FOCUS [IT] INFORMATION SECURITY

GDPR – millest pihta hakata?

Doris Matteus

15.05.2018

Riskid

- “Äri”risk:
  - Töötlemise alus (nõusolek)
  - Andmete kaitsmine (sh turvameetmed, teadlikkus jne)
- Järelevalve:
  - Õiguslik alus
  - Dokumentatsioon
  - Mõjuhinnang

Soovituslikud sammud

- Andmekaitsespetsialist (või keegi teine, kes andmekaitsest teab)
- Andmete kaardistamine
- Gap-analüüs ehk olukorra analüüs
- Tööprotsessid ja dokumendid
- Andmesubjekti õigused
- Andmete kaitsmine
- Mõjuhinnang
- Rikkumised
- Teadlikkus

Andmekaitsespetsialist

- Kas andmekaitsespetsialist (või keegi muu, kes asju teab) on määratud?
- Kas on olemas andmekaitsespetsialisti tööks vajalikud ressursid?
- Kas andmekaitsespetsialist saab teha oma tööd sõltumatult?
- Kas andmekaitsespetsialisti kontaktandmed on kättesaadavad nii organisatsiooni sees kui ka organisatsioonivälistele isikutele?

Andmete kaardistamine

- Kas tead, milliseid isikuandmeid organisatsioon töötleb?
- Kas kõigi andmete töötlemiseks on olemas õiguslik alus?
- Kas kõigi andmete kohta on teada nende päritolu ning koht, kus neid hoitakse?
- Kas kõigil andmetel on määratud töötlemise tähtaeg?
- Kas kõigi andmete kohta on teada, kes neile ligi pääsevad?
- Kas ja kellele andmeid edastatakse?

Gap analüüs

- Kas nõuete kogum on piisav, et saada täielik ülevaade nõuete täitmisest?
- Kas oled hinnanud nii formaalset töökorraldust ehk dokumentatsiooni kui ka seda, kuidas asju tegelikult tehakse?
- Millised sammud tuleb teha puuduste kõrvaldamiseks?
- Millised on iga konkreetse puuduse kõrvaldamise tähtajad ja kes on vastutajad?

Dokumendid ja tööprotsessid

- Kas kõigi andmete töötlemiseks on olemas õiguslik alus?
- Kas on määratud ja koostatud piisav ning tarvilik dokumentatsioon, millega tagada vajalike andmekaitse meetmete loomine, rakendamine ning sisemine igapäevane kontroll kõigil juhtimistasanditel?
- Kas töötajad teavad, kuidas töödelda isikuandmeid?
- Kas töötajad teavad, kuidas rikkumisi ära tunda ning menetleda?
- Kas on olemas protsess andmesubjekti taotluste täitmiseks?

Andmesubjekti õigused

- Kas on tagatud piisav teave andmesubjektile?
- Kas suudetakse anda andmesubjektile infot selle kohta, milliseid isikuandmeid tema kohta töödeldakse?
- Kas andmete õigsuse tagamise protseduur on olemas?
- Kas isikuandmete kustutamine on vajadusel võimalik?
- Kas isikuandmete ülekandmine on võimalik (eeldusel, et töödeldakse on andmeid, mille osas sellist nõuet saab esitada)?

Andmekaitse ajakohastamine

- Kas on määratud andmekaitse kõigi tasemete eest vastutajad – juhtkonnas, IT-juhtimine ja -haldus, IT-turvalisus, isikuandmete andmebaaside omanikud jne?
- Kas andmekaitse kordasid ja rakendatud meetmeid vaadatakse regulaarselt üle ning tehakse täiendusi, muudatusi?
- Kas juhtkonnale tehakse regulaarselt aruandeid ning need on juhtkonnas aruteluks?
- Kas töötajad tunnevad kehtivaid kordasid ning omavad piisavat infot andmekaitsest?

Mõjuhinnang

- Kas kõik isikuandmete töötlemise tööprotsessid on kirjeldatud ja neis kasutatavad isikuandmed kaardistatud?
- Kas on isikuandmete töötlemises toiminguid või kasutusel tehnilisi lahendusi, mis võiksid põhjustada isikutele suurt ohtu läbi andmetega toimuvate intsidentide?
- Kas kõik riskianalüüsis tuvastatud riskid on maandatud?
- Kas kõigile määruses nõutud kriteeriumid on mõjuhinnangus kirjeldatud?

Rikkumiste teavitamine

- Kas on olemas rikkumistest teavitamise kord ja protsess?
- Kas kõik asjasse puutuvad isikud oskavad rikkumisi ära tunda?
- Kas on olemas tehnilised abivahendid rikkumiste äratundmiseks?
- Kas kõik asjasse puutuvad isikud on korrast teadlikud ning teavad, mida teha?

Teadlikkus

- Kas kõik erinevad sihtrühmad on koolitatud?
  - Isikuandmete töötlemine
  - Küberhügieen
  - Andmekaitse
- Kas koolitusi (ja võimaluse korral teste) korratakse regulaarselt?

Tänan!