TOPCERTIFIER
www.topcertifier.com

PALVELUMENETELMÄT GDPR

YLEINEN TIETOSUOJA ASETUS

TOPCERTIFIER
www.topcertifier.com

JOHDANTO GDPR:ään

GDPR-vaatimukset koskevat jokaista Euroopan unionin jäsenvaltiota, ja tavoitteena on luoda lisää kuluttajatietojen ja henkilötietojen johdonmukainen suoja EU-maissa. Osa avaimista GDPR:n tietosuoja- ja tietosuojavaatimukset sisältävät:

- Tietojen käsittelyyn liittyvien suostumuksen vaatiminen
- Anonymisoi kerätyt tiedot yksityisyyden suojaamiseksi
- Tietoturvaloukkausilmoitusten antaminen
- Tiedonsiirron turvallinen käsittely rajojen yli
- Vaaditaan tiettyjä yrityksiä nimittämään tietosuojavastaava valvomaan GDPR:n noudattamista

GDPR velvoittaa sääntelyvaatimukset kaikille yrityksille, jotka käsittelevät EU-kansalaisten tietoja turvata paremmin kansalaisten henkilötietojen käsittelyn ja liikkumisen.

ALKU

Aloituskokous on olennainen työkalu kommunikoida ja suunnitella projektin toteuttamista mahdollisimman vähän esteitä ja saada projekti päätökseen suunnitellussa ajassa ja kustannuksissa. Aloituskokouksen esityslista on:

- Projektisuunnitelmakeskustelu: Tämä sisältää keskustelun vastuullisuudesta ja vastuullisuudesta sidosryhmiä. hankkeen virstanpylväät ja suoritteet
- Palveluiden laajuus
- Laki- ja säädösvaatimukset

YDINTIIMIN LUOMINEN

- Tietosuojavastaavan (DPO) nimittäminen
- Sisäisen GDPR-/GRC-komitean nimittäminen (Governance Risk & Compliance) (*Tarvittaessa)

GDPR TIEDOTUSKOULUTUS

GDPR-tietoisuuskoulutus järjestetään organisaatiosi työntekijöille. Koulutus istunnon tarkoituksena on auttaa työntekijöitä hankkimaan tietoa, ymmärtämään GDPR:n käsitteitä ja mukautumaan prosesseja ja käytäntöjä saavuttaa ja perustaa, toteuttaa, ylläpitää ja parantaa jatkuvasti vaatimustenmukaisuuteen perustuvaa järjestelmätyöympäristöä. Kun esikunnat ovat olleet koulutettuja he voivat ajatella ja toimia sekä edistää tavoitteiden saavuttamista.

TOPCERTIFIER
www.topcertifier.com

GDPR – VAIHE VIISKÄINEN TOTEUTUS

VAIHE I - AUKKO-ANALYYSI

Tämän vaiheen aikana teemme puuteanalyysin tarkistaaksemme, kuinka suuri osa nykyisistä käytännöistäsi on vaatimusten mukaisesti. Nykyiset käytäntösi on verrattu alla oleviin kahteen vertailukriteerit,

- GDPR-vaatimukset
- Laki-, säädös- ja lakisääteiset vaatimukset Tämän analyysin tulokset esitetään Gap Analysis Report -raportin muodossa. Tämä raportti toimii toimintokohteiden luettelona projektin muistutuksessa

VAIHE II – TIETOVIRTA ARVIOINTI

Tässä vaiheessa autamme tietolähteiden tunnistamisessa ja käsittelyssä infrastruktuuria, johon liittyy henkilöstöä, teknologiaa ja fyysistä infrastruktuuria GDPR

VAIHE III – TIETOJEN YKSITYISYYDEN VAIKUTUKSEN ARVIOINTI (DPIA)

DPIA (Data Proctection Impact Assessment) on prosessi, jossa mahdolliset tietosuojaongelmat ja riskit tunnistetaan ja tarkastellaan kaikkien sidosryhmien näkökulmasta. Tämä mahdollistaa organisaatiota ennakoimaan, käsittelemään uusien aloitteiden todennäköisiä vaikutuksia erityisten toimenpiteitä riskien minimoimiseksi/vähentämiseksi. DPIA on suunniteltu minimoimaan haittojen riski voi johtua henkilötietojen käytöstä/väärinkäytöstä puuttumalla tietosuoja- ja yksityisyyteen liittyvät huolenaiheet projektin suunnittelu- ja kehitysvaiheessa

Autamme DPIA-menettelyn ja DPIA-rekisterin kehittämisessä koordinoimalla toimihenkilöiden kanssa päätä niin, että sen pitäisi hyödyttää organisaatiota hallitsemalla riskejä ja välttämällä vahinkoja maine, varmistaa lakisääteisten velvoitteiden noudattaminen ja parantaa suhteita sidosryhmiin.

