EU:n tietosuoja-asetus

“From Compliance to Accountability”

KPMG Finland

kpmg.fi

KPMG:n tuella

- tietosuojahaasteet ja riskit johdon tietoisuuteen
- selkeät vastuut ja roolitukset organisaatiossa
- henkilötietojen tehokas ja lainmukainen käyttö koko tiedon elinkaaren ajan
- oikeudellisten ja taloudellisten riskien sekä maineriskien välttäminen
- valmius osoittaa valvontaviranomaisille organisaation vaatimustenmukaisuus tehokkaasti ja kattavasti
- asiakkaiden ja sidosryhmien luottamuksen vahvistaminen osoittamalla toiminnan vastuullisuus
- tietojenkäsittelyn ulkoistusten ja sopimusten tehokas hallinta
- henkilöstön osaamisen varmistaminen lainsäädännön ja parhaiden käytäntöjen mukaisesti
- tietovuotoihin varautuminen etukäteen sekä julkisuuden hallinta
- tietosuojavastaavalle riittävä osaaminen

Tietosuoja perusoikeutena korostuu modernissa yhteiskunnassa, ja rekisterinpitäjillä on ratkaiseva rooli henkilötietojen suojan toteuttamisessa jokapäiväisessä liiketoiminnassa. Liiketoimintaan ja henkilötietoihin kohdistuvat riskit kasvavat, ja uuden lainsäädännön myötä rekisterinpitäjiä tulevat koskemaan tiukemmat vaatimukset.

Kuinka organisaationne on varautunut tietosuojalainsäädännön murrokseen? Rekisterinpitäjälle on ensiarvoisen tärkeää huolehtia henkilötietojen käsittelyn lainmukaisuudesta laadukkailla ja tehokkailla prosesseilla, sillä jatkossa sääntelyn vastaisista toimista ja velvollisuuksien laiminlyönnistä voidaan määrätä tuntuvat sanktiot. Vaatimustenmukaisuudella vältetään niin taloudellisia, juridisia kuin maineeseen liittyviä riskejä.

KPMG on tietoturvan ja tietosuojan alalla Suomen johtavia neuvonta- ja auditointipalvelujen tarjoajia. KPMG on ainoa suomalainen virallisesti hyväksytty tietoturvallisuuden arviointilaitos, joka voi tehdä tietosuojan varmennuslausuntoja ISAE-standardin mukaisesti. Tarjoamme asiakkaillemme oikein mitoitetut ratkaisut ja tarvittavat tuki- ja auditointipalvelut vaatimustenmukaisen ja kustannustehokkaan kontrolliympäristön rakentamiseksi, ylläpitämiseksi ja todentamiseksi.

Mitä uutta?

1. Osoitus-velvollisuus

Toteuta asianmukaiset kontrollit ja osoita tarvittaessa vaatimustenmukaisuus

2. Privacy by Design

Sisällytä tietosuoja prosesseihin ja teknologiaan jo suunnitteluvaiheessa

3. DPIA

Suorita tietosuojan vaikutustenarviointi (Data Protection Impact Assessment) ennen uusien palvelujen/ teknologioiden käyttöönottoa

4. Tietosuoja-vastaava

Nimitä, resursoi ja kouluta organisaatioosi tietosuojavastaava

5. Varaudu tietoturva-loukkauksiin

Kehitä valmiudet tietovuotojen havainnointiin, hallintaan sekä viranomaisilmoituksen tekemiseen

6. Sanktiot

Jopa 20 MEUR tai 4 % globaalista liikevaihdosta, tietosuoja-asetuksen vastaisista toimista

KPMG Privacy Services

Tietosuojan hallinnan suunnittelu

Nykytilan ja kypsyystason arviointi / gap-analyysit

Tietosuojariskien analyysit ja vaikutusten arvioinnit (DPIA Data Protection Impact Assessment)

