GDPR ja dokumenteerimiskohustus

Mihkel Miidla

10.05.2017

Infoturbe SUMMIT 2017

SORAINEN

www.sorainen.com

Lähtekoht: Vastutuse põhimõte

- **GDPR-is isikuandmete töötlemise põhimõtted üldjoontes väga sarnased Direktiiviga 95/46**
- **Uus: Vastutuse põhimõte** (Art 5 lg 2)
  - Vastutav töötleja **vastutab** GDPR-i nõuete täitmise eest (isikuandmete mis tahes töötlemisel tema poolt ja tema nimel)
  - Peab suutma seda **tõendada**

Vastutava töötleja vastutus (Art 24)

- Kohustus rakendada **asjakohaseid tehnilisi ja korralduslikke meetmeid**, et **tagada** ja **suuta tõendada** isikuandmete töötlemist kooskõlas GDPR-iga.
  - Arvestades töötlemise laadi, ulatust, konteksti ja eesmärke, samuti füüsiliste isikute **õigusi ja vabadusi ähvardavaid** erineva tõenäosuse ja suurusega **ohte**
  - Vajaduse korral tuleb meetmed läbi vaadata ja **kaasajastada**

Dokumenteerimiskohustus

- Suutlikkus tõendada kooskõla GDPRiga ning meetmete tõhusust on saavutatav dokumenteerimise kaudu.
- Üldine soovitus - kui vastutav töötleja midagi hindab, kaalub, kasutab mõnda tingimuslikku õigust GDPR-ist, siis sellised sammud/otsused tuleks alati dokumenteerida.
- Mis kasu on dokumenteerimiskohustuse korrektsest täitmisest?
  - Vastutuse (ulatuse) kindlaksmääramine järelevalvemenetluse käigus
  - *Proper housekeeping*

Isikuandmete töötlemise toimingute registreerimine (Art 30)

- Mida tähendab? *(maintain a record, processing register, data mapping, data flow chart)*
- Kohustuslik, kui:
  - organisatsioonis 250+ töötajat; või
  - kui töötlemine kujutab ohtu andmesubjekti õigustele ja vabadustele; või
  - kui töötlemine ei ole juhtumipõhine; või
  - töödeldakse delikaatseid isikuandmeid (Art 9) või süütegudega seotud andmeid (Art 10).
- NB need ei ole kumulatiivsed, piisab ühest

Isikuandmete töötlemise toimingute registreerimine (Art 30)

- Registreerimine on kirjalik, sealhulgas elektrooniline
  - Andmekaitseasutused on alles vastavaid näidisdokumente välja töötamas
- Nõudmisel tuleb register teha kättesaadavaks järelevalveasutusele
- Registreerimiskohustused ka volitatud töötlejatel! (Art 30 lg 2)

Isikuandmete töötlemise toimingute registreerimine (Art 30)

- Registreerida tuleb muuhulgas:
  - Vastutava töötleja nimi ja kontaktandmed, samuti juhul kui on asjakohane, siis Andmekaitseametniku (DPO) nimi ja kontaktandmed (**KES?**)
  - Töötlemise eesmärgid (**MIKS?**)
  - Andmesubjektide kategooriad (**KELLE?**)
  - Isikuandmete liikide kirjeldus (**MIS?**)
  - Vastuvõtjate kategooriad (**KELLELE?**)
  - Andmeliikide kustutamiseks ettenähtud tähtajad (**MILLAL?**)
  - Turvameetmete kirjeldus (**KUS? KUIDAS?**)

Isikuandmete töötlemise toimingute registreerimine (Art 30)

- Töötlemise toimingute registri pidamine on pidevalt kestev protsess
- Kuidas tagada, et registrisse jõuaksid asjakohased kanded ja kuidas seda tagada selle kaasajastamine?
  - Määra oma organisatsioonis kindlaks (vastutav) isik ja eralda vajalikud ressursid
  - Koosta või uuenda tööprotsesside kirjeldused nii, et oleks tagatud kannete/uuenduste jõudmine registrisse
  - Taga kehtestatud tööprotsesside kirjelduste täitmine

Töötlemine õigustatud huvi korral (Art 6 lg 1 p f)

- Töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi **kaaluvad** üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, **eriti juhul** kui andmesubjekt on laps
- Seos dokumenteerimiskohustusega:
  - Hõlmab vastutava töötleja poolset otsust ja huvide kaalumist. Seega põhjendused ja otsustamisprotsess tuleb dokumenteerida.
  - Teavitamiskohustuse täitmine (Art 13, 14)

Töötlemine õigustatud huvi korral

- Teatud juhtudel jaatab GDPR õigustatud huvi olemasolu, sh:
  - Pettuste vältimiseks;
  - Kontsernisisene edastamine;
  - **Võrgu- ja infoturbe tagamine:**
    - Ulatuses, mis on rangelt vajalik ja proportsionaalne;
    - Piiratud isikute ring – avaliku sektori asutused, CERT, CSIRT, elektroonilise side teenuse osutajad, turvatehnoloogiate ja –teenuste pakkujad.

Rikkumistest teavitamine (Art 33, 34)

- Rikkumistest tuleb teavitada järelevalveasutust ja teatud juhtudel (suur oht füüsiliste isikute õigustele ja vabadustele) ka andmesubjekte
- Vastutav töötleja **dokumenteerib** kõik isikuandmetega seotud rikkumised, sealhulgas isikuandmetega seotud rikkumise asjaolud, selle mõju ja võetud parandusmeetmed.

Muud dokumenteerimiskohustused (mitteammendav loetelu)

- Otsus ja põhjendused andmekaitsespetsialisti (DPO) määramata jätmise kohta;
- Art 49 lg 1 teises lõikes toodud erandi alusel isikuandmete edastamine nn kolmandasse riiki;
- Andmesubjekti nõusolekud, kui töötlemise õiguslik alus on nõusolek (tõendamiskoormis!);
- Andmekaitsealase mõjuhinnangu läbiviimine;
- Juhtumid, kui vastutav töötleja ei nõustu (ei arvesta) DPO soovitustega.

Tänan!

Mihkel Miidla

Vandeadvokaat

+372 6 400 959

mihkel.miidla@sorainen.com

SORAINEN

ESTONIA
Pärnu mnt 15
10141 Tallinn
phone +372 6 400 900
estonia@Sorainen.com

LATVIA
Kr. Valdemāra iela 21
LV-1010 Riga
phone +371 67 365 000
latvia@Sorainen.com

LITHUANIA
Jogailos 4
LT-01116 Vilnius
phone +370 52 685 040
lithuania@Sorainen.com

BELARUS
ul Internatsionalnaya 36-1
220030 Minsk
phone +375 17 306 2102
belarus@Sorainen.com

www.Sorainen.com