Tietoturvaraportti

GDPR-asetuksen noudattaminen

Johdatus tietoturvaan

SHARP
Be Original.

www.sharp.fi

Sisältö

Johdanto

Kaikki nykyaikaiset yritykset kohtaavat haasteita erityisesti henkilötietojen suojaamisen osalta pyrkiessään noudattamaan EU:n tietosuoja-asetusta (GDPR).

Yleinen tietosuoja-asetus (GDPR) on tuonut mukanaan monia haasteita yrityksille niin Euroopassa kuin muualla maailmassa.

Vaikka GDPR kohdistuukin valtaosaltaan verkossa olevien tietojen suojaamiseen, asetus vaikuttaa myös siihen, miten yritykset käsittelevät ja varastoivat tietoja. Siksi yritysten on pohdittava, mitä oikein tapahtuu tiedoille, jotka yritys saa (skannauksen kautta tai sähköisesti) haltuunsa ja jotka se varastoi ja säilyttää, käsittelee, jakaa, tulostaa, kopioi, faksaa ja arkistoi.

Asetuksessa käsiteltäviä osa-alueita ovat muun muassa tunnistettavat henkilötiedot, tietosuoja, tietojen poistaminen, tietojen käsittelijät, rekisterinpitäjät, tietosuojavastaavat, vaatimustenmukaisuus sekä tietosuojaviranomaiset (katso GDPR-sanasto sivulla 9).

GRPR:ää käsitteleviä julkaisuja on runsaasti saatavilla. Niissä käsitellään muun muassa tietosuoja-asetuksen tulkintaa sekä kuvataan, keihin tietosuoja-asetus vaikuttaa ja miten asetusta tulee soveltaa yrityksissä. Saatavilla on kuitenkin vain vähän tekstejä, artikkeleita tai raportteja, jotka käsittelevät GDPR:n kääntämistä aidolle yrityskielelle sekä kaikkia liiketoimintaan ja erityisesti henkilötietoihin liittyviä prosesseja.

Liittämällä toisiinsa yrityksen käyttäjät (työntekijät), yrityksen prosessit (työnkulut ja parhaat käytännöt) sekä yrityksen liikeomaisuuden (laitteet ja ohjelmistot), Sharp on määritellyt kolme yrityksen tietoturvan erillistä osa-aluetta, jotka yhdessä voivat parantaa yrityksen kokonaistietoturvaa GDPR:n vaatimusten mukaisesti.

Nämä kolme aluetta ovat

- **Verkon turvallisuus**
  Verkon turvallisuus liittyy kaikkiin yritysorganisaation käyttämiin ja IT-osaston ylläpitämiin verkkoihin, joissa pääpaino on verkkoon yhteydessä olevilla tulostus-, skannaus- ja faksilaitteilla.

- **Tulostuksen tietoturva**
  Tulostuksen tietoturva liittyy monitoimilaitteilla ja tulostimilla tulostettuihin ja skannattuihin tuotoksiin. Siihen sisältyvät paperille tulostetut asiakirjat sekä asiakirjojen kuvat, joita siirretään tietokoneesta tulostuslaitteeseen (myös erillispalvelimen kautta), skannataan (mukaan lukien skannaus kansioon, sähköpostiin ja pilveen) ja faksataan.

- **Asiakirjojen tietoturva**
  Asiakirjojen tietoturva liittyy paperiasiakirjoista skannaamalla saatuihin tietoihin sekä asiakirjojen sähköisessä muodossa oleviin kuviin, joita säilytetään yrityksen omissa säilytyspaikoissa (esim. sähköpostit, tiedostot, kaavakkeet jne.).

Sharp voi auttaa yrityksiä täyttämään GDPR:n vaatimukset tarjoamalla työvälineet ja parhaat käytännöt verkon, tulosteiden ja asiakirjojen tietoturvaan välittömästi liittyviin liiketoimintaprosesseihin.

Taustaa

GDPR on suurin tietosuojan toteuttamisessa tapahtunut muutos yli 20 vuoteen. Kysymyksiä on kuitenkin edelleen paljon – eikä vastauksia ole tarpeeksi.

GDPR asettaa uusia vaatimuksia ja määrittää taloudellisia seuraamuksia suojauksen ja tietoturvaloukkausten ehkäisyn laiminlyönneille[1]. Kuitenkaan ei ole saatavilla tarpeeksi ohjeistusta siitä, mitä yrittäjien, IT-vastaavien ja käyttäjien on tehtävä täyttääkseen vaatimukset. Jokainen yritys joutuu itse päättelemään, miten sen pitää toimia.

