B 05.2 TIETOTURVAOPAS (23.11.2018, päivitetty 12.12.2019, 24.9.2021, 14.12.2023 ja 19.4.2024)

Suomen Asianajajaliiton hallitus on 23.11.2018 antanut seuraavan oppaan asianajotoimintaan liittyvästä tietoturvasta. Hallitus on hyväksynyt päivityksiä oppaaseen 12.12.2019 (kohdat 1 ja 2), 24.9.2021 (liitteet 1 ja 2), 14.12.2023 (kohdat Taustaksi, 1–3, 6–8, 10, 11, 13–15 sekä liitteet 3 ja 4) ja 19.4.2024 (lisäys kohtaan Taustaksi, muutos kohtaan 15.3 ja uusi liite 5). Tämä opas on voimassa 1.6.2024 lukien.

Taustaksi (14.12.2023)

Asianajajilla on asianajosalaisuudeksi kutsuttu laaja yleinen salassapitovelvollisuus asiakkaansa asioista ja tehtävässään saamistaan tiedoista. Asianajajien tulee huolehtia asianajosalaisuuden turvaamisesta, sillä se on asianajajan asiakkaan perusoikeus, joka perustuu muun muassa Euroopan ihmisoikeussopimuksen oikeudenmukaista oikeudenkäyntiä koskevaan 6 artiklaan sekä yksityis- ja perhe-elämän kunnioitusta suojaavaan 8 artiklaan. Asianajosalaisuuden sisällöstä on Suomessa säädetty muun muassa asianajajista annetussa laissa (AAL 5 c §) ja asianajajia velvoittavissa tapaohjeissa (TO 3.4 ja 4.3). Suomen lainsäädännössä asianajosalaisuuden rikkominen on rikosoikeudellisesti sanktioitu.

Asianajotoiminnassa käsitellään suuria määriä luottamuksellista asianajosalaisuuden ja muiden salassapitovelvollisuuksien, kuten liikesalaisuuden alaista, tietoa. Asianajajalla on tapaohjeiden kohdan 11.6 mukaan velvollisuus huolehtia toimiston tietoturvallisuudesta siten, etteivät sivulliset pääse luvatta käsiksi asiakkaiden luottamuksellisiin tietoihin. Tietoturvavelvoitteiden täsmentämiseksi valtuuskunta on hyväksynyt asianajajia velvoittavan tietoturvaohjeen (B 05.1, 24.1.2019, muut. 16.1.2020 ja 9.6.2023, voimassa 1.1.2024 alkaen).

Tietoturvan merkitys korostuu entisestään, kun suurin osa asianajotoimintaan liittyvästä aineistosta ja viestinnästä on siirtynyt sähköiseksi, prosessit digitalisoituvat, tekoälyn käyttö lisää luottamuksellisen datan käsittelyyn liittyviä riskejä ja alaa koskevien tietoturvahyökkäysten riski on kasvanut.

Tietoturvallisuudella tarkoitetaan tässä oppaassa asianajotoiminnassa käytettävien tietojen, tietojärjestelmien ja viestinnän asianmukaista suojaamista. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan erilaisten vikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

Asianajajan käyttäessä asianajotoiminnassa esimerkiksi tekoälypohjaisia järjestelmiä, hänen tulee huolehtia siitä, että asiakkaiden luottamukselliset tiedot eivät paljastu tai päädy ulkopuolisten käsiteltäväksi. Tietojen kopioiminen yleisille pilvipohjaisille alustoille saattaa vaarantaa tämän luottamuksellisuuden, joten asianajajan on varmistuttava siitä, miten asianajotoimintaan liittyvää tietoa käsitellään eri

järjestelmissä ja palveluissa. Tekoälyä asianajajan työssä on käsitelty erikseen liitteessä 5. (19.4.2024)

Tässä oppaassa käydään läpi esimerkkejä erilaisista tietoturvaan kohdistuvista riskeistä, jotka asianajotoiminnassa on otettava huomioon. Tietoturvaan voidaan vaikuttaa käytettävillä teknisillä ratkaisuilla, toimiston toimintatavoilla sekä henkilöstön kouluttamisella. Opas toimii asianajajan omien tietoturvamenettelyiden suunnittelun pohjana, mutta myös velvoittavaa tietoturvaohjetta täydentävänä kommentaarina. Lisäksi on syytä huomata, että tämä opas on suositusluontoinen, eli jos esimerkiksi jokin tässä oppaassa kielletty toimi voidaan tietyssä tapauksessa tai olosuhteissa toteuttaa tietoturvallisesti, asianajan ei tarvitse jättää tätä tietoturvallista menettelyä tekemättä vain tässä oppaassa todetun välttämissuosituksen vuoksi.

Riittävän tietoturvan vaatimusten arvioinnissa on otettava erityisesti huomioon kyseisessä asianajotoimistossa hoidettavien toimeksiantojen tyyppi ja laatu, toimeksiantoihin liittyvien tietojen merkittävyys ja sensitiivisyys sekä toiminnan laajuus ja sen mahdollistama laajempi tietoturvaorganisaatio. Tietosuoja on huomioitava omana kokonaisuutenaan, mutta korkea tietoturva on tärkeä osa tietosuojavelvoitteiden toteuttamista. Yksityishenkilöiden asioita hoitavan toimiston tietoturvassa voi olla keskeistä suojautua vikatilanteilta ja satunnaisilta murtoyrityksiltä toimitiloihin, kun taas liikejuridiikkaan liittyviä laajoja toimeksiantoja hoitavan toimiston on varauduttava myös ammattimaisempiin tietomurtoyrityksiin.

1 Henkilökunnan kouluttaminen (14.12.2023)

Asianajajan tulee huolehtia siitä, että toimiston henkilökunta saa ajantasaisen ja riittävän koulutuksen tietoturvalliseen laitteiden ja ICT-palveluiden käyttöön sekä sähköiseen viestintään. Koulutuksessa tulee huomioida velvoittava Tietoturvaohje (B 5.1), jota tämä opas täydentää, ja toimistolle mahdollisesti laadittu tietoturvapolitiikka. Suunnittelun apuna voidaan käyttää koulutussuunnitelmaa, joka määrittää esimerkiksi: tarvittavat tiedot ja taidot tietoturvallisen toiminnan toteuttamiseksi, tarpeellisen koulutuksen, tallenteita koulutuksen täytäntöönpanosta sekä saavutetut tiedot ja taidot. Koulutusvaateita voi olla erilaisia eri henkilöstöryhmille. Koulutuksesta on pyynnöstä esitettävä selvitys kuten täydennyskoulutuksesta (B 9).

2 Tietoturvapolitiikka (14.12.2023)

Vähintään 10 työntekijän asianajotoimistolla on tietoturvapolitiikka, joka on toimiston ylimmän johdon hyväksymä.

Tietoturvapolitiikassa esitetään tietoturvaa ohjaavat periaatteet ja ne keskeiset asiat, jotka toimiston johto haluaa saavuttaa tietoturvallisuudelta ja se, miten arvioidaan, saavutettiinko halutut asiat. Tietoturvaperiaatteet ovat toimiston ylimmän johdon hyväksymät. Tietoturvaperiaatteet ohjaavat toimistossa tehtäviä tietoturvatoimia.

Politiikassa voidaan kuvata toimiston tärkeimmät tietoturvatavoitteet ja tavat, joilla asetetaan yksityiskohtaisempia tietoturvatavoitteita sekä arvioidaan niiden toteutumista. Tekniset ja yksityiskohtaiset tietoturvallisuustoimet kannattaa kuvata muissa tietoturvan ohjeissa ja käytännöissä, jotta tietoturvapolitiikalla voidaan viestiä toimiston tietoturvaperiaatteista tarvittaessa myös ulkoisille sidosryhmille.

Tietoturvapolitiikan tulisi kuvata, miten asianajotoimintaa koskevat tietoturvavaatimukset, erityisesti asiakkaiden tietoja silmällä pitäen, huomioidaan. Tietoturvavaatimuksia voi tulla asianajotoiminnan lisäksi asiakkaiden toimialoilta (esimerkiksi finanssiala, terveydenhuolto, sisäpiirisääntelyä soveltavat pörssiyhtiöt, kansainväliset toimijat). Lisäksi tavat, joilla arvioidaan toimiston tietoturvaa uhkaavat riskit ja miten niihin vastataan, sekä miten toimiston toiminnan ja tietojärjestelmien jatkuvuus turvataan.

Politiikassa voidaan kuvata vastuutahot tietoturvan suunnittelun, täytäntöönpanon ja ylläpidon osalta. Lisäksi voidaan kirjata johdon tai asianajotoimiston osakkaiden sitoutuminen tietoturvan toteuttamiseen, parantamiseen ja resursoimiseen. Politiikassa voidaan myös kuvata tietoturvakoulutuksen periaatteet, vastuut ja miten politiikasta on tiedotettava esimerkiksi muille palveluntarjoajille heidän sitouttamiseksi samaan tietoturvan tasoon.

3 Tietoturva-auditointi (14.12.2023)

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.

Tietoturva-auditoinnin avulla tunnistetaan ulkoisen arvioitsijan toimesta, onko liiketoiminnan kannalta tärkeät tiedot suojattu riittävästi riskien varalta ja asianajosalaisuuden säilyttämiseksi. Auditoinnissa selvitetään tietojärjestelmien tietoturvan hallintaan ja toteutukseen liittyvät puutteet sekä niiden kehitystarpeet. Auditoinnissa tulee huomioida velvoittavat tietoturvavaatimukset, kuten edellä mainittu tietoturvaohje ja tämä opas, myös tietoturvan yleiset periaatteet ja käytännöt. Tietoturva-auditointi tulee suorittaa toimiston koko ja liiketoiminnan laajuus huomioiden riittävän usein sekä toimiston tietoturvaympäristössä tapahtuneet muutokset huomioiden – esimerkiksi uusien järjestelmien lanseerauksen myötä tai toimitilojen muuton jälkeen. Se voidaan toteuttaa esimerkiksi osana tilintarkastusta tai erillisenä konsultointina.

Asianajotoimiston asiakkaat tai muut ulkopuoliset tahot eivät voi auditoida asianajotoimistoa esimerkiksi siten, että asiakas tai muu ulkopuolinen taho tilaa auditoinnin suoraan tai välikäsien kautta ja raportti auditoinnista luovutetaan asiakkaalle tai muulle ulkopuoliselle taholle, koska tämä voi vaarantaa muiden asiakkaiden luottamukselliset tiedot sekä asianajotoimiston tietoturvan. Asianajotoimiston itse tilaamasta auditoinnista laadittu yleisluontoinen raportti taikka muu tietoturvan tasoa ku-

vaava lopputulos voidaan kuitenkin asianajotoimiston harkinnan mukaan luovuttaa tai näyttää asiakkaalle taikka sitä voidaan muutoin pitää yleisesti nähtävillä.

4 Ulkopuoliset tarkastukset ja tietopyynnöt (12.12.2019)

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. Tämä ei tarkoita, etteikö asiakas voisi pyytää omaa asiakkuuttaan tai toimeksiantoja koskevia tietoja taikka asiakirjoja. Asiakkaankin tekemä asianajotoiminnan järjestämistä koskeva tarkastus tai laajempi tietopyyntö voi vaarantaa muiden asiakkaiden luottamuksellisten tietojen käsittelyn ja siksi tällaisiin pyyntöihin ei tule suostua asianajosalaisuuksien turvaamiseksi. (12.12.2019)

5 Toimitilat

5.1 Tilojen suunnittelu ja vieraiden liikkuminen

Toimitilojen murto-, palo- ja muut vastaavat vahingot on pyrittävä ennaltaehkäisemään. Toimitilojen lukitus on hoidettava kokonaisuutena arvioiden asianmukaisesti ja ottaen huomioon samassa rakennuksessa tapahtuva muu toiminta ja sen aiheuttamat riskit. Yksittäisen työhuoneen ei välttämättä tarvitse olla lukittava, jos esimerkiksi toimiston tai työhuoneen käsittävän rakennuksen osan kulkureitit ovat lukittuja. Toimistossa tulee olla toimitilojen koko huomioiden mitoitettu hälytysjärjestelmä, joka voi olla osa rakennuksen yhteistä hälytysjärjestelmää. Toimistorakennuksessa voi olla lisäksi tarpeen järjestää erillinen vartiointi riippuen muun muassa toimiston tai toimipisteen kokonaispinta-alasta ja sijaintipaikasta.

Asiakkaiden ja muiden ulkopuolisten henkilöiden liikkuminen ja oleskelu toimitiloissa on suunniteltava niin, ettei toimiston tietoturva vaarannu. Tämä on huomioitava myös neuvottelutiloja järjestettäessä. Asiakkaat ja muut ulkopuoliset henkilöt tulee vastaanottaa heidän saapuessaan toimistoon ja henkilökunnan tulee ohjata heidät oikeaan paikkaan siten, että he eivät pääse vierailun aikana itsenäisesti tutustumaan asianajosalaisuuden alaiseen materiaaliin. Huoltotehtäviä suorittavat henkilöt tulee erikseen tunnistaa ja tarvittaessa huoltotoimenpiteitä on valvottava. Ulkopuolisten palveluntarjoajien, esimerkiksi siivoojien, huoltohenkilöiden tai palvelutoimittajien kanssa, on tehtävä kirjallinen salassapitosopimus.

Jos toimistossa on paljon henkilökuntaa, heidän tunnistamisessaan voidaan käyttää esimerkiksi kulkulupaa tai muuta henkilökorttia. Kulkulupa on peruutettava, avaimet kerättävä pois ja sähköiset kulkuoikeudet päätettävä välittömästi palvelussuhteen päättyessä.

