GDPR:n fyysiset tietoturva- ja yksityisyyssuojat

Euroopan unionin Yleinen tietosuoja-asetus (GDPR) vaatii organisaatioiden ympäri maailman harkitsevan uudelleen sitä, kuinka ne käsittelevät, käyttävät ja ylläpitävät henkilötietoja. Tässä asiantuntijaraportissa kuvaillaan tietoihin liittyviä riskejä, jotka voivat toteutuessaan uuden asetuksen puitteissa johtaa viranomaistoimiin ja rangaistuksiin. Raportissa käsitellään myös fyysisten suojatoimien parhaita käytäntöjä. Tämä on tärkeä, mutta usein vähälle huomiolle jäävä tietoturvan puoli. Yhdessä hallinnolliset ja fyysiset suojaustoimet sekä kyberturvallisuustoimet auttavat arkaluontoisten henkilötietojen suojauksessa ja osoittavat organisaation sitoutuneen tietosuojan tarjoamiseen.

Tärkeimmät aiheet:

- Mitä GDPR:ssä sanotaan tietoja suojaavista fyysisistä tietoturva- ja tietosuojamenetelmistä.
- Mitä alan asiantuntijat pitävät kohtuullisena tietojen ja yksityisyyden suojaustasona.

Tietokeskeinen maailmamme
Luonnollisena osana nykyajan liiketoimintaa useimmat organisaatiot keräävät ja käyttävät henkilötietoja – henkilöstöstä, asiakkaista, mahdollisista asiakkaista tai kolmansista osapuolista. Tyypillisesti nämä tiedot varastoidaan sähköisesti niin, että organisaatio[1] ja ulkopuoliset toimijat voivat käyttää niitä. Lisäksi joidenkin organisaatioiden päätehtävä on kerätä ja analysoida suuria määriä henkilötietoja.

Eri organisaatioiden keräämien tietojen määrä ja tyyppi vaihtelevat, mutta vallitsee laaja yksimielisyys siitä, että tietojen löytäminen ei ole koskaan ollut helpompaa. Yksilöt jättävät jälkeensä suuren määrän tietoja, kun he luovat sosiaalisen median profiileja, osallistuvat verkon yhteisöihin, hakevat tietoja verkosta, vastaavat kyselyihin sekä hyödyntävät kampanjatarjouksia ja "ilmaisia" palveluita, kuten valokuvien tallennuspalveluita ja musiikin suoratoistoa.

Teknologia myös auttaa luomaan profiileja ihmisistä. Tekoälyn, sähköisten tunnisteiden, jäljitteiden, evästeiden ja muiden seurantatyökalujen kehitys on vienyt tätä eteenpäin.

Teknologian ja tiedonlouhinnan avulla organisaatiot ovat voineet kerätä suuria määriä henkilötietoja. Näistä tietovarannoista voivat käydä ilmi henkilön ikä, aviosääty, syntymäpäivä, koulutus, harrastukset, uskonto, työllisyyshistoria, poliittiset näkemykset, ostotottumukset, luetuimmat uutislähteet, tulot, rikostausta ja monet muut seikat.

Vaikka suuri osa näistä tiedoista on keskitetty yritysten tietokantoihin, osa tiedoista on hajallaan ympäri toimitusketjua eri järjestelmissä, joista usein puuttuu tapa ilmaista tietojen tuleville vastaanottajille niiden keräämisen alkuperäinen menetelmä tai syy. Tämän seurauksena henkilötietoja on saatavilla käyttötarkoituksiin, jotka ovat kaukana niiden alkuperäisestä keräämisen syystä.

Organisaatioissa on lukuisia ihmisiä, joilla on pääsy henkilötietoihin esimerkiksi työntekijän palkan maksamista, markkinatutkimuksen tekemistä, sähköpostimarkkinoinnin käynnistämistä tai asiakkaiden sitoutumisen seuraamista varten. Jokainen näistä tietojen käyttöpisteistä merkitsee mahdollisuutta henkilötietojen väärinkäyttöön tai vääriin käsiin joutumiseen.

Faktoja lyhyesti

Mikä GDPR on?
Yleisen tietosuoja-asetuksen (GDPR) tarkoituksena on suojata Euroopan unionissa (EU) olevien henkilöiden yksityisyys.