GDPR:n tärkein tavoite on tunnistettavien henkilötietojen parempi hallinta ja suojaaminen. Tämä tarkoittaa sitä, että kaikki yrityksen järjestelmissä olevat henkilötiedot on suojattava ja käsiteltävä asianmukaisesti. Tämä koskee esimerkiksi liiketoimintasovelluksiin tallennettuja asiakkaiden ja liikekumppanien yhteystietoja, verkkoasetuksia, asiakirjahallintaa, tulostuksen hallintaa sekä henkilöstöhallinnon työntekijöistä säilyttämiä tietoja.

GDPR:n vaatimustenmukaisuus voidaan jakaa kahteen tasoon:

- **Henkilötaso**
  Kaikki käyttäjään liittyvät asiat, mukaan lukien heidän toiminta- ja työskentelytapansa sekä suhteensa yrityksen järjestelmiin ja sääntöihin

- **Organisaatiotaso**
  Organisaation liiketoimintaprosessit (mukaan lukien paperiset ja sähköiset työnkulut), omaisuus (mukaan lukien omaisuus, jonka avulla ihmiset jakavat tietoja ja kommunikoivat sähköisesti tai paperilla), kulttuuri sekä sen tapa reagoida markkinoiden haasteisiin.

Ottamalla organisaatiotasolla käyttöön strategioita ja työvälineitä voidaan ohjata ja hallita loppukäyttäjien käyttäytymisen odotettua muutosta, heidän työskentelytapaansa sekä tapaansa käsitellä saatavilla olevia liiketoimintatietoja. Näin saavutetaan parempi käsitys siitä, miten sekä asiakirjoja että käyttäjien tunnistettavissa olevia tietoja pitää käsitellä[2].

Siksi Sharp keskittyy organisaatiotasoon (prosessit, ratkaisut ja laitteisto) ja voi auttaa rakentamaan kokonaisvaltaiset tietoturvapolitiikat, jotka ovat kriittisen tärkeitä jokaiselle yritykselle.

Keskittymällä kolmeen yrityksen tietoturvan alueeseen Sharp on määritellyt mahdolliset riskit, joiden huomiotta jättäminen saattaa johtaa puutteisiin vaatimustenmukaisuudessa.

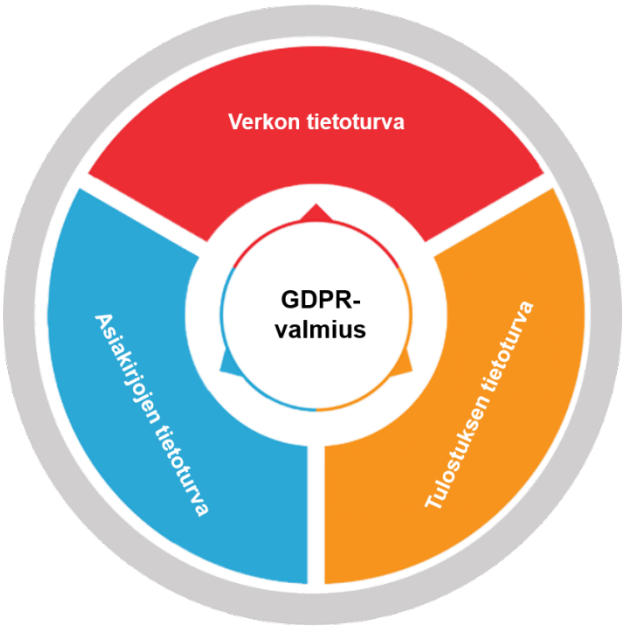
- **Verkkoon liittyvät riskit**
  - Haavoittuvuudet tiedon siirtämisessä paperin ja sähköisten formaattien välillä sekä päinvastaiseen suuntaan.
  - Tarve saada monitoimilaitteiden ja tulostimien tietoturva samalle tasolle palvelimien kanssa sekä tarve ottaa käyttöön suunnitelmallinen ja yhtenäinen tulostuksen tietoturvapolitiikka.
  - Tarve seurata ja hallita laitteita tietoturvapolitiikan pitämiseksi ajan tasalla tarvittavin päivityksin, kun ajan mittaan ilmaantuu uusia haavoittuvuuksia.
  - Tarve hävittää tietoja turvallisesti ja oikea-aikaisesti.