5.2 Laitteiden sijoittaminen ja postin käsittely

Toimiston laitteet on sijoitettava niin, etteivät ulkopuoliset henkilöt pääse näkemään esimerkiksi henkilökunnan näyttöjä, tulostettuja asiakirjoja tai toimistolle saapuvia taikka sieltä lähteviä muita viestejä. Myös paperisen postin käsittelyssä on huomioitava tietoturvan vaatimukset. Kaikenlaisten viestien ja muun asianajotoiminnassa käytettävän aineiston käsittely on pyrittävä sijoittamaan muualle kuin aula- tai vastaanottotiloihin.

Asianajotoimiston palvelimet tulee sijoittaa sellaisiin lukittaviin tiloihin tai kaappeihin, joihin on pääsy vain erikseen sovituilla henkilöillä.

5.3 *Aineiston säilytys*

Asiakirjojen ja muun aineiston säilytys tulee järjestää niin, etteivät ne ole tarpeettomasti muiden henkilöiden nähtävillä. Asiakirjojen säilytystilojen tulee olla riittävällä tavalla suojattuja.

6 Yrityskäyttöön tarkoitetut ohjelmistot ja palvelut (14.12.2023)

Asianajotoiminnassa käytettävien ohjelmistojen ja palveluiden tulee olla yrityskäyttöön tarkoitettuja. Tällä varmistutaan ensinnäkin siitä, että ohjelmistoja ja palveluita käytetään niiden lisenssiehtojen mukaisesti. Toiseksi yritystason ohjelmistoissa ja palveluissa on tyypillisesti korkeampi tietoturvan taso ja tämä on erityisesti syytä ottaa huomioon ohjelmistoja valittaessa.

Muita palveluja voidaan käyttää vain asiakkaan erillisellä suostumuksella. Tämä on poikkeus edellä kirjattuun pääsääntöön ja voi tarkoittaa esimerkiksi kuluttaja-asiakkaan pyynnöstä asiakkaan tietojen tallentamista hänen osoittamansa pilvipalveluun. Asianajajan tulee huolehtia kuitenkin siitä, että palvelujen luottamuksellisuus ja asianajosalaisuus eivät näin toimiessa vaarannu.

7 Laitehallinta ja pääsynhallinta (14.12.2023)

Vähintään 10 työntekijän asianajotoimistossa asianajotoiminnassa käytettävät laitteet on oltava laitehallinnan piirissä. Lisäksi on otettava käyttöön pääsynhallintaratkaisu.

Laitehallinnalla luetteloidaan toimiston käytössä olevat laitteet ja niihin voidaan keskitetysti asettaa laitteiden mukaisia asetuksia. Laitehallinnan tulee kattaa asianajotoiminnan käytössä olevat laitteet, kuten kannettavat tietokoneet, puhelimet ja tabletit. Laitehallinnassa näistä laitteista muodostuu laiterekisteri, jonka avulla voidaan seurata käytössä olevia laitteita ja niiden elinkaaria.

Pääsynhallintaratkaisulla voidaan esimerkiksi rajoittaa muiden kuin toimiston omien laitteiden pääsyä toimiston tietojärjestelmiin ja tietoihin sekä asettaa yhteisiä

määrityksiä toimiston laitteiden asetuksiin. Pääsynhallintaa voidaan useimmiten määrittää laitekohtaisesti (laitehallinta, sertifikaatit), ip-osoitekohtaisesti (esimerkiksi toimiston ip-osoiteavaruus) ja käyttäjäkohtaisesti (käyttäjäluettelo). Pääsy voidaan rajata paitsi toimiston ympäristöön myös vain työtehtävissä tarvittaviin tietoihin henkilön toimenkuvan mukaan esimerkiksi määrittämällä käyttäjä tiettyyn käyttäjäryhmään tai rooliin. Pääsynhallintaratkaisussa voidaan määrittää portaita esimerkiksi epätyypillisen käytöksen perusteella (käyttäjä yrittää ottaa hyväksytyllä laitteella yhteyden epätyypillisestä osoitteesta, jolloin vaaditaan vaikkapa lisävarmennus, esimerkiksi asianajajan tietokone pyrkii kirjautumaan verkkoon vaikkapa ulkomailta, jolloin käyttäjän tulee kirjautumisen mahdollistamiseksi käyttää kaksivaiheista tunnistautumista).

8 Luottamuksellista tietoa sisältävien laitteiden suojaaminen (14.12.2023)

8.1 Tietokoneet ja palvelimet

Koska asianajotoiminnassa käsitellään säännöllisesti luottamuksellisia ja salassa pidettäviä tietoja, lähtökohtana tulee olla tietokoneiden kaikkien tallennusvälineiden (kuten kiintolevyn) tietojen salaus. Kannettavien tietokoneiden osalta riski joutua anastusrikoksen kohteeksi on suurempi kuin pöytätietokoneiden tai palvelimien, joten tallennusvälineiden tiedot tulee aina salata. Salaaminen vaikeuttaa tallennettuun tietoon pääsyä, jos tallennusväline päätyy vääriin käsiin. Salaaminen suojaa tietovälineen sisältöä tapahtuipa tallennusvälineen joutuminen väärinkäsiin anastuksen johdosta tai sen takia, että tietokone kierrätetään. Siksi myös palvelinten levyt on salattava.

Tietokoneiden tulee lukittua automaattisesti, mikäli niitä ei käytetä lyhyen ajan kuluessa. Tietokone tulee lukita myös, jos tietokone jää valvomatta esimerkiksi tauon ajaksi. Erityisesti vastaanotto- ja vierastiloissa olevat tietokoneet on lukittava heti poistuttaessa paikalta lyhyeksikin aikaa. Käytettäessä tietokoneita tai muita laitteita toimiston ulkopuolella tulee huolehtia siitä, että ohikulkevat tai lähistöllä olevat ulkopuoliset eivät voi nähdä ruudulla näkyviä tietoja. Säännöllisesti julkisilla paikoilla tai julkisessa liikenteessä luottamuksellisia tietoja käsittelevän tulee asentaa laitteidensa näyttöön suojakalvo, joka estää näytöllä olevien tietojen näkymisen muille kuin laitteen käyttäjälle, hankkia laite, jossa tällainen toiminnallisuus on toteutettu sähköisesti, tai huolehtia muulla tavoin näytöllä näkyvien tietojen tehokkaasta suojaamisesta.

Asianajotoimintaan tarkoitettu laite on aina ensisijaisesti tarkoitettu työkäyttöön. Tietoturvaan ja salassapitoon liittyvistä syistä muiden henkilöiden, kuten perheenjäsenten, ei tule sallia käyttää tietokonetta tai muuta laitetta. Tietokoneelle tulee asentaa ainoastaan työn kannalta tarpeellisia ja turvallisia ohjelmistoja. Samoin tietokoneella tulee käyttää ainoastaan työn kannalta tarpeellisia ja turvallisia verkkosivustoja.

8.2 Mobiililaitteet

Puhelimeen ja tablettiin tallennetaan usein asianajotoiminnassa käytettävää tietoa tai puhelimella voi olla pääsy verkkoyhteyden kautta erilaisiin asianajotoiminnassa käytettäviin palveluihin, jotka sisältävät luottamuksellista ja salassa pidettävää tietoa. Mobiililaite voi sisältää kalenterimerkintöjä, tietoja asiakassuhteista, osoitekirjoja, puhelulokeja ja muuta asianajosalaisuuden piiriin kuuluvaa tietoa. Mobiililaitteeksi tulee valita sellainen malli, jossa on riittävät tietoturvatoiminnot asianajokäyttöön.

Mobiililaitetta on säilytettävä huolellisesti ja sen tulee lukittua automaattisesti, jos sitä ei ole käytetty vähään aikaan. Mobiililaitteen käyttö on oltava mahdollista vain luotettavan tunnistautumisen jälkeen (ks. kohta 6). Mobiililaitteen lukituksen lisäksi myös siihen tallennettava sisältö on salattava. Mobiililaitteessa tulee olla aktivoituna myös mahdollisuus tietojen poistamiseen, puhelimen paikantamiseen ja sen lukitsemiseen etänä, jos puhelin tarjoaa tällaisen mahdollisuuden. Tällaiset toiminnot voidaan ottaa käyttöön mobiililaitteilla myös kolmannen osapuolen ohjelmistoilla ja tämä on suositeltavaa erityisesti suuremmissa toimistoissa.

Mobiililaitteidenkin osalta on kiinnitettävä huomiota näytöltä näkyviin tietoihin. Mobiililaitteisiin voi asentaa näyttösuojan näytöllä näkyvien tietojen suojaamiseksi.

8.3 Pilvipalvelut, tietokannat ja muut kootut tietoaineistot (esim. taulukot)

Asianajotoiminnassa käytettäviin pilvipalveluihin ja tietokantoihin tallennetut tiedot tulee olla salattu. Jo palvelujen hankintavaiheessa on hyvä varmistaa tietojen salauksen mahdollisuus ja sen oikeanlainen käyttöönotto.

Pilvipalveluita käytettäessä ja hankittaessa on kiinnitettävä huomiota siihen, että palvelu tarjoaa riittävän tietoturvan tason eli tiedot on salattu siten, että ulkopuoliset eivät pääse niihin käsiksi. Tyypillisesti kaupallisessa käytössä olevissa palveluissa on esitetty kuluttajille tarkoitettuja sovelluksia pidemmälle meneviä toiminnallisuuksia tietojen salaamiseen ja myös yritykset pyrkivät suojaamaan ammattikäyttöön tarkoitetut tiedot palvelimillaan huomattavasti kuluttajatietoja tehokkaammin. Jos pilvipalvelusta, esimerkiksi tekoälyratkaisusta, on tarjolla laajempia turvallisuusominaisuuksia sisältävä versio, joissa tiedot on erotettu muiden käyttäjien tiedoista, tällainen versio tulee ottaa käyttöön.

Asiakastietoja kokoavat taulukot, tietokannat ja pilvipalvelut on myös suojattava salauksella. Käytännössä taulukoihin, joissa käsitellään asiakastietoja, tulee asettaa salasana tietojen pääsyn estämiseksi. Tyypillisimmät taulukkolaskentasovellukset käyttävät vahvaa salausta tietoihin pääsyn estämiseksi ja kun salasanasuojaus on otettu käyttöön, se estää tietojen käytön, jos taulukko pääsee vääriin käsiin. Tietokannat, joissa käsitellään asiakastietoja, tulee salata. Riippuen tietokannasta, salaaminen voidaan toteuttaa eri tavoin, mutta tietokantoja salatessa on kiinnitettävä erityistä huomiota siihen, että myös avaimet, joilla salaus vapautetaan, on suojattu riittävällä tavalla, koska avainten yhdistyessä tietokantoihin, tietokannat ovat avattavissa kuten salaamattomat tietokannatkin.

8.4 Käyttöjärjestelmien ja ohjelmistojen päivittäminen

Tietokoneiden, mobiililaitteiden ja muiden laitteiden käyttöjärjestelmät ja muut käytössä olevat ohjelmistot tulee päivittää ilman aiheetonta viivästystä, kun uusia päivityksiä on saatavilla. Käyttöjärjestelmiin on sisäänrakennettu automaattinen päivitystoiminto, joka on syytä pitää päällä ja jonka kautta valmistaja jakaa myös tietoturvapäivityksiä. Käyttöjärjestelmän automaattisen päivitystoiminnon sijaan päivityksiä voidaan asentaa myös toimiston keskitetyn tietojärjestelmäylläpidon toimesta. Päivitykset lisäävät koneessa olevan käyttöjärjestelmän turvallisuutta. Päivitykset tulee aina hankkia vain ohjelmiston alkuperäiseltä toimittajalta ja turvallisesta lähteestä. Yksittäistä päivitystä voidaan kuitenkin lykätä, jos se ei vaaranna tietoturvaa ja se on tarpeen järjestelmän toimivuuden varmistamiseksi esimerkiksi odotettaessa muiden ohjelmien päivityksiä.

Käyttöjärjestelmän lisäksi käytössä olevat ohjelmat ja sovellukset tulee päivittää, kun niille on tarjolla uusia päivityksiä. Päivitykset voidaan yleensä asettaa asentumaan automaattisesti.

Jos käytössä olevaan käyttöjärjestelmään tai sellaiseen ohjelmistoon, joka voi muodostaa tietoturvariskin, ei enää saa päivityksiä, se on vaihdettava tuoreempaan tai tarvittaessa toiseen ohjelmistoon.

8.5 Ulkoiset tallennusvälineet

Ulkoisia tallennusvälineitä (esim. ulkoinen kovalevy tai muistitikku) käytetään nykyään esimerkiksi suurten aineistomäärien siirtämiseen erityisesti silloin, kun aineisto ei ole helposti siirrettävissä internet-yhteyden kautta. Ulkoisiin tallennusvälineisiin liittyy vakavia tietoturvariskejä, jotka asianajajan tulee huomioida. Ulkoinen tallennusväline voi joutua anastusrikoksen kohteeksi tai se voi hukkua. Tallennusvälineiden käytöstä ja säilytyksestä on huolehdittava siten, että niissä olevat luottamukselliset tiedot ovat suojassa.

Ulkoisia tallennusvälineitä käytettäessä on suositeltavaa valita tallennusväline siten, että se itsessään sisältää salausmahdollisuuden ja muita mahdollisia tietoturvaominaisuuksia, kuten mahdollisuuden tietojen tuhoamiseen. Vaihtoehtoisesti tallennusvälineelle siirrettävät tiedostot tulee salata erikseen.