Milloin se astuu voimaan?
25. toukokuuta 2018

Keihin se vaikuttaa?
Sijainnista riippumatta kaikkiin yrityksiin, jotka ohjaavat tai käsittelevät Euroopassa olevien rekisteröityjen henkilötietoja.

Mitkä ovat henkilötietoja?
Mitkä tahansa luonnolliseen henkilöön eli rekisteröityyn liittyvät tiedot. Kyseessä voivat olla esimerkiksi nimi, valokuva, sähköpostiosoite, pankkitiedot, julkaisut sosiaalisessa mediassa, lääketieteelliset tiedot tai tietokoneen IP-osoite.

Mikä vaikutus tällä on?
Sakko, joka voi olla 20 miljoonaa euroa tai jopa 4 % vuotuisesta maailmanlaajuisesta liikevaihdosta (sen mukaan, kumpi näistä on suurempi). Tämä on suurin sakko, joka voidaan antaa vakavimmista rikkomuksista.

Mistä saan lisätietoja?

- Asetuksen yleisesittely
- Asetuksen lukeminen
- Fyysiset suojaustoimet

65 %
vastaajista sanoo,
että tietoturvaloukkauksien
seurauksena he menettivät
luottamuksen organisaatioon,
jossa vuoto tapahtui.[5]

Ymmärtääksesi organisaatioiden kohtaamia fyysisiä tietoturvariskejä voit miettiä seuraavia tilanteita:

Työntekijä tarkastelee lentokentällä puhelimellaan arkaluontoisia tietoja eikä huomaa, että joku katselee hänen näyttöään.

- Työntekijä kadottaa kannettavan tietokoneensa, eikä sen tietoja ole salattu.
- Työntekijä poistuu pöytänsä äärestä hakemaan kahvia ja jättää samalla asiakkaiden yhteystietoja näytölle, minkä jälkeen valtuuttamaton henkilö kävelee työpisteen ohi.
- Tyytymätön työntekijä ottaa valokuvia tulostimelle jätetyistä asiakirjoista, näytöllä näkyvistä tiedoista ja tietokoneen näyttöön teipatuista kirjautumistunnuksista.
- Vanhentuneita tietokoneita lahjoitetaan hyväntekeväisyyteen ilman kiintolevyjen asianmukaista tyhjentämistä.
- Lääkärin toimisto lakkautetaan ja potilastietoja heitetään roskakoriin ilman silppuamista.

Vuonna 2016 hakkerit vaaransivat
miljardi tietuetta[2]

Tällaiset skenaariot ovat entistä huolestuttavampia, koska tietoturvaloukkaukset ovat niin yleisiä nykyajan digitaalisessa maailmassa. Forrester raportoi, että vuonna 2016 hakkerit vaaransivat miljardi tietuetta 12 kuukauden aikana. Vuoden 2017 ensimmäisellä puoliskolla raportoitiin, että 918 tietoturvaloukkausta johti 1,9 miljardin tietueen vaarantumiseen koko maailmassa. Tämä merkitsee 164 prosentin nousua verrattuna vuoden 2016 ensimmäiseen puoliskoon.[2]

Jokaisen uuden tietoturvaloukkauksen sattuessa monet pelkäävät, että tietosuoja on kokonaan menetetty. Hiljattain tehdyn tutkimuksen mukaan ihmiset uskovat tietosuojansa olevan vaarassa tietoturva- ja luottamuksellisuusongelmien takia. 91 prosenttia pelkää, että yksilöt ovat menettäneet mahdollisuuden hallita omia henkilötietojaan ja sitä, kuinka yritykset keräävät ja käyttävät näitä tietoja. Lähes sama osuus ihmisistä uskoo, että olisi hyvin hankalaa poistaa virheellisiä itseään koskevia tietoja verkosta.[3] Merkittävien tietovuotojen lisäksi on siis muitakin huolenaiheita. Pienillä yrityksillä ei välttämättä ole yksittäisistä ihmisistä yhtä paljon tietoja kuin suurilla, mutta näille ihmisille tietojen turvallisuus on yhtä tärkeää.