- **Tulosteisiin liittyvät riskit**
  - Tarve suojata monitoimilaitteiden ja tulostinten käyttöä, valvoa tulosteita sekä reitittää luottamukselliset tiedot.
  - Tulosteiden lukumäärän ja tulostetyyppien (kopioidut, printatut, faksatut, skannatut asiakirjat, mukaan lukien skannaus sähköpostiin ja kansioon) hallinta.
  - Tarve jäljittää ja varmentaa tietojen hankkiminen tai tulostaminen.

- **Asiakirjoihin liittyvät riskit**
  - Asiakirjojen elinkaaren määrittelyn ja ymmärtämisen puute yrityksessä. Tähän sisältyvät kaikki asiakirjan elinkaaren vaiheet luomisesta hävittämiseen.

- Rakenteettomat asiakirjojen säilytyspaikat jättävät asiakirjahallintajärjestelmän auki hyökkäyksille ja mahdollisille tietomurroille.
- Toistuvat (sähköisiin ja paperisiin) asiakirjoihin liittyvät manuaaliset tehtävät, jolloin asiakirja saattaa vahingossa joutua väärään paikkaan ja tietoturvaloukkauksen kohteeksi.
- Valvomaton liiketoimintakriittisten asiakirjojen jakaminen
- Tietojen korruptoitumisen riski versiohallinnan puuttumisen takia.

Sharpin tietoturvan runko



Suositukset

Sharp soveltaa yritysten tietoturvaan kokonaisvaltaista lähestymistapaa. Sen avulla voidaan varmistaa tiukimpienkin vaatimusten noudattaminen sekä luoda yritysten toimintaa tehostavia ratkaisuja.

Sharpin tavoitteena on varmistaa GDPR:n vaatimusten noudattaminen kaikilla tietoturvan osa-alueilla. Tavoitteeseen pyritään yrityksen tietoturvan kolmen pääalueen avulla, jotka ovat verkon tietoturva, tulosteiden tietototurva sekä asiakirjojen tietoturva. Sharpin kokonaisvaltainen optimoitujen tuotteiden ja ratkaisujen valikoima sekä niihin liittyvät Sharp Professional Services -ammattilaispalvelut kattavat tietojenkäsittelyn ja tietosuojan organisatoriset näkökulmat.

Rakentamalla yrityksen organisaatiotasolle vahvan perustan voimme vaikuttaa loppukäyttäjien toimintaan. Tämä yhdessä Sharpin huolellisesti suunniteltujen ja turvallisten järjestelmien kanssa auttaa yrityksiä täyttämään GDPR:n vaatimukset sekä tarjoaa asianmukaiset välineet riskien mittaamiseen, verkkohyökkäysten estämiseen ja käyttäjiin liittyvien luotettavien tietojen saamiseen.

Sharp Professional Services -ammattilaispalvelut kattavat kaikki tietoturvan osa-alueet, kuten tunnistettavien henkilötietojen käsittely yrityksen järjestelmissä, niin että yritykset täyttävät GDPR:n vaatimukset.

Seuraavassa taulukossa esitetään yhteenveto siitä, miten Sharp voi auttaa täyttämään GDPR:n vaatimukset:

Yleinen tietosuoja-asetus ja Sharp		
Tietoturvan osa-alue	Tuotteet ja ratkaisut	Vaatimustenmukaisuus saavutetaan
Verkon tietoturva	• Sharpin monitoimilaitteet • Sharpin tulostimet • Sharp Remote Device Manager	• käyttöoikeuksien valvonnalla • porttien valvonnalla • protokollien valvonnalla • verkkopalvelujen valvonnalla • datan salauksella • datan ylikirjoituksella
Tulostuksen tietoturva	• Job Accounting II • PaperCut MF • SafeQ • Drivve Image • Prism ScanPath	• käyttöoikeuksien valvonnalla • toiminnallisuuksien rajoituksilla • dataloki/tarkastusraporteilla • datalokien säilytyksellä ja tekemällä tiedot tunnistamattomiksi
Asiakirjojen tietoturva	• Cloud Portal Office • Drivve DM • Docuware • Drivve Image • Prism ScanPath	• tietokannan käytön valvonnalla • käyttöoikeuksien valvonnalla • versionhallinnalla • jäljitysketjulla • asiakirjojen säilytyksellä ja hävittämisellä • auditointilokilla

Yhteenveto

Sharp voi auttaa organisaatioita toteuttamaan tehokkaat tietoturva- ja hallintatoimet GRPR:n vaatimusten täyttämiseksi.

GDPR:n vaatimusten mukaisten toimien ja toimintojen ymmärtäminen, suunnittelu, konfigurointi ja toteutus voivat viedä paljon aikaa ja niiden toteuttaminen voi olla hankalaa, varsinkin koska kaikki yritykset ovat erilaisia.