Ulkoiset tallennusvälineet voivat myös olla riskialttiita virusten ja haittaohjelmien kannalta. Ulkopuolisen tahon omistamaa tai käyttämää tallennusvälinettä ei tule kytkeä asianajotoiminnassa käytettäviin laitteisiin varmistumatta ensin huolellisesti, että se on turvallista tehdä.

Asianajajan on erityisen huolellisesti varmistuttava siitä, että ulkoinen tallennusväline poistetaan käytöstä tietoturvallisesti (ks. kohta 13 jäljempänä).

9 Verkkoyhteyksien suojaus

Asianajotoimiston sisäiseen verkkoon saa olla pääsy vain sellaisilla laitteilla, joita käytetään asianajotoiminnassa. Tämä voidaan toteuttaa erilaisin laitteita tai käyttäjiä varmentavin menetelmin, esimerkiksi hakemistopalvelussa (AD) olevien laitteiden rekisterillä, käyttämällä verkkolaitteissa määritettyjä yksilöiviä laiteosoitteita (MAC-osoite), sertifikaattien keinoin tai estämällä liittäminen verkkoliittimiin peittämällä liittimet (yleisistä tiloista). Asianajotoimiston verkko voi olla myös langaton, kunhan sen asianmukaisesta suojaamisesta on huolehdittu.

Asianajotoimistossa voi olla myös vieraille tarkoitettu erillinen verkko internet-yhteyden tarjoamista varten. Asiakkaiden käyttöön tarkoitettu verkko tulee pitää erillään toimiston omassa käytössä olevasta verkosta eikä sitä kautta saa olla pääsyä toimiston sisäisiin tietoihin tai järjestelmiin.

Verkkoyhteys voidaan muodostaa myös asianajotoimiston ulkopuolisten ja julkisten verkkojen kautta esimerkiksi kotoa tai hotellissa. Jos verkkoyhteys on henkilöstön oma ja sitä käytetään säännöllisesti työssä, sen tulee turvallisuuden osalta lähtökohtaisesti noudattaa samaa tietoturvan tasoa kuin toimiston verkon. Ulkopuolisen verkon ja ajoittaisen oman verkon käytössä tietoturva tulee varmistaa käyttämällä salattua yhteyttä. Salattu yhteys voidaan muodostaa suojattuna esimerkiksi Virtual Private Network (VPN) tai Secure Shell (SSH) -yhteytenä. Toimiston käyttöön sopivasta suojausratkaisusta tulee hankkia tarvittaessa lisätietoja teknisiltä asiantuntijoilta.

Sekä sisäisen että asiakkaiden käyttöön tarkoitetun langattoman verkon tulee edellyttää vähintään salasanaperusteista tunnistusta ja verkkoliikenteen tulee olla salattua.

10 Käyttäjätunnukset ja salasanat (14.12.2023)

Käyttäjä voi tunnistautua asianajotoimiston järjestelmiin ja laitteisiin käyttämällä käyttäjätunnusta ja salasanaa, biometristä tunnistautumista, henkilökorttia, tunnistautumisavaimia tai muuta turvallista tunnistautumismenetelmää. Mahdollisuuksien mukaan käytössä olevissa ratkaisuissa ja palveluissa on otettava käyttöön kaksivaiheinen tunnistaminen (tai muu lisätunnistautumismenetelmä), jolloin salasanan tai muun käyttäjäkohtaisen varmenteen lisäksi käytetään toista tunnistamistapaa.

Salasanan tulee olla riittävän tietoturvallinen. Salasanoja yritetään murtaa yleensä ohjelmallisesti, joten pitkä salasana, joka koostuu erilaisista merkeistä eikä sisällä helposti arvattavia merkkijonoja tai sanoja (kuten toimiston nimi tai oma syntymävuosi), on yleensä tietoturvallisin. Samoja salasanoja ei tule käyttää uudelleen. Oman työaseman ja keskeisimpien asianajotoiminnassa käytössä olevien palveluiden salasana tulee vaihtaa tarvittaessa.

Nykykäsityksen mukaan salasanan säännöllinen vaihtaminen ei ole turvallisempi tapa kuin vahvan salasanan valitseminen ja siinä pitäytyminen. Tämä johtuu siitä, että

salasanan vaihtamistarve johtanee lopulta salasanamuotoon, joka on helposti vaihdettavissa ja muistettavissa.

Salasana voi paljastua ulkopuoliselle myös niin, että se nähdään syötettävän tai sitä käytetään jossain muussa palvelussa, johon murtaudutaan. Salasana tulee tarpeen mukaan suojata fyysisesti sitä syötettäessä eikä sitä tule kertoa kenellekään. Edellä mainitusta syystä salasanaa, jota käytetään asianajotoimiston verkossa tai työasemilla, ei saa käyttää internet-palveluiden salasanana ja kaikissa palveluissa, joissa käsitellään asianajotoimintaan keskeisesti liittyvää materiaalia, tulee käyttää eri salasanaa.

10.1 Tietojenkalastelu

Tietojenkalastelu (phishing) tarkoittaa tietojen, kuten verkkopankki- tai käyttäjätunnusten, laitonta hankkimista houkuttelemalla käyttäjä antamaan ne esimerkiksi aidolta näyttävällä huijausverkkosivustolla tai puhelimessa.

Viestin lähettäjätieto saattaa olla väärennetty eli viesti ei välttämättä ole lähettäjäksi mainitun tahon lähettämä. Liite tai linkki saattaa myös olla jotain aivan muuta kuin viestissä tai tiedoston nimessä väitetään.

Vältä vastaamasta kaikkiin epätavallisiin yhteydenotto- ja kirjautumiskehotuksiin, joita et ole itse pyytänyt. Älä koskaan anna tunnistautumistietojasi tai salasanaasi verkkopalvelun, salaamattoman viestin tai puhelimen välityksellä kenellekään.

11 Tietoturvaohjelmistot, palomuuri ja käyttöoikeudet (14.12.2023)

11.1 Virustorjunta ja haittaohjelmien estäminen

Viruksia ja haittaohjelmia on useita tyyppejä. Suurimpia riskejä aiheuttavat ohjelmat, jotka tuhoavat tai lukitsevat tietoja käyttäjän ulottumattomiin, antavat vieraalle pääsyn siihen taikka keräävät näitä tietoja ja lähettävät ne isännälleen. Joihinkin haittaohjelmiin saattaa liittyä myös vaatimuksia maksusta tietojen palauttamiseksi.

Asianajotoimistolla tulee olla toimiva ja ajan tasalla oleva virusten ja haittaohjelmien torjuntaohjelma, joka estää pääsyn toimiston järjestelmiin ja tietokoneille. Ohjelman tulee päivittyä automaattisesti. Virustorjunta tulee tarvittaessa asentaa myös mobiililaitteisiin. Torjuntaohjelman tulee käydä läpi saapuvat sähköpostiviestit sekä tiedostot ennen kuin ne avataan tai suoritetaan. Lisäksi asianajotoimistojen laitteiden tarkastaminen virusten ja haittaohjelmien varalta on suoritettava säännöllisesti.

Virusten ja haittaohjelmien estämiseksi tuntemattomilta tahoilta tulevia, otsikkonsa tai sisältönsä perusteella epäilyttäviä sähköpostiviestejä eikä etenkään niissä olevia liitteitä tai linkkejä tule avata.

Asianajotoiminnassa käytettävillä tietokoneilla on vältettävä käymistä sellaisilla internet-sivuilla, joilta on suurempi riski saada koneelleen haittaohjelmia. Mikäli toimeksiannon hoitaminen edellyttää tällaisilla sivuilla käymistä, asianajajan on erityisen

huolellisesti varmistuttava tietoturvastaan esimerkiksi käyttämällä toimenpiteeseen toimeksiantotyöstä erillistä tietokonetta tai mobiililaitetta.

On myös syytä suhtautua varauksella sinänsä asiallisillakin sivustoilla oleviin mainoksiin, linkkeihin sekä etenkin tarjottaviin ohjelmiin. Asianajotoimiston on huolehdittava myös siitä, että henkilökunnan toimiston ulkopuolella asianajotoimintaan liittyvien tehtävien hoitamiseen käyttämissä koneissa ja laitteissa on asianmukainen torjuntaohjelma.

Jos epäilet, että laitteessa on haittaohjelma tai virus, sen käyttö tulee välittömästi lopettaa, kunnes se on puhdistettu tai varmistettu puhtaaksi.

11.2 Tietoliikenteen suojaaminen

Palomuuria tarvitaan suojaamaan asianajotoimiston verkkoa ja tietokoneita ulkopuolelta (internetistä) tulevilta hyökkäyksiltä. Palomuurin tarkoituksena on päästää läpi vain haluttu verkkoliikenne ja estää luvattomien yhteyksien muodostaminen sisäverkossa oleviin laitteisiin.

Asianajotoimistolla on oltava palomuuri. Palomuuri voidaan toteuttaa ohjelmistolla tai laitteistolla. Usein on suositeltavaa rakentaa palomuurijärjestelmä käyttäen molempien yhdistelmää. Palomuuriohjelmistot ja -laitteet on pidettävä toimintakuntoisina ja ajan tasalla.

11.3 Käyttöoikeudet

Tietoturvallisuuden hallintaan vaikuttavien ohjelmistojen ja järjestelmänvalvojien käyttäjätunnukset ovat tarkimmin varjeltavia käyttöoikeuksia. Väärissä käsissä nämä käyttöoikeudet antavat väärinkäyttäjälle tai hyökkääjälle keinon välttää huomatuksi tulemisen ja oikeutettujen käyttäjien ulossulkemiseen omista järjestelmistään. Useimmat hyökkääjät ja haittaohjelmat tarvitsevat järjestelmävalvojan oikeudet, jotta voivat levittäytyä tai asentua järjestelmiin. Mikäli käyttäjät toimivat käyttäjätason tunnuksilla, haitallisia toimia voidaan rajoittaa tehokkaasti.

Käyttäjätunnuksia kannattaa erottaa vähintään järjestelmänvalvoja – käyttäjä -tasoisesti, mutta hiemankin suuremmissa organisaatioissa esimerkiksi pääkäyttäjille voidaan hyödyntää näiden välissä olevia käyttäjäryhmätasoja.

12 Asiakirjojen tallentaminen ja pääsy tietoihin

Asianajalla on velvollisuus tallentaa ja säilyttää toimeksiantoihin liittyvä kirjeenvaihto. Velvoite täyttyy myös sähköisellä tallenteella, jonka tulee olla tietoturvallinen ja varmistettu. Tietoturvallisempaa on säilyttää tiedostot palvelimella yksittäisten laitteiden sijaan. Ks. säilytysajoista B 10 Asiakirjojen säilyttämistä koskeva ohje.

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

hoitamiseksi. Pääsyä asiakirjoihin tulee tarvittaessa rajoittaa asianajotoimiston sisälläkin, erityisesti kun kyse on sisäpiiriasioista.

13 Varmuuskopiointi (14.12.2023)

Varmuuskopioinnilla hallitaan riskiä tietojen tuhoutumisesta, muuttumisesta (joka voi johtua esim. laitteiston rikkoutumisesta tai tuhoutumisesta), laitteiston anastamisesta, virus- tai haittaohjelmasta tai käyttäjän vahingossa tekemästä tietojen poistamisesta. Varmuuskopiointi ei korvaa asiakirjojen asianmukaista arkistointia, sillä myös asiakirja-arkisto on varmuuskopioitava.

13.1 Varmuuskopioinnin suunnittelu

Toimistossa tulee arvioida asianajotoiminnan kannalta tärkeiden järjestelmien osalta, kuinka pitkältä ajalta tietoa on varaa enintään menettää? Ja määrittää varmuuskopioinnin tiheys arvion mukaan.

Tulee myös arvioida, kuinka pitkään tullaan toimeen ilman järjestelmää, kiirehuiput huomioiden? Ja määrittää varmuuskopioitavalle järjestelmälle palautumisaikataulu arvion mukaan.

Lisäksi tulee arvioida, kuinka pitkältä ajalta varmuuskopiotavia tietoja saatetaan tarvita, toisin sanoen kuinka kauan varmuuskopioitua tietoa tulee säilyttää? Arviossa tulisi huomioida, että voi tulla tilanteita, joissa esimerkiksi tärkeiden tietojen poistoa ei huomata pitkään aikaan tai joudutaan haittaohjelman takia palautumaan tiedostoja pitkänkin ajan takaa.

13.2 Varmuuskopioitavat tiedot

Asianajotoimintaan liittyvien tietojen varmuuskopioinnista on huolehdittava. Suositeltavaa on, että ainakin seuraavat tiedot kuuluvat varmuuskopioitaviin tietoihin:

- työssä tuotettu vielä arkistoimaton tieto kaikilla käytössä olevilla laitteilla, ml. mobiililaitteet
- asianhallintajärjestelmä ja laskutustiedot
- sähköpostiviestit ja muut mahdollisesti käytössä olevat viestintäratkaisut
- sähköiset kalenterit ja yhteystiedot
- arkistoidut asiakirjat ja muu arkistoitu tieto

Jos tietoja on tallennettu erilaisiin ulkoistettuihin palveluihin tai pilvipalveluihin, tulee huolehtia siitä, että hankittuun palveluun kuuluu tietojen riittävä varmuuskopiointi. Tarvittaessa näistä palveluista on otettava fyysiset varmuuskopiot tai varmuuskopioitava tietoja eri palvelujen välillä.

