B 05.3 SUOSITUS TIETOSUOJASTA ASIANAJOTOIMINNASSA (10.12.2020)

Suomen Asianajajaliiton hallitus on 10.12.2020 antanut asianajotoimintaan liittyvästä henkilötietojen käsittelystä seuraavan suosituksen, joka tulee voimaan 1.1.2021.

Tietosuojavelvoitteista yleisesti

Euroopan Unionin yleistä tietosuoja-asetusta 2016/679 (eng. General Data Protection Regulation, jäljempänä tietosuoja-asetus) on sovellettu kaikissa EU:n jäsenmaissa 25. toukokuuta 2018 alkaen. Sääntely velvoittaa dokumentoimaan henkilötietojen käsittelytoimet entistä huolellisemmin ja huolehtimaan rekisteröityjen, kuten esimerkiksi asiakkaiden ja työntekijöiden, läpinäkyvästä informoinnista koko henkilötiedon käsittelyn elinkaaren ajan. Euroopan Unionin lainsäädäntöä on täydennetty kansallisella sääntelyllä, muun muassa tietosuojalailla 1050/2018.

Asianajotoimistot ovat koosta ja oikeudenalasuuntautuneisuudestaan riippumatta tietosuoja-asetuksen soveltamisen piirissä. Vaikka asianajotoimintaa sääntelevä kansallinen erityislainsäädäntö myöntääkin joiltain osin poikkeuksia tietosuoja-asetuksen velvoitteisiin, se asettaa toisaalta asianajotoimistoille korostetun huolellisuusvelvoitteen henkilötietojen käsittelyssä ja suojaamisessa, ennen muuta asianajajan salassapitovelvollisuuden vuoksi.

Tietosuojanäkökulmasta erityisen olennainen asianajotoimintaan liittyvä ominaispiirre on erityisiin henkilötietoryhmiin kuuluvien (ns. arkaluonteisten) henkilötietojen käsittely osana toimeksiantotyötä, minkä vuoksi asianajotoimistojen tulisikin kiinnittää erityistä huomiota riskiperusteiseen henkilötietojen suojaukseen sekä käsittelyn lainmukaisuuteen.

Suositus henkilötietojen käsittelystä asianajajan toimeksiantotyössä

Tähän kahdeksan ydinkohdan tietosuojasuositukseen on koottu asianajotoimiston keskeisimmät tietosuojavelvoitteet sen käsitellessä henkilötietoja osana toimeksiantojen hoitamista. Tarkastuslistaa seuraamalla asianajotoimisto voi tarkistaa, että sen suorittamassa *toimeksiantoihin liittyvässä henkilötietojen käsittelyssä* on huomioitu tärkeimmät tietosuojavelvoitteet. Toimiston tulee kuitenkin arvioida myös muiden henkilötietojen käsittelyä ja toteuttaa niiden suojaamista koskevat toimenpiteet.

1. Käsittelyperusteiden arviointi
Kartoita toimiston käsittelemät henkilötiedot ja niiden sijainnit. Huomioi erityisesti GDPR 9 artiklan erityisvaatimukset arkaluonteisten henkilötietojen osalta. Arvioi määriteltyjen tarkoitusten valossa jokaisen henkilötietoryhmän tarpeellisuus ja huolehdi tarpeettomaksi tulleiden henkilötietojen poistamisesta tai anonymisoimisesta.

2. Informointi
Laadi tietosuojaseloste ja liitä se asianajotoimiston nettisivuille, yleisiin ehtoihin ja/tai toimeksiantosopimuksiin informoimaan asiakkaita heidän henkilötietojensa käsittelystä.

Mikäli käsittely olennaisesti muuttuu, päivitä tietosuojaseloste ja ilmoita rekisteröidyille uudesta tietosuojaselosteesta ja muutosten syistä oma-aloitteisesti.

3. Tietoturvan toteuttaminen
Toteuta riskeihin suhteutetut organisatoriset ja tekniset turvaamistoimenpiteet (auditointi, pseudonymisointi, salaus ym.) noudattamalla myös asianajajia velvoittavaa tietoturvaohjetta B 5.1 ja sitä selostavaa opasta B 5.2.

4. Sopimukset
Laadi GDPR 28 artiklan mukaiset tietojenkäsittelysopimukset sellaisten ulkopuolisten palveluntarjoajien kanssa, jotka käsittelevät henkilötietoja asianajotoimiston puolesta ja sen lukuun. Mikäli tällainen ulkopuolinen toimija tai henkilötietoja sisältävä palvelin sijaitsee Euroopan talousalueen ulkopuolella, huolehdi että tietojenkäsittelysopimuksen lisäksi siirto ETA-alueen ulkopuolelle on turvattu jollakin tietosuoja-asetuksessa vahvistetulla siirtomekanismilla (liitä tietojenkäsittelysopimuksen oheen komission laatimat mallisopimuslausekkeet).

5. Vastuut toimistossa
Laadi tai päivitä toimiston sisäinen tietosuojapolitiikka ja/tai ohjeet henkilötietojen käsittelylle. Määritä sisäiset käytännöt ja ilmoitusmenettely tietoturvaloukkausten varalta sekä suhteessa viranomaisiin että yksilöihin, joita loukkaus koskee. Huolehdi viestinnästä organisaation sisällä, jotta henkilöstö osaa käsitellä henkilötietoja tietoturvallisesti.

6. Kouluttaminen
Varmista, että toimistossasi on henkilö, joka vastaa tietosuojadokumenteista ja toimii yhteyshenkilönä suhteessa rekisteröityihin ja viranomaisiin. Huolehdi asianmukaisesta ja säännöllisestä toimiston työntekijöiden tietosuojakoulutuksesta.

7. Prosessit
Huolehdi, että toimisto kykenee vastaamaan ja toteuttamaan henkilötietojen tarkistamista koskevat pyynnöt kuukauden määräajan puitteissa. Kiinnitä erityistä huomiota seuraaviin seikkoihin: pyynnön lähettäneen yksilön tunnistaminen; relevantin henkilötiedon paikantaminen järjestelmistä sekä pyyntöjen kieltäytymisen perusteet (asianajajasalaisuus). Luo prosessit, joiden avulla voidaan arvioida henkilötietojen tarpeellisuutta ja ajantasaisuutta.

8. Dokumentaatio
Huolehdi, että seuraavat seikat on todennettavasti dokumentoitu: käsiteltävät henkilötiedot; käsittelyn tarkoitus ja laillinen peruste; ulkopuoliset, joille henkilötietoja siirretään ja tietosuoja-asetuksen mukainen siirtoperuste; organisatoriset ja tekniset tietoturvatoimenpiteet; henkilötietojen säilytysajat tai vähintäänkin säilytysajan määrittävät kriteerit; toimiston suorittamat sisäiset koulutukset ja tarkastukset sekä yksilölle suunnatut tietosuojaselosteet.

Laadi kirjalliset arviot siitä, edellyttääkö jokin käsittelytoimi vaikutustenarvioinnin (GDPR 35 art.) laatimista tietosuoja-asetuksen mukaisesti ja tarvittaessa suorita tällainen toimi.