IPRA TECHNOLOGIES LTD

EU:n tietosuoja-asetus ja sähköposti

EU:n uusi yleinen tietosuoja-asetus (GDPR) määrittelee, miten EU-kansalaisten henkilötietojen käsittely tulee järjestää EU:n alueella. Asetus astuu voimaan 25.5.2018 ja korvaa olemassa olevat kansalliset tietosuojalait. GDPR koskee kaikkia EU:n sisällä ja ulkopuolella toimivia organisaatiota, jotka hallinnoivat ja käsittelevät EU-kansalaisten henkilötietoja. Toisin kuin yksityisyyden suojaa koskevat lait muualla maailmassa, uusi tietosuojalainsäädäntö ei ole alakohtainen. Tämä tarkoittaa sitä, että samat säädökset koskevat niin pienyrityksiä kuin suuria monikansallisia yrityksiä toimialasta riippumatta muutamia harvoja poikkeuksia lukuun ottamatta. Tästä syystä EU:n uusi tietosuoja-asetus vaikuttaa kaikkiin organisaatioihin.

EU:n tietosuoja-asetukseen voi tutustua kokonaisuudessaan täällä: http://eur-lex.europa.eu/eli/reg/2016/679/oj.

Mikä GDPR on? Yhteenveto

- Määrää, milloin ja miten organisaatiot voivat kerätä henkilötietoja.
- Määrää, miten henkilötietoja voidaan käyttää ja käsitellä.
- Asettaa organisatoriset ja tekniset säännöt henkilötietojen turvalliselle käsittelylle.
- Velvoittaa organisaatiot ilmoittamaan tietoturvaloukkauksista henkilöille (rekisteröidyille), joita loukkaus koskee, sekä viranomaisille.
- Vaikuttaa kaikkiin organisaatioihin, jotka “hallinnoivat” tai “käsittelevät” henkilötietoja.
- Kun GDPR astuu voimaan, EU:n tietosuojalainsäädännön rikkomisen seuraukset kiristyvät merkittävästi. Asetuksen perusteella suurin mahdollinen sakko yksittäisestä tietosuojarikkomuksesta on 20 miljoonaa euroa tai neljä prosenttia vuotuisesta liikevaihdosta (riippuen siitä, kumpi summista on suurempi).
- Asetus muuttaa merkittävästi sekä tietosuojatarpeita että noudattamatta jättämisestä aiheutuvia seurauksia Suomessa.

IPRA Technologies Ltd., Valtakatu 51, Vapaudenaukio Technopolis 2, 53100 Lappeenranta, Finland.

Henkilötiedot

EU:n tietosuoja-asetuksen **Artiklan 4** (1) mukaan henkilötiedoilla tarkoitetaan “kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”.

Tämä laaja määritelmä kattaa kaikki sellaiset tiedot, joista yksittäinen henkilö voidaan tunnistaa. Tällaisia tietoja ovat esimerkiksi suoraan tai epäsuorasti työntekijöihin, asiakkaisiin, oppilaisiin jne. liittyvät rekisterit.

Rekisterinpitäjä

EU:n tietosuoja-asetuksen **Artiklan 4** (7) mukaan rekisterinpitäjällä tarkoitetaan “luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti”. Tämä voi tarkoittaa mitä tahansa organisaatiota, joka kerää ja käsittelee tietoja joko itse tai ulkoistetun palvelun kautta.

Henkilötietojen käsittelijä

EU:n tietosuoja-asetuksen **Artiklan 4** (8) mukaan henkilötietojen käsittelijällä tarkoitetaan “luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun”. Jokainen organisaatio, joka on tekemisissä henkilötietojen kanssa, on henkilötietojen käsittelijä.

EU:n tietosuoja-asetuksen **Artiklan 4** (2) mukaan käsittelyllä tarkoitetaan “toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista”.

Lyhyesti sanottuna kaikki, mitä tehdään henkilötiedoille tai henkilötiedoilla (mukaan lukien kerääminen, varastointi ja siirtäminen), katsotaan käsittelyksi.

Henkilötietojen tietoturvaloukkaus

EU:n tietosuoja-asetuksen **Artiklan 4** (12) mukaan henkilötietojen tietoturvaloukkauksella tarkoitetaan "tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin".

Käsittelyn turvallisuus

Artikla 32(1): Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit **rekisterinpitäjän** ja **henkilötietojen käsittelijän** on toteutettava riskiä vastaavan **turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet**, kuten:

1. henkilötietojen pseudonymisointi ja **salaus**;
2. kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;
3. kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;
4. menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

(2): 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.**

(3): Jäljempänä 40 artiklassa tarkoitettujen hyväksyttyjen käytännesääntöjen tai 42 artiklassa tarkoitetun hyväksytyn sertifiointimekanismin noudattamista voidaan käyttää yhtenä tekijänä sen osoittamiseksi, että tämän artiklan 1 kohdassa asetettuja vaatimuksia noudatetaan.

(4): Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.

Johdanto-osan 83 kappale: Turvallisuuden ylläpitämiseksi ja asetuksen säännösten vastaisen käsittelyn estämiseksi rekisterinpitäjän tai henkilötietojen käsittelijän olisi arvioitava käsittelyyn liittyvät riskit ja toteutettava toimenpiteitä näiden riskien lieventämiseksi esimerkiksi **salauksella**. Näiden toimenpiteiden avulla olisi varmistettava asianmukainen turvallisuustaso, muun muassa luottamuksellisuus, ottaen huomioon uusin tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Tietosuojariskiä arvioitaessa olisi otettava huomioon henkilötietojen käsittelyyn liittyvät riskit, kuten **siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai laiton tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai henkilötietoihin pääsy**, mikä voi aiheuttaa etenkin fyysisiä, aineellisia tai aineettomia vahinkoja.