13.3 Varmuuskopiointitavat ja tietojen säilytys

Varmuuskopiointiin on saatavilla lukuisia teknisiä välineitä ja sovellusratkaisuja. Yksi vaihtoehto on ulkoistettu varmuuskopiointipalvelu, jossa tiedot lähetetään verkon yli palveluntarjoajan palvelimelle. Tällaisen palvelun hyvänä puolena voidaan pitää, että tiedot ovat toimiston ulkopuolella eri paikassa kuin itse varmuuskopioitava tieto. Sopimusta tehdessä tulee huomioida ne näkökohdat, jotka aina liittyvät ulkoistettujen palveluiden käyttämiseen ja tietojen tietoturvalliseen lähettämiseen. Jos varmuuskopiota ei tehdä pilvipalveluun, on suositeltavaa säilyttää varmuuskopioita turvallisessa paikassa toimiston tai varsinaisen tallennuspaikan ulkopuolella, ellei siihen ole erillistä sopivaa ja turvallista säilytyspaikkaa.

13.4 Varmuuskopioinnin säännöllisyys

Varmuuskopioinnista tulee huolehtia säännöllisesti. Varmuuskopiointi tulee lähtökohtaisesti automatisoida, jotta sen tekeminen ei ole kiinni työtilanteesta tai henkilöstön omasta aktiivisuudesta. Jos varmuuskopiointi kohdistuu vain edellisen varmuuskopiointikerran jälkeen tehtyihin muutoksiin, tulee säännöllisin ajoin tehdä myös koko aineiston täydellinen varmuuskopio varmuuskopioiden eheyden varmistamiseksi.

Asianajajan tulee varmistua siitä, että toimiston tietojen varmuuskopiointi toimii tarkoitetulla tavalla ja että tiedot ovat tarvittaessa nopeasti ja vaikeuksitta palautettavissa.

14 ICT-palveluiden ostaminen ja ulkoistaminen

Asianajotoiminnassa on usein tarpeen käyttää ulkopuolista ICT-tukea teknisen asiantuntemuksen varmistamiseksi ja toisaalta myös ostaa tietotekniikkapalveluita (kuten pilvipalvelut) ulkopuoliselta toimittajalta. Kumpaankin käyttötilanteeseen liittyy tietoturva- ja tietosuojakysymyksiä, jotka asianajajan täytyy ottaa huomioon.

14.1 Ulkopuolinen tekninen tuki

Ulkopuolista teknistä tukea käytettäessä asianajotoimiston on huolehdittava asianmukaisista salassapitosopimuksista palveluntarjoajan kanssa. Tukea voidaan käyttää esimerkiksi asianajotoimiston laitteistoympäristön ja käytössä olevien järjestelmien rakentamiseen, ylläpitoon, huoltoon, tietoturvan tason arviointiin, käyttötukeen ja muuhun teknistä osaamista vaativaan työhön.

Teknisen tuen tarjoajalla ei tule olla tarpeettoman laajaa pääsyä asianajotoiminnassa käytettäviin tietoihin. Pääsy on rajattava mahdollisimman suppeaksi ja lyhytaikaiseksi. Pääsyjä tulisi katselmoida ajoittain, jolloin voidaan poistaa tarpeettomaksi käyneet oikeudet. Etäyhteyksiä toimiston järjestelmiin on annettava erikseen ja valvottava.

14.2 Tietotekniikkapalvelujen ostaminen

Tietotekniikkapalveluiden ostamisessa asianajosalaisuuksia sisältävää tietoa säilytetään, käsitellään ja siirretään palvelimilla tai palveluissa, jotka eivät ole asianajajan yksinomaisessa hallinnassa. Monet yritykset tarjoavat palveluita, joissa asianajotoimistojen salassa pidettäviä tietoja käytetään ja säilytetään palveluntarjoajan palvelimella. Tyypillisiä ulkoista palvelintilaa hyödyntäviä palveluita ovat sähköposti, verkkosivut, varmuuskopiointi, sähköinen kalenteri, laskutus, asiakas- ja toimeksiantorekisteri tai tallennustila verkossa. Ulkoisen palvelimen käyttäminen on joissakin tapauksissa, esimerkiksi verkkosivun osalta, järkevä ja jopa ainoa käyttökelpoinen ratkaisu. Palveluita kutsutaan usein pilvipalveluiksi tai SaaS (Software as a Service) -palveluiksi.

Asianajajan on palveluita hankkiessaan ja sopimuksia tehdessään kiinnitettävä erityistä huomiota asianajajalta edellytettävän salassapidon asettamiin vaatimuksiin ja asianajotoimiston asianmukaiseen järjestämiseen ja laadittavan palvelusopimuksen päättymiseen. Palveluntarjoajaa valittaessa on ehdottoman välttämätöntä varmistua palveluntarjoajan sitoutumisesta täydelliseen tietojen salassapitoon. Pääsy tietoihin tulee olla vain palvelua hankkivalla asianajajalla ja hänen toimistonsa henkilökunnalla.

Tietojen luottamuksellisuus on varmistettava palveluntarjoajan kanssa tehtävällä salassapitosopimuksella. Palveluntarjoajan henkilökunnan pääsy asianajajan tietoihin on normaalissa tilanteessa estettävä. Lisäksi on syytä varmistua palvelun päätyttyä tietojen poistamisesta ja tarvittaessa siirtämisestä toiseen palveluun. Palveluntarjoajan teknisen tietoturvan on oltava riittävän korkeatasoista. Ulkopuolisten pääsy tietoihin on teknisin ratkaisuin estettävä ja tietojen säilyminen on varmistettava. Palvelun taso on sovittava sellaiseksi, että asianajajalla on riittävän luotettava pääsy omaan aineistoonsa milloin tahansa. Jos asianajajan oma tietotekninen tietämys ei riitä tietoturvan tason arviointiin, on syytä arvioituttaa palvelu ulkoisella teknisellä asiantuntijalla.

Palveluntarjoajaa valittaessa on tietoturvan lisäksi syytä kiinnittää huomiota palveluntarjoajan referensseihin, sertifikaatteihin, taustaan ja vakavaraisuuteen sekä palvelimien sijaintimaahan. Palveluntarjoajan palvelimet voivat sijaita eri puolilla maailmaa ja palvelun tekniikka voi perustua tiedon paloitteluun ja kopioimiseen useille palvelimille mahdollisesti eri maissa tai maanosissa sijaitsevissa palvelinfarmeissa. Henkilötietojen siirtämisestä ETA-alueen ulkopuolelle tutustu henkilötietojen käsit- telyä asianajotoiminnassa koskeviin ohjeisiin.

Joidenkin palveluiden käytön aloittaminen on hyvin yksinkertaista. Verkkopalveluiden käyttämisestä syntyy usein palvelusopimus esimerkiksi vain klikkaamalla linkkiätai aloittamalla palvelun käyttö luomalla itse käyttäjätunnukset, jolloin käyttäjä ilmoittaa hyväksyvänsä palvelun tarjoajan ehdot. Mitä tahansa pilvipalvelua ei kuitenkaan voida alkaa käyttää asianajotoiminnassa, vaan palvelun sopivuus – ottaen huomioon myös tietoturva- ja -suojanäkökohdat – on arvioitava tapauskohtaisesti.

Toisaalta pilvipalvelu saattaa olla tietoturvallisempi ratkaisu verrattuna siihen, että asianajotoimisto alkaa itse rakentaa tietoturvan edellyttämää palvelininfrastruktuu-

ria. Pilvipalveluiden etuna on, että tietotekniikan ja tietoturvan ammattilaisten palvelun saa käyttöönsä murto-osalla siitä hinnasta, mitä palveluiden ylläpito maksaisi omiin tietokoneisiin tuotettuna.

Käytettäessä asianmukaista tietoliikenteen salausta ja luotettavaa tunnistautumista pilvipalveluun, on mahdollista pitää kaikki luottamuksellinen tieto palvelussa ilman, että esimerkiksi mobiililaitteessa tai tietokoneessa on tallennettuna paljoakaan luottamuksellista tietoa. Näin yksittäisen laitteen katoamisen aiheuttamat tietoturvariskit voidaan minimoida. Pilvipalvelun käyttö suojaa myös laitteiden rikkoutumisesta aiheutuvilta vahingoilta.

Pilvipalveluita käytettäessä tulee palvelun tarjoajien varmuuskopioinnin vastata sitä, mitä asianajotoiminnassa toimiston omalta varmuuskopioinnilta edellytetään kohdassa 9. Pilvipalveluita käytettäessä on kuitenkin huomioitava myös riski, että pääsy pilvipalveluun yllättäen päättyy tai palveluntarjoaja lopettaa palvelun tarjoamisen.

14.3 Uhkia, joihin tulee varautua

On mahdollista, että viranomaiset kohdistavat mahdolliset tietopyyntönsä tai -vaatimuksensa pilvipalvelun tarjoajaan ja saavat näin haltuunsa myös asianajajan salassapidettäviä tietoja. Sopimusjärjestelyillä ja varmistumalla palveluntarjoajan palveluiden riittävästä teknisestä toteutuksesta ja myös osaamisesta on varmistuttuva eri tahoille kuuluvan tiedon erillään pitämisestä.

Se, miten tiedot ovat viranomaisten tai muiden sivullisten saatavissa palveluntarjoajalta voi riippua palvelimen sijaintimaasta tai palveluntarjoajan kotipaikasta.

15 Sähköinen viestintä

Sähköinen viestintä on muodostunut asianajotoiminnassakin pääsääntöiseksi viestintätavaksi. Sähköinen viestintä edellyttää lähtökohtaisesti asiakkaan suostumusta, joka kuitenkin voidaan nykyään usein olettaa esimerkiksi sillä perusteella, että asiakas on ottanut yhteyttä asianajajaan sähköpostitse. Sähköisen viestinnän käytöstä toimeksiannon hoitamisessa on suositeltavaa ottaa mainінta asianajajan käyttämiin sopimusehtoihin.

Asianajajan tulee kuitenkin huomioida, että sähköisen viestinnän luvaton seuraaminen tai sen salausjärjestelmien purkaminen on mahdollista. Sähköisen viestinnän aukoton suojaaminen viestin syntymisestä sen lukemiseen ja lukemisen jälkeiseen tallentamiseen on käytännössä mahdotonta, mikä asianajajan tulee ottaa kaikessa sähköisessä viestinnässään huomioon ja arvioida tilannekohtaisesti, milloin sähköpostin käyttö voi tai ei voi tulla kysymykseen.

Tarvittaessa asianajajan on opastettava asiakastaan käyttämään salausmenetelmiä arkaluonteisten aineistojen toimittamiseksi.

15.1 Luottamuksellisen viestin suoja

Laki suojaa sähköistä viestintää samalla tavalla kuin muutakin luottamuksellista viestintää. Luottamuksellisuuden suoja ei riipu teknisestä suojauksen tasosta tai viestin mahdollisesta salausjärjestelmästä tai sen puutteesta.

Sähköpostiviesti on luottamuksellinen, ellei sitä nimenomaisesti ole tarkoitettu julkiseksi, eikä väärä vastaanottaja saa hyödyntää viestin sisältöä millään tavalla, vaikka viesti olisikin osoitettu virheellisesti hänelle. Viestissä oleva luottamuksellisuusilmoitus on asianajajalle suositeltava käytäntö ja se korostaa vastaanottajalle viestin luottamuksellisuutta, mutta se ei yksipuolisena voi asettaa väärälle vastaanottajalle toimintavelvollisuutta tai poista lähettäjän vastuuta tiedon lähettämisestä väärälle vastaanottajalle. (Laki sähköisen viestinnän palveluista 136 §).

Malli luottamuksellisuusilmoituksesta:

Tämä viesti on luottamuksellinen ja tarkoitettu ainoastaan vastaanottajalle. Mikäli ette ole viestissä tarkoitettu vastaanottaja, olkaa hyvä ja ilmoittakaa siitä lähettäjälle ja tuhotkaa viesti välittömästi.

—-

Detta meddelande är konfidentiellt och avsett endast för mottagaren. I fall Ni inte är den avsedda mottagaren, vänligen informera avsändaren om detta och förstör meddelandet omedelbart.

This e-mail is confidential and is meant for the recipient only. If you are not the intended recipient, please inform the sender of this and destroy the message immediately.

15.2 Huolellisen toiminnan merkitys

Asianajajan tulee suhtautua korostetun huolellisesti viestinnän suojaamiseen erityisesti silloin, kun viesti sisältää henkilötietoja tai jos toimeksianto on erityisen sensitiivinen tai merkittävä. Edes asiakkaan hyväksyntä viestintävälineen käyttöön ei vapauta asianajajaa vastuusta henkilötietojen suojaamisen osalta ja lähtökohtaisesti sensitiivisiä henkilötietoja sisältävä viesti on lähetettävä aina salattuna (ks. henkilötietojen käsittelyä asianajotoiminnassa koskevat ohjeet).

Suurimman osan viestinnässä tapahtuvista virheistä aiheuttaa lähettäjä tai vastaanottaja itse esimerkiksi lähettämällä tai välittämällä viesti väärälle jakelulle. Asianajajan tulee sähköisessä viestinnässä toimia huolellisesti ja aina varmistaa, että viestit lähetetään oikeisiin ja varmistettuihin sähköpostiosoitteisiin. Asianajajan huolellisuusvelvoite ulottuu oikean vastaanottajan varmistamiseen asti.

Asianajajan on aina viestiä lähetettäessä varmistuttava oikeasta vastaanottajasta. Lisäksi on hyvä varmistua siitä, että dokumentteihin ei jää metatietoja, jotka paljastavat esimerkiksi toisen asiakkaan nimen tai tietoja. Metatietojen puhdistaminen voidaan esimerkiksi automatisoida ennen viestin lähettämistä.

15.3 Sähköisen viestinnän tekninen suojaus (19.4.2024)

Sähköposti siirtyy tietoverkossa usein salaamattomana ja tallentuu erilaisiin välijärjestelmiin, joten tunnistamattomalla määrällä ulkopuolisia henkilöitä on mahdollisuus käsitellä viestiä.

