GDPR és ISO 27001, tanúsíthatóság – fél évvel a GDPR életbe lépése után

XXVII.
MAGYAR MINŐSÉG HÉT
2018

Móricz Pál –ügyvezető igazgató
Szenzor Gazdaságmérnöki Kft.
2018. november 06.

Tartalom

- 27001 és GDPR viszonya
- szemelvények az elmúlt félévben felmerült kérdésekből
- GDPR haszna a szervezetek számára
- hol tartunk
- tanúsítás

27001 és GDPR közötti kapcsolat

- személyes adat is információ védelme része információbiztonságnak
- IBIR követelmények között
  - jogszabályok (külső kontexusok) azonosítása
  - érintettek (érdekelt felek) elvárásainak meghatározása
  - magántitok és személyhez köthető info-k védelme
- *IBIR megfelelés része GDPR megfelelés*
  - *IBIR tanúsító vizsgálja GDPR megfelelést*
  - *de nem nézi tételesen GDPR követelmények teljesítését*

Hol kezelünk - számbavétel

- Hol kezelünk, tárolunk személyes adatokat
  - hasonló funkció, mint IBIR vagyonleltár, de kapcsolódó információk, mélység más
  - dokumentálása: adatkezelési nyilv. (ahol van)
- Gyűjtés,felmerült kérdések
  - nincs kérdés: jogi köv. (m.ügy, bér, TB, adó), IT alkalmazások, kamera, beléptető rendszer, partner-kapcsolati adatok, toborzási adatok, DM lista, teljesítmény értékelés, stb.
  - „fájl szerver, levelezés nem nyilv. rendszer” *de az*
  - „hozzáférnek, de nem használják” *ez is benne*
  - „tevékenységeivel összefüggésben végzett” adatkezelés határai, pl. belső rendezvény fénykép?, személyes mappákban tárolt adatok?

Adatkezelői, feldolgozói nyilvántartás

- Hol kell?
  - **250 főnél nagyobb szervezetnél**, **és**
    ha kockázattal jár, *nem alkalmi jellegű*, vagy különleges vagy büntetőjog/bűncselekmény adatot kezelnek
- Hol célszerű? kulcs: mi a cél, hozzáadott érték, pl:
  - áttekinthetőség (*ha adat csak jogi előírás miatt és kapcsolattartás szerződés teljesítéshez??*)
  - válaszhoz info, ha kérdeznek (érdekelt, hatóság)
- Mélység
  - adat, vagy rekord szintű?, kapcsolódó info-k köre)
  - *ami a nyilvántartási céljához kell*

Adatvédelmi tisztviselő (DPO)

- Hol kell
  - „közhatalmi és közfeladatot ellátó szervnél (kivéve bíróság)
  - fő tevékenységben érintettek rendszeres és szisztematikus, nagymértékű megfigyelése
  - fő tevékenységben különleges adatok vagy büntetőjoghoz kapcsolódó adatok nagy számban”
- Szerep
  - felügyeleti, tanácsadói funkció (nem ibtv adatvédelmi felelős!) – *legtöbb helyen bevezetésért is felel??*
  - érintett info kérésekre válaszadó

Technikai és szervezési intézkedések

- megfelelő adatbiztonság, figyelembe véve
  - „tudomány, technika állása, megvalósítás ktg, kezelés jellege, hatóköre, körülményei, céljai, személyekre jelentett kockázat”
  - jellemző kockázatok, néhány kezelési eszköz felsorolás
- *ez kockázatfelmérés és IBIR*
  - de új (GDPR) kritériumok miatt új kockázatok, szigorodó következmények miatt súlyosság nőhet
  - kontrollok is áttekintendők, célszerű-e újabbat bevezetni
  - fejlesztések, változások esetén újra átgondolás
  - (de ezek is IBIR követelmények…)
  - szükség esetén érdeksérelmi vizsgálat (ez pedig egy célzott, speciális kockázatfelmérés)

Adatvédelmi szabályzat

- Adatvédelmi szabályzat
  - „a jogszabályi követelményeket másoljuk be egy szabályzatba, néhány felelőst, papírt rendeljünk hozzá” (lásd MIR 1998 megközelítés…)
  - minden benne van, hosszú, senki sem olvassa (és így naprakészsége sem érdekel senkit)
  - pedig szabályozás struktúra, tartalom kiindulópont:
    - ki a vevője,
    - mire van szüksége (pl. folyamat átláthatóságra, felelősség/szerepek/feladat tisztázásra, info háttér helyére?),
    - hogyan használják