Johdanto-osan 78 kappaleessa: Luonnollisten henkilöiden **oikeuksien ja vapauksien suoja** henkilötietojen käsittelyssä **edellyttää**, että toteutetaan **asianmukaiset tekniset** ja **organisatoriset toimenpiteet**, joilla varmistetaan, että asetuksessa säädetyt vaatimukset täyttyvät. Jotta voidaan osoittaa, että asetusta on noudatettu, rekisterinpitäjän **olisi hyväksyttävä sisäisiä menettelyjä ja toteutettava toimenpiteet**, jotka vastaavat erityisesti **sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita**.

Huomioita GDPR:stä

EU:n uusi tietoturva-asetus tekee salauksesta pakollista. Tiedot tulee salata aina, kun se on mahdollista. Tämä tarkoittaa myös tilanteita, jolloin tietoja **tallennetaan** tai **niitä siirretään**. Salausvelvoite koskee yhtälailla myös julkisia pilvipalveluita, joissa tulisi mieluiten olla käytössä käyttäjien hallitsemat salausavaimet pilvipalvelun tarjoamien avainten lisäksi.

Jos henkilötiedot salataan koko niiden elinkaaren ajan vahvoilla ja hyväksytyillä algoritmeilla, ne eivät kuulu GDPR:n soveltamisalaan. Artikla 32(1) toteaa salauksen olevan asianmukainen suojausmenetelmä. Salauksessa tulee tällöin huomioida kaikki päätepisteet. **Henkilötiedot ovat aina henkilötietoja riippumatta siitä, missä niitä säilytetään.** Jos esimerkiksi henkilötietoja sisältävä mobiililaite murretaan matkustamisen aikana, tämä vertautuu EU:n tietosuoja-asetuksen mukaan tietokantaan kohdistuneeseen tietoturvaloukkaukseen.

Vaikuttaako GDPR organisaatiosi sähköpostikäytäntöihin?

Käytetäänkö organisaatiossasi sähköpostia EU:n alueella olevien asiakkaittenne, työntekijöittenne, harjoittelijoidenne tai johtohenkilöidenne henkilötietoja sisältävien viestien ja tiedostojen lähettämiseen? Nämä henkilötiedot voivat olla esimerkiksi nimiä, osoitteita, sähköpostiosoitteita, puhelinnumeroita, tieto sukupuolesta tai kansallisuudesta, henkilötunnuksia, tilinumeroita, verkkotunnisteita (esim. IP-osoitteita) tai sellaisia tunnusomaisia fyysisiä, fysiologisia, psyykkisiä, taloudellisia, kulttuurillisia tai sosiaalisia tekijöitä, joista voidaan tunnistaa yksittäisiä EU-kansalaisia. Lyhyesti sanottuna henkilötiedot ovat mitä tahansa tietoja, joista voidaan tunnistaa yksittäinen henkilö.

Jos lähettämäsi sähköpostit tai liitetiedostot sisältävät tällaisia tietoja, niihin sovelletaan EU:n tietosuoja-asetusta. Henkilötietojen välittäminen ja säilyttäminen katsotaan käsittelyksi.

EEZY KEYZ® ja GDPR

Välttääkseen GDPR:n säännösten rikkomisen, henkilötietoja valvovien ja käsittelevien organisaatioiden tulee ryhtyä erilaisiin toimenpiteisiin, esimerkiksi ottaa käyttöön tietojen **salaus,** välttääkseen henkilötietojen käsittelyyn liittyviä riskejä, kuten siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

EEZY KEYZ® suojaa sähköpostit ja liitetiedostot end-to-end-teknologiaan perustuvalla salauksella niin PC-tietokoneilla kuin Android- ja iOS-järjestelmissä. Salatut sähköpostit ja liitetiedostot pysyvät salattuina sekä laitteilla että pilvessä (sähköpostipalvelimellasi). Tämä estää mm. henkilötietoja sisältävien sähköpostien ja liitetiedostojen luvattoman luovuttamisen sekä luvattoman pääsyn henkilötietoihin siirron ja säilytyksen aikana.

EU:n tietosuoja-asetus on monimutkainen kokonaisuus, mutta EEZY KEYZ® -sovellusta käyttävät organisaatiot voivat olla varmoja siitä, että heidän lähettämänsä sähköpostit ovat asetuksen määräysten mukaisia. Sovellus on kehitetty noudattaen sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita, joita myös GDPR korostaa. Kun EEZY KEYZ® on otettu käyttöön organisaatiossa, kaikki organisatoriset sähköpostit on oletusarvoisesti salattu end-to-end-teknologialla.

IPRA TECHNOLOGIES LTD

Monialustainen sovelluksemme on saatavilla PC-tietokoneille sekä iOS- ja Android-alustoille. Se mahdollistaa henkilötietoja sisältävien sähköpostien turvallisen ja EU:n tietosuoja-asetuksen mukaisen lähettämisen ja tarkastelun älypuhelimilla ja tableteilla. EEZY KEYZ® on helppo ja edullinen ratkaisu sähköpostipalvelun turvallisuuden ja EU:n tietosuoja-asetuksenmukaisuuden varmistamiseen. Sovelluksen avulla organisaatiosi pystyy välttämään merkittävät sakkorangaistukset, joita voi seurata sähköpostitse välitettyjen henkilötietojen tietoturvaloukkauksista.

Ota meihin yhteys välttääksesi tietosuojarikkomuksesta seuraavat sakot ja varmistaaksesi ettei yrityksenne sähköposti joudu tietomurron kohteeksi:

EEZY KEYZ®

https://eezykeyz.eu

sales@eezykeyz.eu