisesti. Varmuuskopioita sisältävät laitteet ja mediat on salattu ja huolellisesti säilytetty. Varmuuskopioiden säännöllisestä testaamisesta huolehditaan.

10. Kaikkien ulkopuolisten palveluntarjoajien kanssa tehtävät sopimukset täyttävät tietoturvavaatimukset, ts. sisältävät etenkin salassapitoa koskevat ehdot (erityisesti ulkoistetut it-palvelut, toimitiloihin pääsevät tahot).

11. Kaikki sähköpostilla tai muulla sähköisellä tavalla lähetettävä aineisto on tarvittaessa salattu. Asianajajan on huolehdittava aineiston salaamisesta, jos sisältö on erityisen sensitiivistä tai asiakas edellyttää salattua liikennettä, sekä tarvittaessa ohjeistettava asiakastaan toimittamaan aineisto suojatulla menetelmällä.

12. Asiakirjat ja muu aineisto tallennetaan, säilytetään, arkistoidaan ja tuhotaan tietoturvallisella tavalla.

13. Kaikki tietoa sisältävät laitteet poistetaan käytöstä ja tyhjennetään tietoturvallisella tavalla (*tietokoneet, mobiililaitteet, tallennusvälineet jne)*. Sama koskee käytössä olevia tallennus- ja verkkopalveluita.

14. Toiminnan jatkuvuudesta on huolehdittu siten, että toimiston jatkuvuuden kannalta tarvittavat tiedot on kootusti dokumentoitu ja tämä dokumentointi on jatkuvuudesta huolehtivien tahojen saatavilla.