Oman sähköpostiviestinnän varmentamiseksi kannattaa hankkia oma domain (esimerkiksi aatoimisto.fi), jolla erottaa oman viestinnän yleisluontoisista palveluista (kuten yleisesti saatavilla olevat sähköpostipalvelut).

Sähköpostiviestejä voi lähettää tietoturvallisemmin salattuna. Tällöin viesti välitetään salatussa muodossa ja vasta vastaanottaja avaa sen selkokieliseksi tekstiksi salausavaimella. Asianajajan on huolehdittava aineiston salaamisesta, jos sisältö on erityisen sensitiivistä tai asiakas edellyttää salattua liikennettä, sekä tarvittaessa ohjeistettava asiakastaan toimittamaan aineisto suojatulla menetelmällä.

Sähköpostiliikenne voi olla:

1) *täysin suojaamaton/salaamaton,*

2) *TLS-suojattu (ns. normaalisähköpostiliikenteen perussuojaus, joka on oletusarvoisesti käytössä useissa eri sähköpostipalveluissa) taikka*

3) *S/MIME-tekniikkaan tai muuhun salausavainta taikka muuta sähköpostin erillistä purkamista edellyttäen salattu (esim. Citrix Secure Mail, SSH:n Deltagon Secure Email, Suomen Turvaposti Oy:n turvaposti tai erikseen asetettava Microsoft 365:n S/MIME).*

TLS-suojauksen ei ole katsottu täyttävän salaamisen vaatimusta esimerkiksi oikeusministeriönkään hallinnonalalla ja siksi esimerkiksi tuomioistuimissakin käytetään erillistä turvapostia (https://turvaviesti.om.fi). Myös Office 365 -sähköposti edellyttää erillistoimenpiteitä viestin salaamiseksi eikä perusmuotoisena täytä salaamisen kriteerejä (https://support.microsoft.com/fi-fi/office/sähköpostiviestien-salaaminen-373339cb-bf1a-4509-b296-802a39d801dc).

Asianajajalla ei ole velvollisuutta käyttää yksinomaan salattuja sähköpostiviestejä toiminnassaan, mutta asianajan tulee ottaa huomioon salaamattoman viestinnän rajoitteet. Asianajajan on suositeltavaa hankkia tekninen valmius ja osaaminen salattujen sähköpostiviestien lähettämiseen ja vastaanottamiseen.

Vaihtoehtoisesti aineisto voidaan salata suojaamalla arkaluonteinen sisältö salattuihin tiedostoihin. Tällöin normaalin viestin liitteenä lähetetään yksi salattu tai useita salattuja tiedostoja, jotka tulee vastaanottajan päässä avata erikseen ja toisella viestintävälineellä toimitetulla salasanalla riippumatta sähköpostiviestin salauksesta.

Salasanasuojaus riippuu tiedoston tyypistä ja siitä, millä ohjelmalla tiedosto on luotu. Yksinkertaisimmillaan tällainen tiedosto on Office 365 -ohjelman salausta käyttämällä tallennettu tiedosto tai vaihtoehtoisesti jollakin pakkausohjelmalla (Winzip, 7-zip) luotu salattu tiedostopaketti. Salattuja tiedostoja voidaan lähettää linkillä myös monen dokumentinhallintajärjestelmän kautta (esim. Sharepoint, OneDrive Business tai Google Workspace), jolloin käyttäjä varmennetaan vielä erikseen kirjautumalla

15.4 Muut viestintäkanavat

Asianajajan on mahdollista viestiä erilaisten reaaliaikaisten viestintä- tai pikaviestipalvelujen, jotka ovat yhä useammin saatavilla myös mobiililaitteella, välityksellä. Asianajajan tulee suhtautua viestintään suurella huolellisuudella varmistuen aina siitä, että viestin vastaanottaja on oikein tunnistettu ja selvittäen, onko tässä kanavassa kulkevat viestit salattu.

On huomattava, että perinteisiin työvälineisiin liittyy myös tietoturvauhkia. Telefaksia ei tule pitää sähköpostia turvallisempana tietojen lähettämistapana. Usein telefaksissa yhdistyvät sekä sähköisen liikenteen riskit että paperitulosteiden tietoturvaan liittyvät ongelmat. Tekstiviestejä voidaan käyttää asianajotoiminnassa, mutta luottamuksellisen tiedon tai henkilötiedon lähettämistä tekstiviestillä ei voi suositella. Tekstiviestit siirtyvät matkaviestinverkossa yleensä salaamattomina.

16 Asiakirjojen arkistointi ja tuhoaminen

Asianajajan tulee huolehtia siitä, että asiakirjat arkistoidaan ja tuhotaan asianmukaisella tavalla (ks. B 10 Asiakirjojen säilyttämistä koskeva ohje).

Salaisten ja luottamuksellisten tietojen asianmukainen hävittäminen on yhtä tärkeää kuin niiden suojaus ja muu käsittely. Asiakirjat tulee tuhota tietoturvallisesti käyttämällä esimerkiksi luotettavaa ulkopuolista palveluntarjoajaa. Luottamuksellisia asiakirjoja ei koskaan tule heittää tavalliseen roskakoriin vaan erilliseen lukittuun astiaan, josta ne hävitetään turvallisesti. Asianajajan tulee ohjeistaa toimiston henkilökunta, siivoojat ja muut toimiston aineistoa käsittelevät ulkopuoliset henkilöt asiakirjojen asianmukaiseen käsittelyyn.

Asiakirja hävitetään joko tuhoamalla se fyysisesti esimerkiksi silppurilla tai saattamalla se muutoin sellaiseen muotoon, ettei sen sisältämää tietoa voida enää käyttää. Jos hävittäminen tehdään itse, on hyvä myös varmistaa, että asiakirjat tuhotaan oikein esimerkiksi riittävän pieneksi silpuksi.

17 Tietoa sisältävien laitteiden poistaminen käytöstä

Tietokoneille, mobiililaitteille, ulkoisille tallennusvälineille tai muille asianajotoiminnassa käytettäville laitteille voi olla tallennettuna luottamuksellista tietoa. Käytöstä poistuvien laitteiden tiedot tulee aina poistaa tietoturvallisella tavalla riippumatta siitä, menevätkö laitteet romuksi vai uuteen käyttöön.

Kaikkien tiedostojen poistaminen käytöstä poistettavista laitteista tai tallennusvälineiden alustaminen (formatointi) ei ole riittävä toimenpide tietoturvan varmistamiseksi. Tallennusvälineiden fyysinen hajottaminenkaan ei aina takaa, että tiedot eivät olisi palautettavissa. Tietojen turvallinen poisto on tehtävä erillisellä tietojentuhoamisohjelmalla, joka varmistaa, että tietoja ei saada palautettua. Tiedot ja laitteet voidaan myös antaa siihen erikoistuneen yrityksen hävitettäviksi, etenkin jos täyttä varmuutta siitä miten tieto tuhotaan turvallisesti ei ole. Tietojen hävittäminen voi myös kuulua osaksi leasinglaitteiden vuokrasopimusta, mutta tällöin on huolehdittava, että laitteita ei esimerkiksi väliaikaisesti varastoida tietoturvan kannalta epäasianmukaisesti.

Tietojen täydellinen tuhoaminen suoritetaan kaikille tietokoneille, mobiililaitteille ja ulkoisille tallennusvälineille sekä muille laitteille aina, kun laite siirtyy pois asianajajan hallusta. Tämä koskee

- leasing-käytössä olevien laitteiden palautustilanteita,
- uusintakäyttöön/myytäväksi tarkoitettuja laitteita sekä
- tuhottavaksi toimitettavia laitteita.

18 Toiminnan jatkuvuus

Asianajajan tulee huolehtia, että toimiston jatkuvuuden kannalta tarvittavat tiedot on kootusti dokumentoitu ja tämä dokumentointi on jatkuvuudesta huolehtivien tahojen saatavilla. Ks. tarkemmin B 10 Arkistointiohje, kohta 5.

LIITE 1

OFFICE 365 / MICROSOFT 365 -PALVELUN SUOJAAMINEN TIETOMURROILTA (24.9.2021)

Office 365 / Microsoft 365 mahdollistaa pääsyn monenlaiseen toimistotyön palveluun,ja on siksi myös tietojen kalastelijoiden ja krakkereiden mielenkiinnon kohde. Asianajajan tulee huolehtia seuraavista asioista tietojen kalastelun estämiseksi ja Office 365 / Microsoft 365 -palvelun (”365-tilaus”) suojaamiseksi:

1. Asianajotoimintaa varten tulee hankkia lisenssiehtojen mukaisesti yrityskäyttöön tarkoitettu 365-tilaus.

2. Monivaiheinen tunnistautuminen tulee ottaa käyttöön kaikille 365-tilauksen käyttäjille ja tunnistautumisen voimassaolo tulisi määrittää ajallisesti rajoitetuksi. Lisäksi tulee varmistaa, että palveluun päästään kirjautumaan niissä tapauksissa, jossa tunnistautumispalvelu on vikaantunut (esimerkiksi luomalla pöytä-laatikkokäyttäjä, jolle kaksivaiheista tunnistautumista ei ole otettu käyttöön).

3. 365-tilauksen sisäänkirjautumissivu tulisi räätälöidä yrityksen ilmeen mukaiseksi. Näin käyttäjiä on vaikeampi erehdyttää syöttämään tietoja mahdolliselle huijauskirjautumissivustolle.

4. 365-tilauksen pääkäyttäjätunnuksia (järjestelmänvalvoja) tulee myöntää ainoastaan tarpeiden mukaisesti ja mahdollisimman pieni lukumäärä (kuten 1–2 kpl). Pääkäyttäjätunnukset ja muut käyttäjätunnukset tulee poistaa henkilöiltä, jolla ei ole niille enää käyttöä.

5. Käyttäjät tulee kouluttaa erityisesti yleisimpien 365-tilauksen tietoturvallisuutta vaarantavien tapahtumien ehkäisemiseksi. Käyttäjän tulisi tuntea vähintään: tunnistamaan oikea kirjautumissivu, mistä voi tunnistaa huijausviestit, käyttäjätunnuksensa ja salasanansa turvalliset käsittelytavat sekä miten tulee toimia, jos on joutunut huijauksen tai huijausyrityksen kohteeksi.

6. 365-tilauksessa käytettävän salasanan tulee olla vahva ja sitä ei tulisi käyttää muissa palveluissa.

7. Salasanojen omatoimisen nollaamisen mahdollisuus tulisi ottaa käyttöön, mikäli käyttäjän salasanan nollauksen yhteydessä joudutaan lähettämään uusi salasana turvattomalla tavalla.

8. Sähköpostiviestien edelleen lähetystä koskevien sääntöjen luominen tulee olla mahdollista vain pääkäyttäjällä, näin pyritään estämään käyttäjätilin kaikkien sähköpostien edelleen lähetys ja viestiliikenteen seuraaminen hyökkääjän toimesta.

9. Asianajotoiminnan säilytysvelvollisuuden piirissä olevien tietojen varmuuskopiointi tulee järjestää luotettavasti.

10. Hyökkääjän sulkeminen pois 365-tilauksesta tulee ennalta suunnitella. Tulee muodostaa systemaattinen tapa hyökkääjän sulkemiseksi kattavasti pois palveluista ja laatia muistilista mahdollisesti tarvittavista toimista (kuten kaikkien palveluiden yhteyksien katkominen, tietosuojavaltuutetulle ja muille sidostyhmille ilmoittaminen, toimiston maksettavien laskujen sekä asiakkaiden tilitietojen muutosten oikeellisuuden varmistaminen hyökkäyksen jälkeen).

11. 365-tilausta käyttävien mobiililaitteiden suojaukseen tähtäävät toimet tulee ottaa käyttöön vähintään Asianajajaliiton tietoturvaohjeessa ja -oppaassa kuvatulla tavalla (laitteen salaus, automaattinen lukitus jne.).

Tässä liitteessä kuvattuja suojausmenetelmiä voi soveltaa myös muihin asianajotoiminnassa käytössä oleviin pilvipalveluihin.

Teknisempien yksityiskohtien osalta katso Kyberturvallisuuskeskuksen organisaatioiden ylläpidosta ja tietoturvasta vastaaville henkilöille suunnattu opas Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta.

Tämä Tietoturvaoppaan liite on valmisteltu Suomen Asianajajaliiton IT-valiokunnassa, joka on hyväksynyt sisällön 23.8.2021. Asianajajaliiton hallitus on hyväksynyt oppaan uudet liitteet kokouksessaan 24.9.2021.

LIITE 2

Salassapitosopimus (24.9.2021)

1. **Osapuolet**

   Tilaaja:

   [Asianajotoimisto Oy]
   [y-tunnus]

   [Osoite]

   Sopimuskumppani:

   _____

   _____

   _____

2. Tausta ja tarkoitus

Tilaaja kuuluu Suomen Asianajajaliittoon ja harjoittaa lain asianajajista (496/1958, jäljempänä ”Asianajajalaki”) mukaista asianajotoimintaa. Asianajaja on suojattu ammattinimike ja vain Suomen Asianajajaliiton jäsen saa käyttää nimikettä asianajaja.

Asianajajan tulee rehellisesti ja tunnollisesti täyttää hänelle uskotut tehtävät sekä kaikessa toiminnassaan noudattaa hyvää asianajajatapaa (Asianajajalaki 5 § 1 momentti ja Suomen Asianajajaliiton sääntöjen 33 §). Asianajajalla on Asianajajalain 5 c

§ mukainen ehdoton ja ajallisesti rajoittamaton salassapitovelvollisuus. Salassapitoa koskevia määräyksiä on lisäksi muissa laeissa. Suomen Asianajajaliiton hyvää asianajajatapaa koskevien ohjeiden kohdan 11.5 mukaisesti asianajajan on huolehdittava, että asianajotoimistolle palveluksia suorittavat henkilöt noudattavat salassapito- ja vaitiolovelvollisuutta.