Tällaiset pelot kasvavat entisestään, vaikka tiukkoja tietosuojadirektiivejä ja -asetuksia on ollut jo yli vuosikymmenen ajan. Merkittäviä esimerkkejä ovat Yhdysvaltain terveysalan Health Insurance Portability and Accountability Act -laki (HIPAA), pankkialan Fair Credit Reporting Act -laki ja Euroopan unionin Tietosuojadirektiivi.

Tietosuojadirektiivissä esitetään periaatteita, kuten tietojen turvallinen varastointi ja käsittely rajattua tarkoitusta varten sekä niiden säilyttäminen vain tarvitun ajan. Se on kuitenkin direktiivi eikä laki, joten sen käyttöönotto ja soveltaminen vaihtelevat Euroopassa maittain.

Mukaan astuu GDPR
GDPR on kattavin ja maailmanlaajuisesti merkittävin henkilötietojen suojaamista koskeva asetus. Se luotiin jaetun käsityksen pohjalta, jonka mukaan kaikilla on perustavanlaatuinen oikeus yksityisyyteen. Sen tavoitteena on EU:ssa olevien yksilöiden yksityisyyden suojaaminen uudella asetuksella siitä, kuinka yritykset suojaavat, käsittelevät ja käyttävät henkilötietoja.

GDPR on mahdollisesti tärkein kehitys tietoturvan ja yksityisyyden suojaamisessa 20 vuoteen kirjanpidon vastuullisuusvaatimuksien ja mahdollisten taloudellisten vaikutusten vuoksi. Organisaatioita voidaan rankaista kaksiportaisilla sakoilla. Alemmalla portaalla näiden suuruus on kaksi prosenttia vuosittaisesta maailmanlaajuisesta liikevaihdosta tai 10 miljoonaa euroa muun muassa seuraavista rikkomuksista:

- Tietoturvaloukkauksen jättäminen ilmoittamatta valvovalle viranomaiselle ja yksilöille, joihin vuoto vaikuttaa
- Tietosuojavastaavan (DPO) nimittämättä jättäminen, jos organisaatiolla on oltava sellainen

Organisaatiot voivat saada sakon, jonka suuruus on neljä prosenttia vuosittaisesta maailmanlaajuisesta liikevaihdosta tai 20 miljoonaa euroa, muun muassa seuraavien vaatimusten rikkomuksista:

- Puutteet rekisteröityjen oikeuksien kunnioittamisessa
- Valvovan viranomaisen käskyn jättäminen noudattamatta
- Kansainvälisten tiedonsiirtojen vaatimusten jättäminen noudattamatta[4]

Näiden sakkojen lisäksi vaarana on maineen, brändin arvon ja luottamuksen menetys, mikä voi olla yhtä haitallisia yrityksen tulokselle. Itse asiassa tietoturvaloukkausten seurauksena jopa 65 prosenttia ihmisistä voi menettää luottamuksensa organisaatioon, jossa vuoto tapahtuu.[5]

GDPR on kattavin ja maailmanlaajuisesti merkittävin henkilötietojen suojaamista koskeva asetus.[1]

GDPR:n noudattaminen ei ole pieni työpanos, sillä organisaatiot asetetaan vastuuseen siitä, kuinka ne keräävät, käyttävät, ylläpitävät ja poistavat henkilötietoja ja varmistavat niiden tietoturvan. Vaikka käytössä olisi jo tietosuoja- ja tietoturvaohjelmat, käytännöt täytyy arvioida uudelleen. GDPR vaatii organisaatioita erityisesti ottamaan käyttöön asianmukaiset tekniset ja organisatoriset menetelmät henkilötietojen menetystä ja luvatonta käyttöä vastaan.

Tämä herättää kysymyksiä, kuten:

K. Mitkä ovat henkilötietoja?
V. Kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön.[6] Tähän voi kuulua tunnisteita (kuten nimi tai tunnusnumero) tai tietoja, jotka paljastavat etnisen alkuperän, poliittiset mielipiteet, uskonnon tai filosofiset uskomukset, ammattiyhdistysten jäsenyyden, geneettiset tiedot, terveystiedot, rikostaustan, työssä suoriutumista koskevat ennusteet, taloudellisen tilanteen, henkilökohtaiset mieltymykset tai kiinnostuksen kohteet, luotettavuuden tai käytöksen, sijainnin tai liikkeet jne.[7]

