B 05.1 TIETOTURVAOHJE (24.1.2019, muut. 16.1.2020 ja 9.6.2023)

Suomen Asianajajaliiton valtuuskunta on 24.1.2019 antanut asianajotoimintaan liittyvästä tietoturvasta seuraavan ohjeen, joka tulee voimaan 1.6.2019. Valtuuskunnan 9.6.2023 hyväksymät muutokset tulevat voimaan 1.1.2024.

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. Henkilöiden osaaminen on varmistettu siihen suunnitellulla koulutuksella. Koulutuksesta on pyynnöstä esitettävä selvitys kuten täydennyskoulutuksesta (B 9). *(9.6.2023, voimaan 1.1.2024)*

2. Vähintään 10 työntekijän asianajotoimistolla on tietoturvapolitiikka, joka on toimiston ylimmän johdon hyväksymä. *(9.6.2023, voimaan 1.1.2024)*

3. Vähintään 10 työntekijän asianajotoimiston on järjestettävä ulkoinen tietoturva-auditointi säännöllisin väliajoin. Lisäksi auditointi tulee suorittaa, mikäli tietoturva- tai toimistoympäristöön taikka keskeisiin järjestelmiin toteutetaan muutoksia. Auditoinneista on pidettävä kirjaa. *(9.6.2023, voimaan 1.1.2024)*

4. 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)

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

6. Asianajotoiminnassa käytettävät ohjelmistot ja palvelut ovat tarkoitettu yrityskäyttöön. Muita palveluita voidaan käyttää vain asiakkaan suostumuksella. *(9.6.2023, voimaan 1.1.2024)*

7. Vähintään 10 työntekijän asianajotoimistossa asianajotoiminnassa käytettävät laitteet on oltava laitehallinnan piirissä. Lisäksi on otettava käyttöön pääsynhallintaratkaisu. *(9.6.2023, voimaan 1.1.2024)*

8. Asianajotoiminnassa käytettävien laitteiden ja välineiden tiedot on salattu (kryptattu). Asiakastietoja kokoavat taulukot, tietokannat ja pilvipalvelut on myös suojattava salauksella. Asianajotoiminnassa käytettäviä 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. *(9.6.2023, voimaan 1.1.2024)*

9. 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).

10. Käytettävät salasanat ovat riittävän pitkiä ja monimutkaisia, ne vaihdetaan tarpeen vaatiessa ja huolehditaan, etteivät muut pääse niihin käsiksi. Lisätunnistautumismenetelmiä käytetään mahdollisuuksien mukaan korkeamman tietoturvatason saavuttamiseksi. *(9.6.2023, voimaan 1.1.2024)*

11. Tietoturvaohjelmistot ja palomuuri ovat kunnossa. Tietoturvaohjelmistojen ja järjestelmänvalvojien käyttäjätunnuksien myöntämistä on rajoitettu toimenkuvan ja osaamisen mukaan eikä järjestelmänvalvojan käyttäjätunnuksia käytetä päivittäisessä käytössä. Laitteiden, käyttöjärjestelmien, ohjelmien ja sovellusten päivitykset asennetaan ilman aiheetonta viivästystä. *(9.6.2023, voimaan 1.1.2024)*

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

13. Varmuuskopiointi tehdään säännöllisesti ja sen tarpeenmukaisuus perustuu toimistossa tehtyyn arvioon tietojen menettämisestä aiheutuvista seurauksista. Varmuuskopioinnista on huolehdittu myös pilvipalvelujen osalta. Varmuuskopioita sisältävät laitteet ja mediat on salattu ja huolellisesti säilytetty. Varmuuskopioiden säännöllisestä testaamisesta huolehditaan*. (9.6.2023, voimaan 1.1.2024)*

14. Kaikkien ulkopuolisten palveluntarjoajien kanssa tehtävät sopimukset täyttävät tietoturvavaatimukset, ts. sisältävät etenkin salassapitoa koskevat ehdot (erityisesti ulkoistetut it-palvelut, toimitiloihin pääsevät tahot) ja pääsyoikeuksia koskevat ehdot, niiden rajaamisesta tarkoituksenmukaiselle tasolle ja ajantasaisuuden säännöllisestä tarkastamisesta. Tietojen tuhoamisesta ja siirrettävyydestä toiseen palveluun on tarvittaessa sovittu. *(9.6.2023, voimaan 1.1.2024)*

15. Asianajotoiminnassa käytettävien sähköisten viestintäkanavien turvallisuus vastaa viestityn tiedon vaatimaa tasoa. Toimistossa on määritetty viestintäkanavat salassa pidettävään viestintään. 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*. (9.6.2023, voimaan 1.1.2024)*

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

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

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

Muutokset ja voimaantulo:

Valtuuskunnan 9.6.2023 hyväksymät muutokset tulevat voimaan 1.1.2024.

Valtuuskunnan 16.1.2020 hyväksymät muutokset tulevat voimaan 1.2.2020.