Sopimuskumppani on halukas erikseen sovittavalla tavalla tarjoamaan palveluitaan Tilaajalle. Tilaaja ei voi Tilaajaa velvoittavien säännösten mukaisesti tilata tai käyttää Sopimuskumppanin palveluita ilman, että Sopimuskumppani sitoutuu vastaavaan salassapito- ja vaitiolovelvollisuuteen kuin mihin Tilaaja on itse velvoitettu. Sopimuskumppani on tietoinen asian merkityksestä. Näiden velvoitteiden täyttämiseksi Osapuolet sopivat seuraavaa:

3. Sopimusehdot

1. Tilaaja ja Sopimuskumppani ovat sopineet, sopivat tai aikovat sopia palveluista, joita Sopimuskumppani suorittaa vakituisesti tai tilapäisesti Tilaajalle tai tämän osoittamalle (nämä jäljempänä ”Palvelu” tai ”Palvelut”). Palvelun tuottamisesta sovitaan erikseen ja tämä Sopimus muodostaa erottamattoman osan Palvelun tuottamisen ehtoja. Tätä Sopimusta sovelletaan kaikkiin vastaisuudessa tilattaviin Palveluihin, olivatpa ne mitä palveluita tahansa.

2. Kaikki Tilaajan asiakkaita ja toimeksiantoja koskevat tiedot tai niiden osat, olivatpa ne mitä tietoja tahansa, esitetty missä muodossa tahansa, tai tulleet Sopimuskumppanin tietoon miten tahansa Palvelujen suorittamisen yhteydessä, ovat poikkeuksetta ehdottoman luottamuksellisia ja salassa pidettäviä (nämä tiedot jäljempänä ”Asianajosalaisuudet”). Selvyyden vuoksi, myös muutoin julkiset tiedot ovat Asianajosalaisuuksia.

3. Sopimuskumppanin on pidettävä kaikki Asianajosalaisuudet salassa ja luottamuksellisina (”Sopimuskumppanin Salassapito- ja vaitiolovelvollisuus”). Sopimuskumppanin Salassapito- ja vaitiolovelvollisuus koskee myös kaikkia niitä Asianajosalaisuuksia, jotka ovat mahdollisesti tulleet Sopimuskumppanin tietoon jo ennen tämän Sopimuksen allekirjoitusta suoritettujen Palvelujen yhteydessä.

4. Sopimuskumppanin Salassapito- ja vaitiolovelvollisuus on ikuinen eikä se ole mitenkään irtisanottavissa.

5. Mikäli Sopimuskumppania suoraan velvoittavasta laista, Sopimuskumppania velvoittavasta lakia alemman asteisesta säännöksestä tai muusta Sopimuskumppania velvoittavasta viranomaismääräyksestä taikka Sopimuskumppanin ja Tilaajan välisestä palvelusopimuksesta johtuu Sopimuskumppanille laajempi salassapito- tai toimimisvelvoite kuin mitä tällä Sopimuksella on sovittu, ei tämä Sopimus kavenna Sopimuskumppanin velvollisuuksia miltään osin.

6. Mikäli muussa Sopimuskumppanin ja Tilaajan välisessä sopimuksessa on sovittu tätä Sopimusta suppeammasta salassapito- tai toimimisvelvoitteesta, noudetaan tältä osin tätä Sopimusta.

7. Sopimuskumppani on velvollinen huolehtimaan, että jokainen Sopimuskumppanin henkilökuntaan kuuluva tai muuten Sopimuskumppanin Tilaajalle suoritettavien palvelujen toteutukseen osallistuva henkilö tai muu henkilö, jolla on pääsy Asianajosalaisuuksiin, sitoutuu henkilökohtaisesti vastaavaan salassapito- ja vaitiolovelvollisuuteen kuin mitä Sopimuskumppanin Salassapito- ja vaitiolovelvollisuus on, ellei vastaavasta salassapito- ja vaitiolovelvollisuudesta ole sovittu tämän henkilön työsopimuksessa. Sopimuskumppani on velvollinen Tilaajan pyynnöstä esittämään tällaisen sitoumuksen kopion tai muun selvityksen tämän ehdon mukaisen velvoitteen täyttämisestä.

8. Sopimuskumppanin on huolehdittava tarvittavin teknisin ja työjärjestelyratkaisuin, että vain niillä henkilöillä on pääsy Asianajosalaisuuksiin, joilla on siihen Palvelujen suorittamiseen liittyvä välttämätön tarve. Sopimuskumppanin on huolehdittava siitä, että niistä henkilöistä, joilla on fyysinen, tietotekninen tai muu pääsy Asianajosalaisuuksiin, pidetään luotettavaa ja ajantasaista rekisteriä. Sopimuskumppanin on mahdollisuuksien mukaan huolehdittava myös siitä, että tietoteknisten yhteyksien ottamista Asianajosalaisuuksiin valvotaan soveltuvin pysyvin lokitiedoin. Sopimuskumppanin on opastettava, tiedotettava ja koulutettava henkilökuntaansa Sopimuskumppanin Salassapito- ja vaitiolovelvollisuuden merkityksestä. Sopimuskumppanin on Tilaajan perustellusta pyynnöstä annettava Tilaajalle kopio, ote tai muu selvitys pidetyistä rekistereistä ja lokitiedoista.

9. Sopimuskumppani ei saa toisintaa, tallentaa, kopioida tai jäljentää Asianajosalaisuuksia muutoin kuin sillä tavoin kuin on välttämätöntä Sopimuskumppanin tarjoaman palvelun toteuttamiseksi tai nimenomaisesti erikseen Tilaajan kanssa sovittu. Sopimuskumppanin on huolehdittava siitä, että kaikki Asianajosalaisuuksista valmistetut kopiot hävitetään Palvelun suorittamisen jälkeen tai kun kopioita ei enää tarvita Palvelun suorittamiseksi, ellei niiden arkistoimisesta ole erikseen sovittu Tilaajan kanssa ja Tilaajan lukuun.

10. Sopimuskumppani ei ole oikeutettu luovuttamaan Asianajosalaisuuksia eteenpäin kolmansille tahoille kuten alihankkijoilleen tai omille palveluntarjoajilleen ilman, että tästä on erikseen kirjallisesti sovittu Tilaajan kanssa. Tällaisen kolmannen osapuolen on lisäksi sitouduttava vastaavaan salassa- pito- ja vaitiolovelvoitteiseen kuin mitä tässä Sopimuksessa on sovittu.

11. Sopimuskumppanin on noudatettava palvelujen suorittamisessa ja kaikessa Asianajosalaisuuksien käsittelyssä tietoturvan osalta toimialalleen soveltuvaa huolellisuutta ja yleisesti hyväksyttyjä käytänteitä.

12. Sopimuskumppanin on niin pian kuin mahdollista ilmoitettava Tilaajalle kaikista sellaisista Sopimuskumppanin tietoon tulevista tai epäillyistä seikoista kuten puutteista, poikkeamista, riskeistä ja vastaavista seikoista, joilla voi olla merkitystä Sopimuskumppanin Salassapito- ja vaitiolovelvollisuuden täyttämisen kannalta, koskivatpa nämä Sopimuskumppania, sen henkilöstöä tai kolmansia.

13. Mikäli Sopimuskumppanin tiloihin, tietojärjestelmiin tai muualle missä on mahdollisestikin Asianajosalaisuuksien kopioita, kohdistetaan kotietsintä tai muu viranomaisen tai muun valvovan tahon tarkastus, on Sopimuskumppanin ilmoitettava Asianajosalaisuuksien olemassaolosta välittömästi tarkastuksen suorittajalle ja oltava yhteydessä Tilaajaan niin pian kuin se on sallittua.

14. Mikäli Sopimuskumppani tai sen työntekijä tai muu suoritusapulainen rikkoo tätä Sopimusta, on Tilaajalla yksipuolinen oikeus purkaa Palvelujen tuottamista koskeva Sopimus välittömin vaikutuksin määräaikaisuuksista riippumatta. Tilaaja on velvollinen suorittamaan vain purkamiseen asti tehtyihin Palveluihin liittyvät veloitukset.

15. Sopimuskumppani on tietoinen, että Sopimuskumppanin Salassapito- ja vaitiolovelvollisuuden vähäinenkin rikkominen voi aiheuttaa Tilaajalle tai tämän asiakkaille tai muille tahoille mittaamattoman suurta ja yllättävää vahinkoa. Sopimuskumppani on velvollinen korvaamaan Tilaajalle, tämän asiakkaalle tai muulle vahinkoa kärsineelle kaikki vahingot, joita Sopimuskumppani tai sen suoritusapulaiset aiheuttavat Sopimuskumppanin Salassapito- ja vaitiolovelvollisuutta rikkomalla. Asianajosalaisuudet saattavat sisältää tietoja, joiden paljastaminen on rikosoikeudellisesti rangaistavaa.

16. Tätä Sopimusta voidaan muuttaa vain kirjallisesti.

17. Tähän Sopimukseen sovelletaan Suomen lakia.

18. Tästä Sopimuksesta aiheutuvat riidat ratkaistaan siinä käräjäoikeudessa, jonka tuomipiirissä Tilaajan kotipaikka sijaitsee.

[Sivun loppu on jätetty tarkoituksella tyhjäksi. Allekirjoitukset seuraavalla sivulla.]

4. Allekirjoitukset

Tilaaja

_____

Aika ja paikka

_____

Allekirjoitus

_____

Nimenselvennys

Sopimuskumppani

_____

Aika ja paikka

_____

Allekirjoitus

_____

Nimenselvennys

Tämä tietoturvaoppaan liite on valmisteltu Suomen Asianajajaliiton IT-valiokunnassa, joka on hyväksynyt sisällön 17.9.2021. Asianajajaliiton hallitus on hyväksy- nyt oppaan uudet liitteet kokouksessaan 24.9.2021.

LIITE 3 (14.12.2023)

[Organisaation logo]

[XX Asianajotoimisto Oy]

TIETOTURVAPOLITIIKKA

Versio:	
Versiopäivä:	
Luonut:	
Hyväksynyt:	
Luottamuksellisuustaso:	Sisäinen

Muutoshistoria

Päivä-määrä	Versio	Luonut	Muutoksen kuvaus

Sisällysluettelo

1. TARKOITUS, LAAJUUS JA KÄYTTÄJÄT 31

2. VIITEASIAKIRJAT 31

3. TIETOTURVAN PERUSTERMINOLOGIA 31

4. TIETOTURVAN HALLINTA 32

4.1. TAVOITTEET JA MITTAUS 32

4.2. TIETOTURVAA KOSKEVAT VAATIMUKSET 32

4.3. TIETOTURVAN RISKIENHALLINTA JA HALLINTAKEINOT 32

4.4. TOIMINNAN JATKUVUUS 32

4.5. TIETOTURVAN KOULUTUS 32

4.6. TIETOTURVAN VALVONTA 33

4.7. VASTUUT 33

4.8. TIETOTURVAPOLITIIKASTA VIESTIMINEN 33

5. TUKI TIETOTURVAN HALLINNAN TOTEUTUKSELLE 33

6. VOIMASSAOLO JA ASIAKIRJOJEN HALLINTA 34

Tarkoitus, laajuus ja käyttäjät

Tämän tietoturvapolitiikan tavoitteena on määritellä tietoturvan päämäärä tai tarkoitus, linjaukset sekä vastuut ja organisointi.

Politiikan käytäntöjä sovelletaan [XX Asianajotoimisto Oy] toimintaan.

Tämän asiakirjan käyttäjiä ovat kaikki [XX Asianajotoimisto Oy:n] työntekijät sekä asiaankuuluvat ulkoiset sidosryhmät.

Viiteasiakirjat

- Luettelo oikeudellisiin, sääntelyyn ja sopimuksiin liittyvistä vaatimuksista
- Riskienhallintapolitiikka
- Riskienkäsittelysuunnitelma
- Jatkuvuussuunnitelma
- Koulutussuunnitelma
- Auditointisuunnitelma
- [Toipumissuunnitelma]
- [Tieto-omaisuusluettelo]
- [Tietoturvahäiriöiden hallintamenettely]

Tietoturvan perusterminologia

Luottamuksellisuus – ominaista tiedolle, joka on vain valtuutettujen henkilöiden tai järjestelmien saatavilla.

Saatavuus – ominaista tiedolle, jota valtuutetut henkilöt voivat käyttää sitä tarvittaessa.

Eheys – ominaista tiedolle, jota vain valtuutetut henkilöt tai järjestelmät muuttavat sallitulla tavalla.

Tietoturva – tiedon luottamuksellisuuden, eheyden ja tietojen saatavuuden säilyttäminen.

Tietoturvan hallinta – osa kokonaisvaltaista hallintaprosessia, joka huolehtii tietoturvan suunnittelusta, toteuttamisesta, ylläpidosta, tarkistamisesta ja parantamisesta.