K. Mitä on pseudonymisointi ja miksi minun tulisi välittää siitä?
V. GDPR:ssä 15 kertaa mainittu termi "pseudonymisointi" tarkoittaa menetelmää, jossa tietueen sisältämät tunnistavat kentät korvataan yhdellä tai usealla keinotekoisella tunnisteella eli pseudonyymillä. GDPR suosittelee pseudonymisoinnin käyttöönottoa henkilötietojen kanssa, jotta rekisteröityjen riskejä voidaan vähentää ja auttaa rekisterinpitäjiä ja tietojen käsittelijöitä täyttämään tietosuojavastuunsa.[8]

K. Voivatko organisaatiot saada yksilöiltä suostumuksen henkilötietojen keräämiseen?
V. Kyllä, mutta suostumus täytyy antaa selkeästi suostumusta ilmaisevalla toimella, jossa rekisteröity antaa vapaaehtoisen, yksilöidyn, tietoisen ja yksiselitteisen tahdonilmaisun, jolla hän suostuu henkilötietojen käsittelyyn. Valmiiksi rastitetut ruudut, vaikeneminen tai toimen jättäminen tekemättä eivät täytä suostumuksen kriteerejä.[9] Organisaatioiden täytyy pitää kirjaa suostumusten saannista ja varmistaa, että suostumuspyynnöt ovat erotettavissa muista pyynnöistä ja että niiden kieli on selkeää ja yksinkertaista.[10] 13 artikla sisältää paljon tietoja, jotka täytyy antaa rekisteröidylle henkilötietojen keräämisen yhteydessä, kuten tietojen keräämisen tarkoitus, henkilötietojen vastaanottajat tai vastaanottajakategoriat ja tietojen säilytyksen kesto.

K. Mikä on Tietosuojaa koskeva vaikutustenarviointi (DPIA)?
V. Korkean riskin toimintoja varten vaadittava DPIA auttaa organisaatioita arvioimaan riskien alkuperää, olemusta, erikoispiirteitä ja vakavuutta sekä ottamaan käyttöön asianmukaisia toimenpiteitä riskien alentamiseen, kuten tietojen salaus. Tietosuojariskiä arvioitaessa on syytä ottaa huomioon henkilötietojen käsittelyssä muodostuvat riskit, kuten siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingollinen tai laiton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai tietoihin pääsy, joiden seurauksena voi olla fyysisiä, aineellisia tai aineettomia vahinkoja.[11]

K. Täytyykö minun nimittää tietosuojavastaava (DPO)?
V. Tietosuojavastaavan nimittäminen on pakollista aina, kun tietojenkäsittelyn suorittaa viranomainen (paitsi virkaansa toimittavat oikeusistuimet) tai yritys, jonka ydintoimintoihin kuuluu tietojen käsittely, joka vaatii rekisteröityjen säännöllistä ja systemaattista seurantaa suuressa mittakaavassa. Tietosuojavastaava on myös pakollinen kaikille yrityksille, jotka käsittelevät suuressa mittakaavassa arkaluontoisia tietoja, kuten terveyteen, uskontoon tai poliittisiin näkemyksiin liittyviä tietoja. Tarkemmin:

- Tietosuojavastaavan nimittämisessä täytyy ottaa huomioon ammattipätevyys sekä erityisesti asiantuntemus tietosuojalainsäädännöstä ja alan käytänteistä.
- Tietosuojavastaava voi olla henkilöstön jäsen tai ulkopuolinen palveluntarjoaja.
- Yhteystiedot täytyy toimittaa asianmukaiselle DPA:lle.
- Tietosuojavastaavalle täytyy antaa asianmukaiset resurssit tehtävien suorittamiseen ja asiantuntemuksen ylläpitämiseen.
- Tietosuojavastaava on raportointivastuussa ylimmälle johdolle
- Tietosuojavastaava ei saa suorittaa sellaisia muita tehtäviä, jotka voisivat aiheuttaa eturistiriidan.[12]

Fyysiset tietoturva- ja tietosuojavaatimukset
Mitä organisaatioiden tulee tehdä tietoturvaloukkausten estämiseksi? GDPR:n artiklassa 24 kerrotaan organisaation vastuut "tarvittavien teknisten ja organisatoristen toimenpiteiden" suorittamiseksi, jotta henkilötietojen käsittely on asianmukaista. Artiklassa 32 mennään pidemmälle ja siinä sanotaan: "Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä huomiota erityisesti käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi."