Sharp suosittelee, että yritysjohto ja IT-vastaavat tutustuvat nettisivuillamme oleviin raportteihin, joissa annetaan ohjeita verkon tietoturvan, tulostamisen tietoturvan ja asiakirjojen tietoturvan varmistamiseksi: https://www.sharp.fi/cps/rde/xchg/fi/hs.xsl/-/html/tietoturvallisuus.htm

Näissä teksteissä kuvataan riskit ja riskien torjuntatoimet. Lisäksi niissä esitellään

- Sharpin tietoturvalliset verkkolaitteet
- Sharpin tietoturvaohjelmistot, jotka auttavat suojaamaan yrityksen tietojen hankintaa ja tuottamista
- Sharpin tietoturvaohjelmisto, joka auttaa suojaamaan sähköiset asiakirjat.

Lisäksi Sharp Professional Services -tiimit tarjoavat konsultointia ja apua tehokkaiden tietoturvatoimien toteuttamisessa sekä erilaisille yrityksille ja erilaisiin tarpeisiin sopivia työkaluja.

Organisaationne muilla alueilla mahdollisesti esiintyvien haavoittuvuuksien torjumiseksi voimme myös auttaa valitsemaan muita tietoturvamenettelyjä Sharpin portfoliosta, niin että voitte varmistaa täysin kattavan suojan kaikille yrityksenne osa-alueille:

- Verkon tietoturva
- Tulostuksen tietoturva
- Asiakirjojen tietoturva
- GDPR-asetuksen noudattaminen.

GDPR-sanasto[3]

Osoitusvelvollisuus – rekisterinpitäjä on vastuussa tietosuojaperiaatteiden noudattamisesta. Rekisterinpitäjän on pystyttävä osoittamaan, miten yritys varmistaa vaatimustenmukaisuuden.

Tietoturvaloukkaus – mikä tahansa vahingossa tapahtuva tai laiton rekisteröidyn tietojen tuhoaminen, kadottaminen, muuttaminen taikka luvaton luovutus tai käyttö.

Rekisterinpitäjä – oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Tietojen poistaminen – (käytetään myös nimitystä oikeus tulla unohdetuksi) rekisteröidyllä on oikeus pyytää rekisterinpitäjää poistamaan rekisteröidyn henkilötiedot.

Tietojen käsittelijä – "käsittely" tarkoittaa kaikkia toimintoja tai toimintojen joukkoa, joka kohdistuu henkilötietoihin tai henkilötietojen ryhmiin. Nämä toiminnot voivat olla automatisoituja tai manuaalisia. Tietojen käsittelyä on esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, käyttö, jäsentäminen, säilyttäminen, muokkaaminen, haku ja hävittäminen. Tietojen käsittelijä voi olla organisaatio tai kolmannen osapuolen palveluntarjoaja, joka hallinnoi ja käsittelee henkilötietoja rekisterinpitäjän puolesta. Tietojen käsittelijöillä on tiettyjä lain mukaisia velvoitteita, kuten tallennettujen henkilötietojen ylläpito, ja he ovat vastuussa tietoturvarikkomuksen sattuessa.

Tietosuojaviranomainen – tietosuojaa valvova kansallinen viranomainen.

Tietosuojavastaava – nimetty henkilö, joka varmistaa, että GDPR:n mukaiset periaatteet ja menettelytavat otetaan käyttöön ja niitä noudatetaan.

Rekisteröity – henkilö, jonka henkilötietoja rekisterinpitäjä tai tietojen käsittelijä käsittelee.

Henkilötiedot – kaikki tunnistettavissa olevaan henkilöön liittyvä suora tai välillinen tieto, jota voitaisiin käyttää kyseisen henkilön tunnistamiseen. Tällaisia tietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitiedot ja internet-tunnisteet.

Käsittely – kaikki henkilötietoihin kohdistuva toiminta tietojen keräämisestä niiden lopulliseen hävittämiseen. Siihen sisältyy muun muassa tietojen sähköinen tai manuaalinen järjestäminen, muuttaminen, tarkastelu, käyttö, luovutus, yhdistäminen ja säilytys.

Lähteet

1. “UK firms could face £122bn in data breach fines in 2018”, ComputerWeekly, lokakuu 2016
2. “CEO Survey”, PwC, 2017
3. “GDPR Glossary of Key Terms”, High Speed Training, helmikuu 2018

SHARP

Be Original.