Tietosuojan kehitystyön tuki

Tietosuoja-auditoinnit

Tietosuojavastaavan tuki / ulkoistettu tietosuojavastaava

Tietovuotojen hallinta

Tietosuojakoulutukset

Tietosuojavastaavan kouluttaminen

Henkilötietojen käsittelyn ulkoistusten/sopimusten konsultointi ja arviointi

Juridiset erillisselvitykset

ISAE 3000-varmennuslausunnot (vaatimustenmukaisuuden todentaminen)

Tietosuoja-asetuksen tuoma murros

Yrityksen tietosuojatoimia sääntelee toukokuusta 2018 alkaen EU-tasolla yleinen tietosuoja-asetus. Asetus on suoraan sovellettavaa oikeutta ja koskee kaikkia rekisterinpitäjiä sekä henkilötietojen käsittelijöitä EU:n alueella. Tietosuojaviranomaisten toimivaltaa laajennetaan samalla kun rekisterinpitäjien omavalvontaa ja näyttövelvollisuutta korostetaan, huomattavien sanktioiden uhalla. Rekisterinpitäjän tulee jatkossa kyetä osoittamaan tietosuojatoimiensa lainmukaisuus.

Tietosuoja-asetus tuo uusia vaatimuksia rekisterinpitäjän toimintaan, samalla kun vanhoja tietosuojaperiaatteita vahvistetaan. Nk. Osoitusvelvollisuuden periaatteen tulee toimia johto-ajatuksena tietosuojan hallinnan sekä henkilötietojen elinkaaren suunnittelussa ja toteuttamisessa.

Tämä tarkoittaa muun muassa vastuiden selkeää määrittelyä, sisäänrakennetun tietosuojan huomioimista sekä toimien dokumentointia ja todentamista. Rekisterinpitäjän henkilöstön ja tietosuojavastaavan osaamisen tulee olla riittävällä tasolla. Riskilähtöinen toimintatapa edellyttää riskien arviointia ja kontrolliympäristön mitoittamista arvioinnin tulosten perusteella.

KPMG:n panos organisaationne hyödyksi

Uusi tietosuojalainsäädäntö asettaa rekisterinpitäjinä ja tietojenkäsittelijöinä toimiville organisaatioille ison kehityshaasteen. KPMG:n kansainvälistä kokemusta omaavat, sertifioidut tietosuoja-asiantuntijat avustavat organisaatiotanne arvioimaan liiketoimintaympäristön ja oman toiminnan riskit sekä räätälöimään organisaatiollenne mitoitetut työvälineet ja prosessit vaatimustenmukaisuuden saavuttamiseksi. Avustamme organisaatiotanne myös järjestämään tietosuojatyön seurannan ja jatkuvan kehittämisen sekä kouluttamaan henkilöstönne. Yhdistämme juridisen ja teknisen näkökulman tuottaaksemme organisaatiollenne käytännönläheisiä ratkaisuja.

Tietosuojan hallintamallin nykytilan arviointi ja kehittäminen

Tietosuojan hallintamallin ja kontrolliympäristön kehittäminen tietosuoja-asetuksen vaatimusten mukaiseksi on hyvä aloittaa tietosuojatoimien nykytilan arvioinnista ja sen peilaamisesta lainsäädännön, markkinoiden ja tehokkuuden vaatimuksiin. Tehokas tietosuojaohjelma perustuu aina huolellisesti suoritettuun riskianalyysiin ja on suhteutettu toimintaympäristöön sekä käsiteltävien henkilötietojen luonteeseen.

Contact us

Mika Laaksonen
Partner, Cyber Security
P: 020 760 3337
E: mika.laaksonen@kpmg.fi

Kira Ahveninen-Kuha
Tietosuoja-asiantuntija, Legal
P: 020 760 3799
E: kira.ahveninen-kuha@kpmg.fi

KPMG
PL 1037 | Töölönlahdenkatu 3 A
00101 Helsinki

P: 020 760 3000
E: contact@kpmg.fi
E: etunimi.sukunimi@kpmg.fi

www.kpmg.fi

Tutustu tietoturvablogiimme:
www.hackingthroughcomplexity.fi/