Tässä asetuksessa korostuu luvattoman tietoihin pääsyn estäminen. Fyysiset turvatoimet ovat tässä avainasemassa. Ne voivat erityisesti auttaa tietojen suojaamisessa sellaisia sisäisiä ja ulkoisia ihmisten aiheuttamia uhkia vastaan, jotka pyrkivät hyödyntämään organisaation seinämien ja henkilöstön tietoturvan aukkoja. Tähän kuuluu sen rajoittaminen, mitä tietoja voidaan tarkastella, varastaa tai käyttää. Tarkista seuraavat kohdat ja arvioi, onko työvoimallasi käytössä asianmukaiset tekniset ja organisatoriset toimet määräyksen noudattamiseen.

Ota käyttöön sisäänrakennettu ja oletusarvoinen tietosuoja:
Oletusarvoista tietosuojaa varten organisaatioiden täytyy ennakoivalla tavalla tunnistaa ja kerätä vain käyttötarkoituksen mukaiset henkilötiedot, säilyttää tietoja vain niin kauan kuin on tarpeen (minimoinnin periaate) ja varmistaa, että tuntemattomalla määrällä henkilöitä ei ole pääsyä henkilötietoihin. Tätä varten tietosuojariskit on tunnistettava etukäteen ja järjestelmät on suunniteltava vähentämään näitä riskejä. Tarvittaessa on käytettävä pseudonymisointia ja anonymisointia, luotava käsittelyyn läpinäkyvyyttä ja tunnistettava tietyt henkilöt tai roolit, jotka tarvitsevat tietoja. Kysy itseltäsi: Otatko huomioon yksilöiden tietosuojariskit, ennen kuin suunnittelet tietojärjestelmiä, liiketoimintaa ja fyysisiä tekijöitä? Oletko IT-henkilöstösi kanssa arvioinut nykyisiä järjestelmiä ja käsittelytoimenpiteitä sekä keskustellut mahdollisesti tarvittavista lisätoimenpiteistä henkilötietojen suojaamisen dokumentoinnissa koko tietojen elinkaaren aikana?

Fyysisten suojaustoimien käyttö:
Kyberturvallisuustoimet, kuten tietojen salaus ja monimutkaiset salasanat, ovat tärkeitä, mutta teknisesti yksinkertaiset hallinnolliset ja fyysiset toimet ovat yhtä tärkeitä. Arvioi fyysisten toimenpiteiden käyttökohteita sen perusteella, missä arkaluontoisia tietoja käsitellään. Työntekijät käyttävät esimerkiksi usein mobiililaitteita tietojen käsittelyyn ja jakamiseen missä tahansa. Kasvava osuus näistä työntekijöistä käyttää arkaluontoisia tietoja julkisilla paikoilla, usein muiden ihmisten nähden. Myös toimiston sisällä on entistä suurempi tietojen paljastumisen riski. Yleisistä avotoimistoista puuttuvat fyysiset näköesteet, jotka ennen suojasivat tietokoneiden näyttöjä. Kysy itseltäsi: Oletko sijoittanut tietokoneiden näytöt kauemmas ikkunoista, ovista ja yleisölle avoimista alueista? Onko näytöissä ja mobiililaitteissa käytössä tietoturvasuojat, jotka estävät mahdollisia ulkopuolisia näkemästä tietoja? Ovatko jaetut tulostimet/kopiokoneet/faksit suojatuilla alueilla tai onko niissä lukittavat kannet? Säilytätkö tietojen fyysisiä kopioita kulkuvalvotussa toimipisteessä? Ovatko silppurit vakiovaruste kaikkien toimipisteiden yksiköiden, erityisesti kopiokoneiden, tulostimien ja faksien kanssa ja ovatko ne vaatimus kaikille etätyöntekijöille ja niille, jotka käyttävät yrityksen tietoja etäyhteyden kautta?