VAIHE IV – TURVALLISTA HENKILÖTIETOJEN SIIRTOANALYYSI

Autamme analysoimaan, mitä henkilötietoja siirretään yrityksesi ulkopuolelle ja kun autamme myös tarvittavien turvatoimenpiteiden suunnittelussa riittävän suojan takaamiseksi henkilötiedot sekä henkilötiedot, jotka siirretään yrityksen ulkopuolelle

VAIHE V – PROSESSIN KÄYTTÖÖNOTTO TIETOJEN RIKKOJEN VARTEN

Autamme prosessien määrittämisessä henkilötietoloukkausten tunnistamiseksi ja käsittelemiseksi. (Esim. Data loukkausilmoitusmenettelyt) ja avustaa myös tapausten raportoinnin menettelyjen kehittämisessä asianomaiselle valvontaviranomaiselle

VAIHE VI – DOKUMENTAATIOTUKI

Autamme tarvittavien organisatoristen ja teknisten suojatoimenpiteiden toteuttamisessa rekisteröityjen henkilötietoja ja auttaa myös asiaa koskevien asiakirjojen suunnittelussa valvontakäytännöillä ja -menettelyillä, jotka varmistavat, että GDPR on hyvin sisällytetty tietosuojaan organisaatioprosessit

TOPCERTIFIER
www.topcertifier.com

TIETOSUOJAOHJELMA SISÄINEN TARKASTUSKOULUTUS

GDPR Tietosuojavastaavalle järjestetään sisäisen tarkastajan (IA) koulutusta. Tämä koulutus varustaa sellaisia henkilöstöä analysoimaan vaikutustenarvioinnin tarvetta, suunnittelemaan ja ajoittamaan vaikutustenarvioinnin, laatimaan tarkastuslistoja ja suorittamaan vaikutustenar vioinnin sekä dokumentoimaan ja raportoimaan havainnot ylimmälle johdolle

GDPR SISÄINEN TARKASTUS

Asiantuntijamme valvovat tietosuojavastaavan suorittamaa sisäisen tarkastuksen suorittamista. Tämä sisäinen tarkastus tekee tunnistaa vielä olemassa olevat puutteet järjestelmässä ja osoittaa valmiustason kohdata ongelma vaatimustenmukaisuuden tarkastus. Tämä auditointi antaa organisaatiolle mahdollisuuden tunnistaa ja korjata kaikki ei-vaatimustenmukaisuus ennen kuin jatkat vaatimustenmukaisuustarkastukseen. Ylimmälle johdolle ilmoitetaan asiasta sisäisen tarkastuksen havainnot.

GDPR - PERUSSYYANALYYSI (RCA) JA KORJAAVAT TOIMENPITEET

Kaikki sisäisen tarkastuksen, asiakkaan tai kolmannen osapuolen auditoinnissa tai alkaen havaitut poikkeamat Riskirekisteri, DPIA-rekisteri, Tapahtumalokit, Tietojen varmuuskopiointilokit, Tietoturvaloukkausilmoitukset, Vulnerability Assessment & Penetration Test (VAPT), tietojen säilytyslokit ja muut lähteet pitää listata. RCA suoritetaan käyttämällä tekniikoita, kuten Brainstorming- ja Fish-Bone-menetelmiä. Optimaaliset korjaus- ja korjaavat toimenpiteet toteutetaan ja niiden tehokkuus toimet dokumentoidaan ja tarkistetaan GDPR-korjausraportin (CAR) avulla.

Asiantuntijamme ovat paikalla tiimisi kanssa opastamassa prosessin läpi.

TOPCERTIFIER
www.topcertifier.com

GDPR JOHDON KATSAUS KOKOUS (MRM)

MRM on tilaisuus kaikille sidosryhmille tavata sovituin väliajoin tarkastelemaan, keskustelemaan ja suunnittelemaan toimia alla olevissa asialistan kohdissa,

- DPIA-raportit
- Poikkeamat vaatimustenmukaisuusnäkökohdista
- Toimituksen jälkeiset raportit
- Toimintasuunnitelma avoimien asioiden ratkaisemiseksi
- Järjestelmässä tarvittavat parannusmahdollisuudet ja muutokset

GDPR:N NOUDATTAMISEN TARKASTUS

Kun valmiusaste on saavuttanut riittävän tason, Compliance-prosessi sertifiointi alkaa. Sertifiointielimen (CB) nimetty auditoija varmistaa valmiuden ulkoisen auditoinnin kautta. Tämä edellyttää, että tarkastaja tarkistaa politiikat, prosessit, SOP:t, kriittiset operatiiviset tiedot sekä IA- ja MRM-tietueet. Kaikki merkittävät poikkeamat CB:n odotuksista ilmoitetaan tässä vaiheessa tarvittavien korjausten tekemiseksi. Tämä vähentää mahdollisuuksia merkittäviä poikkeamia sertifiointitarkastuksen aikana. TOPCertifier on yhteydessä kaikkiin sidosryhmiä ja valvoa tarkastuksen sujuvaa loppuunsaattamista.

NOUDATTAMISEN JATKAMINEN

TOPCertifier on osa organisaatiosi vaatimustenmukaisuuspolkua ja auttaa sinua säännöllisesti välein tarvittavat koulutukset, järjestelmätuki ja puput, sisäiset ja ulkoiset auditoinnit ja vaatimustenmukaisuustodistuksesi säännöllinen uusiminen.