Külső, belső tájékoztatók

XXVII. MAGYAR MINŐSÉG HÉT 2018

- Külső,belső tájékoztatók
  - sok papír, aláírás,
    pedig pl. tv-t aláírás nélkül is be kell tartani…
  - szabályzatnál leírtak itt is igazak…
  - más cél, más mód (pl. utcai kamera, vásárlói nyereményjáték, jelentkezési vagy közösségi oldal regisztráció)
  - legyen minden (az érintett számára!) fontos részlet elérhető, de egyszerre csak annyi, amennyiből eldöntheti, érdekli-e a többi

Adatfeldolgozói szerződések

- Jogász szemmel, megfelelés formális biztosítása
  - jogszabály követelmények bemásolása
  - minden felelősség áthárítása
  - legyen „papír”
- XXI. század: gyors döntés, egyoldalas megállapodások ⇔ hosszú jogi szöveg
  - ki olvassa el?
- Mindig le kell írni? hozzáadott értéke (érintettnek)
  - kockázat? félreérthetőség?

    pl. csak kapcsolattartási információk és üzleti információ (közte személyes adatok is), van titoktartási előírás – kockázat, érintettre hatás indokolja?

Továbbítás EU-n kívül

- Anyacég EU-n kívüli
  adatok nála, vagy szolgáltatójánál
  - GDPR: „jóváhagyott ország vagy szerződés vagy belső szabályozás…”
  - átgondolandó, de megoldható
- Felhő, közösségi oldalak
  - felhőben van kockázat, de a nem felhőben is
  - kellő gondosság
  - *kockázattal arányos védelmi intézkedés (pl. titkosítás, hozzáférés szabályozás, 2 faktoros azonosítás, stb.)*

Törlés

- Egyik legkeményebb GDPR előírás
  - **„jogalap megszűnt – törlendő, minden másolatból is”**
  - megőrzési idő meghatározandó (ez IBIR)
  - *lejártakor lehet-e új jogalap?*
    pl. adatbázis, mentés integritás megőrzés, jogos érdek („ami érdekeltnek nem fáj”)
- Technikai ill. aránytalan ráfordítás gondok
  - kamera szoftver nem tudja automatikusan
  - összes mentésben megkeresés, törlés?
- *De: gondoskodni kell, ne lehessen más célra használni!*

Adatvédelmi hatásvizsgálat

XXVII. MAGYAR MINŐSÉG HÉT 2018

- Mikor kell?
  - magas kockázatú adatkezelés, új technológia esetén, kezelés előtt (hatóság is előírhatja)
  - kockázat változása esetén ellenőrzés
  - Elemei
    adatkezelés leírása, célja
    műveletek, szükségesség, arányosság vizsgálata
    kockázatok vizsgálata
    kezelési intézkedések
- Ez ma is IBIR folyamat
  - *információs rendszer biztonsági követelmények meghatározása, kockázatfelmérés és kezelés, biztonsági tesztek – de bele kell tenni!*
- Ma még csak néhány példa

És még van sok részkérdés

- incidenskezelés, nyilvántartás, bejelentés
- profilozás
- hordozhatóság
- álnevesítés
- érintettek jogainak biztosítása,
- stb.

GDPR előnyök (a szervezet számára)

- Követelmények, kockázatok áttekintése
- Cél, jogalap áttekintése
- Szerepek tisztázása
- Folyamatok, gyenge pontok áttekintése
- Rendcsinálás, takarítás
- Biztonsági intézkedések felülvizsgálata (IBIR)
  - hozzáférés felülvizsgálat, titkosítás, álnevesítés
  - biztonsági tesztek, sérülékenység vizsgálatok
  - rendcsinálás, felesleges kezelés/másolat/őrzés/ mentés kitakarítása, stb.
- Áttekinthetőség

Hol tartunk

- Helyzet
  - sokan foglalkoznak vele, de
  - kevesen, akik már csak „üzemeltetik”, és
  - sokan kivárnak
  - sok kisördög
- Veszély
  - sok adminisztráció, nem a lényegről,
  - formális megfelelések
- Fő szempont legyen:

Józan ész + érintett érdeke alapján döntés

Tanúsítás

- Akkreditálási törvényben: NAH + NAIH
- Még nincs tisztázva
  - Akkreditálási követelményrendszer (ISO 17021 rendszer, vagy ISO 17065 termék tanúsítási alap
  - hozzá GDPR vonatkozó fejezet
  - + útmutató? (NAIH EU-ra vár, szeptemberben elnapolták…
  - tanúsítók már jelentkeztek…
- Kell még
  - „NAR”
  - érdekelt fél egyeztetés
- Mikor?

Elérhetőség

Móricz Pál **Mobil: 20-931-0584**

p.moricz@szenzor-gm.hu

Szenzor Gazdaságmérnöki Kft.

1087 Budapest, Könyves Kálmán körút 76.

Telefon: (+36)-1-331-5523

Fax: (+36)-1-311-9636

E-mail: szenzor@szenzor-gm.hu

Honlap: www.szenzor-gm.hu

„Változással a sikerért”