Työntekijöiden koulutuksen aikataulutus:
Koulutuksessa tulee käsitellä kolme tärkeää aihetta: Tarkkailun, fyysisen pääsyn ja varkauksien estämisen parhaat käytännöt Työntekijöitä tulee esimerkiksi muistuttaa olemaan tietoisia ympäristöstään, kun he käyttävät tai hallitsevat liitettyjä laitteita julkisilla paikoilla kannettavalla, tabletilla tai älypuhelimella. Laitteiden näytöt eivät saa olla ohikulkijoiden ja mahdollisten sivustakatsojien nähtävissä, varsinkaan kirjautumistietoja syötettäessä tai arkaluontoisia tilitietoja katseltaessa. Fyysiseen pääsyyn liittyen organisaatioiden tulee kouluttaa työntekijät pyyhkimään tiedot valkotauluilta ja keräämään luottamukselliset paperit kokousten jälkeen, opettelemaan salasanat ulkoa ylös kirjoittamisen sijaan, lukitsemaan arkistokaapit ja kannettavat, käyttämään tietojenkäsittelylaitteiden näyttöjen tietoturvasuojia ja noudattamaan puhtaan pöydän käytäntöä, mukaan lukien kirjautuminen ulos valvomattomilta laitteilta. Kysy itseltäsi: Kattaako koulutusohjelma tilannetajun, jonka avulla työntekijät voivat tiedostaa ympäristönsä sekä tunnistaa epäilyttävän käytöksen ja vastata siihen? Ymmärtävätkö työntekijät organisaation "puhtaan pöydän" käytäntöä koskevat odotukset? Muistutatko työntekijöitä usein hyvistä tietoturvakäytännöistä, joita tulee seurata?

Selkeiden käytäntöjen kehittäminen:
Jotta organisaation sitoutuminen asianmukaisiin tietoturva- ja tietosuojatoimiin voidaan osoittaa, käytännöissä tulee mainita tietojen katselun ja käytön suositellut ja kielletyt toimet työntekijöille ja alihankkijoille, olivatpa nämä toimistossa tai etätöissä. Työntekijöiden sopimuksissa tulee ilmaista selkeästi vastuu arkaluontoisten ja luottamuksellisten tietojen suojaamisesta.[13] Kysy itseltäsi: Oletko kertonut yksilöille tietosuoja- ja tietoturvalausunnosta, jossa selitetään, kuinka organisaatiosi suojaa, jakaa ja hävittää henkilötietoja sekä mahdollistaa pääsyn niihin? Onko sinulla oman laitteen tuomista koskeva käytäntö, joka säätelee työntekijöiden toimintaa ja vaadittuja suojaustoimia, kun he käyttävät yrityksen resursseja henkilökohtaisella laitteella? Vaaditko osana tietoturvakäytäntöjä, että työntekijät käyttävät suojautumiseen sekä visuaalisia että kyberturvallisuuden keinoja?

Tietojen säilytyksen rajojen asettaminen:
Aseta aikarajat henkilötietojen säilyttämiselle soveltuvan lainsäädännön mukaisesti. Poista turvallisesti kaikki henkilötiedot, jotka eivät ole välttämättömiä niiden liiketoimien tukemisessa, joita varten ne on kerätty. Kysy itseltäsi: Mitä teknisiä toimia on käytettävissä tietojen poistamiseksi oikeaan aikaan? Ovatko organisaatiosi tietojen tuhoamisen menetelmät vahvojen tietoturvaohjeiden, kuten NIST:n julkaisun Special Publication 800-88, mukaisia? Kuuluuko niihin esimerkiksi käyttöikänsä päähän tulleiden kiintolevyjen tuhoaminen?

Kolmansien osapuolten tarkistaminen:
Käytä vain tietojenkäsittelijöitä, jotka takaavat riittävän asiantuntemuksen, luotettavuuden ja resurssit teknisten ja organisatoristen toimenpiteiden suorittamiseen, myös tietojenkäsittelyn turvallisuuteen. Kysy itseltäsi: Onko käytössä toimittajien hallintaohjelma, joka sisältää sopimusvelvoitteet ja esittelee johdon valvontatoimet kolmansille osapuolille, joilla on pääsy henkilötietoihin?