Tietoturvan hallinta

Tavoitteet ja mittaus

[XX Asianajotoimisto Oy] tietoturvan hallinnan yleiset tavoitteet ovat seuraavat: asiakastietojen salassapitäminen (luottamuksellisuus), lainsäädännön ja asianajotoimintaa koskevan sääntelyn vaatimusten noudattaminen, asianajoliiketoiminnassa tarvittavien tietojen käytettävyyden varmistaminen (saatavuus, eheys, käytettävyys), luotettavan asianajopalveluntarjoajan maineen ylläpitäminen tietoturvaosaamista ja tietoisuutta parantamalla, luotettavan asianajopalveluntarjoajan maineen ylläpitäminen mahdollisia tietoturvahäiriöitä vähentämällä ja estämällä. Tietoturvapolitiikka luo perustan [XX Asianajotoimisto Oy] liiketoiminnalle ja tietoturvallisuuden varmistamiselle.

[Tehtävänimike] vastaa näiden yleisten tietoturvan hallinnan tavoitteiden asettamisesta ja seurannasta. Kaikki tavoitteet on katselmoitava vähintään [kerran vuodessa] taikka jos tietoturva- tai toimistoympäristöön taikka keskeisiin järjestelmiin toteutetaan muutoksia.

Tavoitteiden saavuttamista tulee seurata säännöllisesti. Seurannan tulosten perusteella tulee laatia korjaavat toimenpiteet. [Tehtävänimike] on vastuussa seurannasta ja sen tulosten yksityiskohtien raportoimisesta [tehtävänimikkeelle].

Tietoturvaa koskevat vaatimukset

Tämän tietoturvapolitiikan ja koko tietoturvallisuuden hallinnan on oltava organisaation kannalta olennaisten tietoturvallisuutta koskevien oikeudellisten ja sääntelyyn liittyvien sekä sopimus- ja muiden olennaisten velvoitteiden mukainen.

Yksityiskohtainen luettelo kaikista sopimus- ja oikeudellisista vaatimuksista on Luettelo oikeudellisiin, sääntelyyn ja sopimuksiin liittyvistä vaatimuksista -asiakirjassa [sis. luettelon asianajotoimintaa koskevista säädöksistä ja alemmanasteisista normeista, sääntelyyn liittyvistä vaatimuksista (kuten tapaohjeita täydentävä velvoittava tietoturvaohje), sopimuksiin liittyvistä vaatimuksista (asiakkaiden vaatimukset, erilaiset sidosryhmien kanssa tehdyt sopimukset) ja muista olennaisista tietoturvavaatimuksista (esimerkiksi sisäiset vaatimukset).].

Tietoturvan riskienhallinta ja hallintakeinot

Tietoturvariskejä arvioidaan ja analysoidaan säännöllisesti niiden liiketoimintavaikutusten perusteella. Riskiarviointi tulee laatia myös toimisto- tai tietoturvaympäristön muuttuessa esimerkiksi uusien järjestelmien määrittelyvaiheessa ja merkittävien toiminnan kriittisyyteen vaikuttavien muutosten yhteydessä.

Toiminnan jatkuvuus

Tietoturvan ensisijaisena päämääränä on asianajotoiminnan jatkuvuuden turvaaminen kaikissa olosuhteissa. [Toiminnan jatkuvuuden hallinta on määritelty Jatkuvuussuunnitelmassa [ja Toipumissuunnitelmassa].]

Tietoturvan koulutus

Tietoturvaan liittyvä osaaminen varmistetaan säännöllisinä tietoturvakoulutuksina. Koulutukset on dokumentoitu [menetelmä tai järjestelmä].

Tietoturvan valvonta

Tietoturvan valvontaa suoritetaan säännöllisinä ulkoisina tietoturva-auditointeina. Auditoinneista pidetään kirjaa. Auditointi on tarkemmin määritelty Auditointisuunnitelmassa (liite x), joka määrittää auditointijaksot, auditointikriteerit, auditoinnin kattavuuden ja auditoijan. Auditointi voidaan suorittaa kokonaisuudessa yhdellä kerralla tai osissa niin, että kokonaisuus tulee katettua. Auditointisuunnitelmasta voidaan todentaa tehdyt ja tulevat auditoinnit.

Vastuut

Tietoturvanhallintaa koskevat vastuualueet ovat seuraavat:

- [tehtävänimike] on vastuussa sen varmistamisesta, että tietoturvan hallinta pantu täytäntöön ja sitä ylläpidetään tämän politiikan mukaisesti, ja sen varmistamisesta, että kaikki tarvittavat resurssit ovat käytettävissä
- [tehtävänimike] vastaa tietoturvan hallinnan toiminnan koordinoinnista sekä suorituskyvyn raportoinnista [poikkeamat, häiriötilanteet ja sidosryhmien palaute]
- [Ylimmän johdon] on katselmoitava tietoturvan hallinta vähintään kerran vuodessa tai aina, kun merkittävä muutos tapahtuu, ja laadittava pöytäkirjat katselmoinnin kokouksesta. Johdon katselmuksen tarkoituksena on selvittää tietoturvan hallinnan soveltuvuus, riittävyys ja tehokkuus [suhteessa riskeihin]
- [tehtävänimike] toteuttaa tietoturvakoulutussuunnitelman työntekijöille
- tieto-omaisuuden eheyden, käytettävyyden ja luottamuksellisuuden suojaaminen on kunkin tieto-omaisuuserän omistajan vastuulla
- kaikista tietoturvahäiriöistä tai -heikkouksista on ilmoitettava [tehtävänimikkeelle]
- [tehtävänimike] määrittelee, mitä tietoturvaan liittyviä tietoja kommunikoidaan millekin sidosryhmälle (sekä sisäiselle että ulkoiselle), kenen toimesta ja milloin
- [tehtävänimike] vastaa koulutus- ja valistussuunnitelman hyväksymisestä ja täytäntöönpanosta, jota sovelletaan kaikkiin henkilöihin, joilla on rooli tietoturvan hallinnassa.

Tietoturvapolitiikasta viestiminen

[Tehtävänimikkeen] on varmistettava, että kaikki [organisaation nimi] työntekijät sekä asianmukaiset ulkoiset sidosryhmät tuntevat tämän Tietoturvapolitiikan.

Tuki tietoturvan hallinnan toteutukselle

[Hallitus/johtoryhmä] ilmoittaa, että tietoturvan hallinnan täytäntöönpanoa ja jatkuvaa parantamista tuetaan riittävillä resursseilla, jotta voidaan saavuttaa kaikki tässä politiikassa asetetut tavoitteet ja täyttää kaikki tunnistetut vaatimukset.

Voimassaolo ja asiakirjojen hallinta

Tämä asiakirja on voimassa [päivämäärä].

Tämän tietoturvapolitiikan omistaja on [tehtävänimike], jonka on katselmoitava ja tarvittaessa päivitettävä tämä asiakirja [vähintään kerran vuodessa].

[tehtävänimike]

[nimi]

_____

[allekirjoitus]

LIITE 4 AUDITOINTIOPAS (14.12.2023)

Tietoturvaohje (B 05.1) velvoittaa yli 10 työntekijän asianajotoimistoa järjestämään ulkoisen tietoturva-auditoinnin säännöllisin väliajoin ja määrättyjen muutosten toteutuessa sekä pitämään auditoinneista kirjaa.

Taustaksi

Tämän auditointioppaan tarkoituksena on määrittää auditoinnin laajuus asianajotoimistossa, jos toimintaan ei sovelleta jotakin muuta yleisesti hyväksyttyä tietoturvastandardia (kuten International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001 -standardia). Yleisesti hyväksyttyihin tietoturvastandardeihin kuuluu erillisen auditointiohjelman laatiminen ja säännöllinen auditointi osana tietoturvastandardin ylläpitoa.

Tietoturva-auditointi on käytäntö, jonka tehtävänä on parantaa tietoturvallisuuden hallintaa toimistossa. Auditoinnissa voidaan löytää piileviä kehityskohteita, jotka saattavat vaarantaa asianajotoiminnan ja paljastaa asianajosalaisuuden alaisia luottamuksellisia tietoja. Tietoturvallisuusympäristössä tapahtuvat ei-toivotut muutokset ja virheet ovat luonnollisia tapahtumia, joita ei voida kokonaan välttää. Auditointia voidaan hyödyntää yhtenä tehokkaimpana keinona niiden löytämiseksi ja korjaamiseksi.

Tietoturva ohjeen velvoittama säännöllinen auditointi kannattaa hyödyntää keinona toimiston tietoturvatoiminnan jatkuvaksi parantamiseksi.

Auditointisuunnitelma ja auditointiraportti

Auditointisuunnitelma määrittää tavallisesti auditointijaksot, auditointikriteerit, auditoinnin kattavuuden ja auditoijan. Auditoinnin suorittaminen on suositeltavaa tehdä vuosittain. Auditointi voidaan suorittaa kokonaisuudessa yhdellä kerralla tai osissa niin, että kokonaisuus tulee katettua. Auditointisuunnitelmasta voidaan todentaa tehdyt ja tulevat auditoinnit.

Auditointiraportti kuvaa auditoinnin aikana tehdyt havainnot ja poikkeamat vaatimuksien vastaisesta toiminnasta. Poikkeama kirjataan tyypillisesti silloin kun toiminta ei täytä laisinkaan sille asetettua vaatimusta. Havainto voi kuvata vaatimuksien osittaista täyttämättä jättämistä tai positiivista havaintoa koskien toimintaa. Auditointiraportista voidaan todentaa auditoinnin löydökset ja korjaamista vaativat toimet.

Auditoija

Auditoijan tulee olla pätevä auditoinnin suorittamiseen, vaikka varsinaisia kriteerejä auditoijalle ei ole asetettu. Auditoijan tulisi tuntea vaatimukset, käytännössä Asianajajaliiton tietoturvaohje (B 05.1), jota vastaan auditointi suoritetaan ja yleinen toimintaympäristö, joissa vaatimuksia toteutetaan.

Auditoijalla tulisi olla kokemusta auditointiprosessista, jotta auditoinnin löydökset ja niistä tehtävä raportti pystytään hyödyntämään toiminnan kehittämiseksi.

Olennaista on, että auditoinnin tekee taho, joka ei vastaa olemassa olevan ICT-ympäristön ylläpidosta ja hallinnasta.

Auditoinnin kulku

Auditointi jakautuu yleensä vaiheisiin, joissa kukin vaihe pitää sisällään erityisiä tehtäviä kuten tietoturvadokumentaation katselmus, auditoinnin tarkastuslistan laatiminen, varsinaisen auditoinnin suorittaminen, raportointi ja korjaavien toimien seuranta.

Asianajotoiminnan tietoturva-auditointi suoritetaan Asianajajaliiton minimissään tietoturvaohjeen (B 05.1) vaatimuksia vastaan. Käytännössä auditoija huomioi kuitenkin myös toimiston oman tietoturvallisuusympäristön asettamat muut vaatimukset.

Ensimmäisessä vaiheessa, tietoturvadokumentaation katselmuksessa, kerätään tarvittava dokumentaatio yhteen (kuten Asianajajaliiton tietoturvaohje (B 05.1) ja toimiston oma tietoturvallisuuden ohjeistus) läpikäyntiä varten ja listataan dokumentaatiosta asiat, jotka halutaan tarkastaa.

Auditoinnin tarkastuslistaan kirjataan auditoinnissa tarkastettavat asiat: vaatimuksen lähde ja tarkastettava asia, tarkastettavat järjestelmät, haastattelukysymykset, aikataulu, jne.

Varsinaisessa auditoinnissa, auditoija valitsee lähteen vaatimukselle, tarkastettavan kohteen ja todentaa toimitaanko vaatimuksen mukaan. Tämä voidaan tehdä havainnoin ja haastatteluin. Löydökset ja niitä koskevat muistiinpanot voidaan kirjata tarkastuslistaan asian todentamiseksi.

Auditointiraporttiin kirjataan auditoinnissa löydetyt poikkeamat ja havainnot. Poikkeaman kirjaaminen tulee tehdä sillä tarkkuudella, että sen perusteella on mahdollista tehdä sille korjaavat toimenpiteet. Poikkeaman kirjaaminen tulisikin perustua varsinaisessa auditoinnissa tehtyihin muistiinpanoihin.

Auditoinnin tarkastuslistan kysymyksiä

Alla olevan tarkastuslistan kysymysten on tarkoitus toimia toimiston oman toiminnan tietoturvallisuuden arvioimisen tukena esimerkiksi auditointiin valmistauduttaessa. Tarkastuskysymyksillä voidaan arvioida toimiston tietoturvallisuuden tilaa Asianajajaliiton tietoturvaohjeen (B 05.1) velvoittavia kohtia vastaan.

Tarkastuskysymyksessä on määritetty Tietoturvaohjeen kohdan asettama vaatimus toiminnalle ja vaatimuksenmukaisuutta määrittävä esimerkkikysymys.

Auditoinnin tarkastuskysymykset

Tarkastuskysymykset Asianajajaliiton B tietoturvaohjeen (05.1) mukaisesti.

Ohjekohta	Vaatimus	Vaatimuksen- mukaisuus Kyllä / Ei	Vaatimuksen- mukaisuuden todentaminen
1. Koulutus	Onko toimistolle laadittu koulutussuunnitelma?		
	Onko koulutuksista saaduista pätevyyksistä tallenteita?		
2. Tietoturva-politiikka	Onko toimistolla tietoturvapolitiikka kuvattuna?		
	Onko politiikassa kuvatut tietoturva-periaatteet ylimmän johdon hyväksymät?		
3. Tietoturva-auditointi	Onko toimistossa toteutettu tietoturva-auditointi, jossa tietoturvallisuutta on arvioitu Asianajajaliiton B 05.1 Tietoturvaohjeen vaatimuksia vastaan, lainsäädännön vaatimuksia vastaan ja toimiston omia itselleen asettamia tietoturvallisuuden vaatimuksia vastaan?		

	Onko tietoturva-auditointi toteutettu säännöllisesti?		
	Onko tietoturva-auditointi toteutettu keskeisiin järjestelmiin kohdistuvien muutosten jälkeen? [vaatimuksen kohdentaminen/todentamisperuste?]		
	Onko tietoturva-auditointi toteutettu tietoturvaympäristöön kohdistuvien muutosten jälkeen? [vaatimuksen kohdentaminen/todentamisperuste?]		
	Onko tietoturva-auditointi toteutettu toimistoympäristöön kohdistuvien muutosten jälkeen? [vaatimuksen kohdentaminen/todentamisperuste?]		
4. Tarkastukset	Onko asianajotoiminnan järjestämistä, asiakkuuksia ja toimeksiantoja koskevat tiedot suojattu, erilleen ja salassa pidettyjä toimistoon kohdistuvien tarkastusten ajan?		
5.Tietoturvaperiaatteet	Onko toimistolla kuvatut tietoturvaperiaatteet?		
	Ovatko kuvatut periaatteet ylimmän johdon hyväksymät toimintaperiaatteiksi? [joilla se sitoutuu vastaamaan vaatimuksiin >]		
	Onko tietoturvaperiaatteissa huomioitu lainsäädännön ja sääntelyn asianajotoiminnalla asettamat vaatimukset?		
	Onko tietoturvaperiaatteissa huomioitu toimistossa tehtyjen sopimusten sille asettamat vaatimukset?		

	Ohjaavatko tietoturvaperiaatteet toimintaa käytännön tasolla?		
6. Toimitilaturvallisuus	Ovatko toimitilan ovet ja muut kulkuaukot lukittu niin, että vain oikeutetut henkilöt pääsevät kulkemaan niistä?		
	Ovatko kaikki asianajajasalaisuuden piiriin kuuluvat aineistot (kuten paperiaineistot, tallennusvälineet) säilytetty suojatusti toimitiloissa?		
7. Ohjelmistot ja palvelut	Ovatko asianajotoiminnassa käytettävät ohjelmistot yrityskäyttöön tarkoitettuja ohjelmistoja?		
	Ovatko asianajotoiminnassa käytettävät palvelut kuten pilvipalvelut yrityskäyttöön tarkoitettuja palveluita?		
	Onko muunlaisen kuin yrityskäyttöön tarkoitetun ohjelmiston tai palvelun käytöstä asiainhoitamisessa sovittu todennettavasti asiakkaan kanssa?		
8. Laite- ja pääsynhallintaratkaisu (yli 10 työntekijän toimistossa)	Ovatko asianajotoiminnassa käytettävät tietokoneet ja mobiililaitteet laitehallinnalla hallittuja laitteita?		
	Ovatko asianajotoiminnassa käytettävillä tietokoneilla ja mobiililaitteilla pääsynhallintaratkaisulla toteutettu pääsynhallinta niin, että vain oikeutetut käyttäjät pystyvät käyttämään laitteita?		

9. Salaus	Ovatko asianajotoiminnassa käytettävät tietokoneet, mobiililaitteet, tallennusmediat salattu?		
	Ovatko asiakastietoja sisältävät taulukot, tietokannat, pilvipalvelut salattu?		
	Ovatko asianajotoiminnassa käytettävät laitteet kuten tietokoneet, mobiililaitteet [ja tulostimet] ainoastaan asiaa ajavan henkilön käytössä?		
	Käytetäänkö asianajotoiminnassa ainoastaan siihen nimenomaisesti turvalliseksi määritettyjä laitteita?		
	Ovatko turvallisiin laitteisiin kytkettävät lisälaitteet määritetty turvallisiksi?		
	Saavatko kaikki asianajotoiminnassa käytettävät laitteet laitevalmistajan säännöllisesti julkaisemat, ajantasaiset ohjelmistopäivitykset?		
	Tyhjennetäänkö tiedot käytöstä poistettavista laitteista, tietoturvallisesti niin, että tietoja ei ole enää mahdollista palauttaa?		
10. Verkot	Onko toimistossa käytössä oleva verkko suojattu niin, että siihen voi kytkeytyä vain oikeutetulla laitteella?		
	Ovatko toimiston langattomat verkot salattu ajanmukaisella, pätevällä salauksella?		
	Onko julkisen verkon yli käytetyt yhteydet salattu pätevästi [versio] (kuten VPN, TLS)?		

11. Salasanat	Onko salasanakäytäntö olemassa?		
	Vaaditaanko salasanakäytännössä riittävän pitkiä ja monimutkaisia (isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä) salasanoja?		
	Onko salasanakäytännössä määritetty tapaukset, jolloin salasana tulee vaihtaa?		
	Onko salasanakäytännössä määritetty salasanojen turvallinen säilyttäminen?		
	Onko salasanakäytännössä määritetty vahvan tunnistautumisen (kuten monivaiheisen todentamisen) käytölle vaatimukset?		
12. Tietoturva-ohjelmistot	Onko asianajotoiminnassa käytettävillä laitteilla tarpeenmukainen tietoturvaohjelmisto käytössä?		
	Onko asianajotoiminnassa käytettävillä laitteilla tarpeenmukainen palomuuriohjelmisto käytössä?		
	Onko käyttäjärajoituksia ohittamaan kykenevät tietoturvaohjelmistot rajoitettu vain järjestelmävalvojien käyttöön?		
	Onko järjestelmävalvojien käyttäjätunnukset rajoitettu toimenkuvan ja osaamisen mukaan niitä tarvitseville henkilöille?		
	Käytetäänkö järjestelmävalvojan tunnuksia ainoastaan silloin kun kyseistä oikeustasoa tarvitaan (kuten järjestelmän hallinnointitoimet)?		

	Asennetaanko kaikkien asianajotoiminnassa käytettävien laitteiden, käyttöjärjestelmien, ohjelmistojen, sovellusten päivitykset suunnitelmallisesti ja päivityksen julkaisemisen jälkeen ilman aiheetonta viivästystä?		
13. Pääsyoikeudet	Rajoitetaanko käyttäjien pääsyoikeutta tietoihin heidän työtehtävästänsä, johtuvan tiedon tarpeen mukaan?		
14. Varmuuskopiointi	Varmuuskopioidaanko kaikki B 10 Asiakirjojen säilyttämistä koskeva ohje -vaatimuksen mukaiset aineistot?		
	Tehdäänkö varmuuskopiointi säännöllisesti?		
	Onko varmuuskopiot mitoitettu perustuen arvioon tietojen enimmästä hyväksyttävästä menettämisen määrästä?		
	Ovatko myös pilvipalvelut varmuuskopioitu säilyttämistä koskevien vaatimusten mukaisesti?		
	Onko varmuuskopioiden säilytysaika riittävä?		
	Ovatko varmuuskopiot salattu ja turvallisesti säilytetty?		
	Ovatko varmuuskopioitujen tietojenpalautuksen testaukset suoritettu onnistuneesti?		
15. Toimittaja-turvallisuus	Onko toimittajien kanssa tehty tietoturvavaatimukset täyttävät tietoturvasopimukset?		

	Onko toimittajien kanssa tehty tietoturvavaatimukset täyttävät salassapitosopimukset?		
	Onko toimittajien kanssa sovittu pääsyoikeuksien rajaamisesta työtehtävien mukaisiksi?		
	Onko toimittajien kanssa sovittu pääsyoikeuksien ajantasaisuuden säännöllisestä tarkastamisesta?		
	Onko toimittajan kanssa sovittu tarpeenmukaisesta tietojen siirrettävyydestä toiseen palveluun?		
	Onko toimittajan kanssa sovittu tietojen tuhoamisesta palvelun käytön päättyessä?		
16. Viestinnän salaaminen	Täyttääkö asianajotoiminnassa käytetty viestintäkanava tiedolle asetetut tietoturvavaatimukset?		
	Onko toimistossa määritetty salassa pidettävälle tiedolle hyväksytyt viestintäkanavat?		
	Käytetäänkö sähköpostitse lähetettävällä salassa pidettävälle tiedolle salattua sähköpostia?		
	Onko asiakkaan kanssa sovittu salassa pidettävän tiedon lähettämisen tavoista?		
	Onko asiakkaan kanssa sovittu salassa pidettävän viestinnän tavoista?		

17. Aineistot	Täyttävätkö asianajotoiminnan aineistot niiden tallennukselle asetetut vaatimukset?		
	Täyttävätkö asianajotoiminnan aineistot niiden säilytykselle asetetut vaatimukset?		
	Täyttävätkö asianajotoiminnan aineistot niiden arkistoinnille asetetut vaatimukset?		
	Täyttävätkö asianajotoiminnan aineistot niiden tuhoamiselle asetetut vaatimukset?		
18. Käytöstä poisto	Ovatko kaikki käytöstä poistetut laitteet kuten tietokoneet, mobiililaitteet ja tallennuslaitteet tyhjennetty tiedoista niin, että tietoja ei ole mahdollista palauttaa laitteeseen?		
	Ovatko kaikki käytöstä poistetut verkon kautta toimivat tallennuspaikat tyhjennetty tiedoista niin, että tietoja ei ole mahdollista palauttaa?		
19. Toiminnan jatkuvuuden turvaaminen	Ovat toiminnan jatkuvuuden kannalta oleelliset tiedot huolellisesti selvitetty?		
	Ovatko toiminnan jatkuvuuden kannalta oleelliset tiedot dokumentoitu?		
	Ovatko toiminnan jatkuvuuden kannalta oleelliset dokumentit käytettävissä häiriötilanteessa, niitä tarvitsevilla henkilöillä?		

LIITE 5

TEKOÄLYTYÖKALUT ASIANAJAJAN TYÖSSÄ

Erilaisia tekoälyyn perustuvia julkisia työkaluja tai tekoälyjärjestelmiä on saatavana runsaasti. Näistä monet soveltuvat myös asianajajan työhön. Tällaisia ovat esimerkiksi Open AI:n ChatGPT, Googlen Gemini ja Microsoftin Copilot. Nämä työkalut voivat tehostaa työskentelytapoja ja nopeuttaa erityisesti suurien aineistojen läpikäyntiä sekä parantaa työn tarkkuutta. Tekoälyjärjestelmistä voi myös saada uudenlaisia näkökulmia käsillä olevaan oikeudelliseen ongelmaan.

Asianajajan on huolehdittava kaikessa toiminnassaan salassapito- ja vaitiolovelvollisuutensa täyttämisestä sekä noudatettava tekoälyä hyödynnettäessä aina hyvää asianajajatapaa. Asianajaja vastaa henkilökohtaisesti asiakkaalle annettavasta neuvosta.

Useat tekoälytyökalut käyttävät oletusarvoisesti kaikkea niille syötettyä aineistoa tekoälyn oppimismateriaalina. Tällaista aineistoa ovat esimerkiksi tekoälytyökalulle esitetyt kysymykset taustatietoineen ja tekoälytyökalulle analysoitavaksi ladatut tiedostot. Tällöin riskinä on, että tekoälytyökalulle syötetty salassapidettävä materiaali tulee yleisesti saataville.

Joidenkin tekoälytyökalujen asetukset ovat säädettävissä niin, että työkalu ei käytä sille syötettyä aineistoa tekoälyn opettamistarkoituksessa.

Riippumatta siitä, käyttääkö tekoälyjärjestelmä sinne syötettyä tietoa oppimistarkoituksissa vai ei, tekoälyjärjestelmälle ei saa ilmaista mitään sellaista, josta asianajajalla on salassapitovelvollisuus. Vaikkei tekoälyjärjestelmä käyttäisi käyttäjän syöttämää tietoa oppimistarkoituksissa, tieto siitä huolimatta lähetetään tekoälyjärjestelmän palvelimille eikä asianajaja voi kontrolloida sitä, miten tietoa käytetään ja tallennetaan jatkossa.

Yleiseen käyttöön tarkoitetuille tekoälytyökalulle ei saa syöttää sellaisia kysymyksiä, jotka sisältävät asianajotoiminnassa salassa pidettäviä tietoja, eikä työkalulle voi luovuttaa analysoitavaksi asiakkaan salassa pidettäviä tietoja sisältäviä asiakirjoja.

- Tekoälytyökalulle ei voi antaa luettavaksi asiakkaan tietoja sisältävää perukirjaa tai osakassopimusta,

- Tekoälytyökalun voi pyytää tutustumaan minkä tahansa lain hallituksen esitykseen tai pörssiyhtiön vuosikertomukseen, mutta ei mihinkään sellaiseen asiakirjaan, joka ei ole julkinen.

- Tekoälylle voi esittää kysymyksiä mistä tahansa aiheesta, mutta kysymykset eivät saa pitää sisällään asiakkaan salassa pidettäviä tietoja tai asiakkaan olosuhteisiin liittyviä vaitiolovelvollisuuden alaisia tietoja. Asianajaja ei saa ilmaista avustavansa tiettyä asiakasta tai hoitavansa tiettyä toimeksiantoa.

Mikäli asianajotoimiston sisäisessä tai yksityisessä käytössä olevassa tietoverkossa toimii sinne erikseen suunniteltu tekoälyä hyödyntävä niin sanottu suljettu järjestelmä, asianajotoimiston on kiinnitettävä erityistä huomiota siihen, miten ja minne järjestelmälle syötetyt tiedot tallennetaan ja kenellä on niihin pääsy ja kuka voi vaatia tietojen poistamista.

Asianajajan salassapitovelvollisuus vaarantuu, mikäli asianajaja syöttää tekoälyjärjestelmien ohella esimerkiksi internethakuun, kääntäjään tai muuhun julkisessa verkossa olevaan työkaluun salassa pidettäviä tietoja. Esimerkiksi Googlen kääntäjällä ei voi käännättää mitä tahansa salassa pidettäviä tietoja sisältäviä tekstejä.