Tietoturvaloukkausprotokollan luominen:
Organisaatioiden täytyy olla valmiita ilmoittamaan valvovalle viranomaiselle ilman aiheetonta viivytystä, kun järjestö saa tietoonsa, että on tapahtunut henkilötietojen tietoturvaloukkaus (kun mahdollista, 72 tunnin kuluessa). Tai on kyettävä näyttämään, että henkilötietojen tietoturvaloukkaus ei todennäköisesti aiheuta riskiä luonnollisten henkilöiden oikeuksille ja vapauksille. Jos riski on korkea, rekisteröidy(i)lle on myös ilmoitettava tietoturvaloukkauksesta ilman aiheetonta viivästystä.[14] Kysy itseltäsi: Milloin viimeksi arvioit organisaatiosi ongelmatilanteissa toimimisen ja tietoturvaloukkauksesta ilmoittamisen käytännöt ja suunnitelmat? Tietävätkö työntekijät, kenelle organisaation sisällä ilmoitetaan, jos oma laite on vaarantunut tai jos työntekijä on tietoinen tietoturvaloukkauksesta? Onko käytössä ajan tasalla oleva ongelmatilanteissa toimimisen ja vuodoista ilmoittamisen suunnitelma, jossa määritetään, milloin ja kuinka viranomaisille ilmoitetaan tietoturvaloukkauksesta?

Yksilöiden oikeuksien tunteminen:
EU:n asukkailla on nyt oikeus nähdä, mitä heitä koskevia henkilötietoja organisaatioilla on hallussaan, ja pyytää tietyissä tilanteissa tietojensa poistamista. Poistamispyyntöoikeus vaatii organisaatioita poistamaan kyseisiin henkilötietoihin johtavat linkit tai näiden henkilötietojen jäljennökset ja kopiot. Organisaatioiden tulee antaa ihmisille mahdollisuus lähettää pyyntö sähköisesti varsinkin, jos henkilötietoja käsitellään sähköisesti.[15] Kysy itseltäsi: Ymmärretäänkö organisaatiosi, mitkä ovat "henkilötietoja" ja kuinka henkilötietoja koskeviin kyselyihin vastataan?

Johtopäätös:

GDPR on tärkein tietosuoja-asetusten muutos 20 vuoteen. Siinä vaaditaan, että henkilötietoja käsitellään tavalla, jolla varmistetaan asianmukainen tietoturva ja luottamuksellisuus. Tämä vaatii sekä teknisiä että organisatorisia suojatoimenpiteitä. Noudattamatta jättämisestä annettavat sakot voivat olla lamauttavia. Asetuksessa eritellyt parhaat käytännöt ovat kuitenkin yrityksille yksinkertaisesti hyvä tapa toimia. Kukaan ei halua tietojensa väärinkäyttöä, eikä mikään organisaatio halua joutua tietoturvaloukkauksen seuraamusten kohteeksi. Organisaatiot, jotka eivät näe tietosuojaa vain lainsäädännöllisenä rasitteena vaan yrityksensä vastuualueena, voivat käyttää tätä strategisena etuna maineen ja brändin arvon kasvattamiseksi, parempien työntekijöiden houkuttelemiseksi ja yleisen luottamuksen säilyttämiseksi.

3msuomi.fi/3M/fi_FI/privacy-protection-ndc/visual-privacy-issues/data-security-study/

[1]Forrester, "Lessons Learned from the World's Biggest Security Breaches and Data Abuses", 9. tammikuuta 2017
[2]Gemalton vuoden 2017 tietovuotojen tason indeksi, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK:n tietosuojapaneeli, "Public Perceptions of Privacy and Security in the Post-Snowden Era", 2014.
[4]GDPR:n 83 artikla, 2017
[5]Ponemon Institute, "The Impact of Data Breaches on Reputation & Shared Value", Centrifyn sponsoroima, 2017.
[6]GDPR:n 4 artikla, 2017
[7]GDPR:n johdanto-osa 75, 2017
[8]GDPR:n johdanto-osat 26 ja 28, 2017
[9]GDPR:n johdanto-osa 32, 2017
[10]GDPR:n 7 artikla, 2017
[11]GDPR:n 35 artikla ja johdanto-osat 83-84, 2017
[12]GDPR:n 37–38 artiklat, 2017
[13]GDPR:n johdanto-osat 74 ja 77–78, 2017
[14]GDPR:n johdanto-osa 81, 2017
[15]GDPR:n johdanto-osat 59, 63, 65 ja 66, 2017