IFKA gazdaságfejlesztési konferencia, 2018.12.06.

GDPR TANÁCSADÓI SZEMÜVEGGEL

Dr. Horváth Zsolt

INFOBIZ

Miről is beszélünk? – Mi a GDPR?

- **AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről**

- **általános adatvédelmi rendelet**
  (**G**eneral **D**ata **P**rotection **R**egulation)

- **Kötelező számon kérhető betartása 2018. május 25-től. – MÁR ELMÚLT!**

Része-e a GDPR megfelelés az ISO-nak?

ISO 9001 – minőségirányítási rendszer:

- 4.2. Külső érdekelt felek lényeges követelményei → *jogszabály betartása*
- 7.5. Dokumentált információk kezelése → *a személyes adatok a dokumentált információkban jelennek meg*
- 6.1. Kockázatok kezelése → *a személyes adatok nem megfelelő kezelésével jogsértés, közvetlen károkozás, stb. lehetséges*

ISO 27001 – információbiztonsági irányítási rendszer:

- Az egész rendszer célja: a folyamatokban kezelt adatok biztonsága (bizalmassága, sértetlensége és rendelkezésre állása) sérülése miatti károk minimalizálása → *a személyes adatok részei a folyamatokban kezelt adatoknak!!!*

Miben segít egy már bevezetett 'ISO rendszer' – a GDPR megfelelésben?

- Adatkezelési tevékenységek felmérése folyamatok mentén → *vannak definiált, (dokumentáltan) szabályozott folyamatok*
- Kezelt személyes adatok azonosítása
  → ***ISO 9001 esetén:*** *dokumentált információk azonosítottak, kiindulási alap lehet*
  → ***ISO 27001 esetén:*** *van módszertan és folyamat adatvagyon azonosítására és osztályozására, adatvagyon (esetleg személyes adatokkal is) már azonosított*
- Az adatvédelmi kockázatok meghatározása
  → ***ISO 9001 esetén:*** *szemlélet a fejlesztések kockázatalapú bevezetése*
  → ***ISO 27001 esetén:*** *van módszertan és folyamat információbiztonsági fenyegetések, gyengepontok és kockázatok felérésére, ami alkalmazható*
- Adatvédelmi intézkedések → ***ISO 27001 esetén*** *már van információbiztonsági intézkedés katalógus, ami kiterjed ezekre a követelményekre is*
- Adatvédelmi menedzsment keretrendszer meghatározása → *már van vállalati menedzsment keretrendszer, ami alkalmazható erre a témára is*

Mit is vár el a GDPR a szervezetektől?

- **Követelményeket fogalmaz meg a személyes adatok kezelésével kapcsolatban**
  - **Mikor kezelhető egyáltalán** (adatkezelés jogalapja)
  - **Milyen alapelvek legyenek betartva** (szempontok a kezelés mértékére, módjára, …)
  - **Érintettek jogainak biztosítása és ennek kommunikálása**
  - **Elszámoltathatóság** (mindig, garantáltan működjön, és ez igazolható is legyen)
  - **Adatbiztonság** kellő mértékű megléte (mindig, kockázat-alapú)

- **De végrehajtási keretet nem ír elő hozzá …**
  - **Ránk bízza a végrehajtás módját**!

GDPR-szerű működés komponensei

- Személyes adatkezelések a szervezet tevékenységeinek részei
- Személyes adatkezelések jogi megfelelése
- Kezelt személyes adatok nyilvántartása
- Kezelt személyes adatok biztonsága (főképp bizalmassága)
- Megfelelés elszámoltathatósága (dokumentált szabályozottság, feljegyzések)

Szükséges ismeretek a GDPR-szerű működéshez

• Személyes adatkezelések a szervezet tevékenységeinek részei	• Folyamatmenedzsment / ISO ismeretek
• Személyes adatkezelések jogi megfelelése	• Jogi ismeretek
• Kezelt személyes adatok nyilvántartása	• Folyamatmenedzsment ismeretek
• Kezelt személyes adatok biztonsága (főképp bizalmassága)	• Információbiztonsági ismeretek (IT biztonság és nem IT biztonság, szervezés)
• Megfelelés elszámoltathatósága (dokumentált szabályozottság, feljegyzések)	• Folyamatmenedzsment, vezetési / ISO ismeretek

Tapasztalatok – ISO-s szervezeteknél

- Sok helyen nincs még semmi
  (kivárás, „úgyse minket fognak ellenőrizni”)
- Rengeteg a letölthető, (majdnem) ingyen minta, illetve a (CTRL C + CTRL V)-módszer alkalmazása
  (valami már van, és a KKV szektorban első esetben nincs büntetés)
- Megbízott külső tanácsadók általi anyagok színvonala, tartalma, használhatósága … nagyon eltérő
  (külső tanácsadó melyik szakmát … melyik iskolát …képviseli)
- Volt régi adatvédelmi szabályozás … azt aktualizálták.
- …
- És persze vannak gondosan összerakott, jó rendszerek is. ☺

Problémák

Hatósági (külső elvárási) oldalról:

- GDPR követelményei túl általánosak – ellentmondások is vannak benne
- Infotörvény és maga a GDPR több helyen ellentmondanak egymásnak
- Nincsenek még meg az ágazati jogszabályok, illesztések
- Nincs (kevés) a használható hatósági állásfoglalás, útmutató

Szervezeti, vállalati (megfelelési) oldalról:

- Nagyon sok szervezet még semmit se csinált
- Sokan csak formális szabályozást készítettek valódi működés nélkül
- GDPR kiépítést (szabályozást) sokszor csak egy területnek adják oda (egyféle szaktudás)
- A jogászok külön sziget-megoldása sokszor nem integrált a vállalati szabályozási rendszerbe
- Valódi, életszerű problémákra kevés a jó megoldás

KÖSZÖNÖM MEGTISZTELŐ FIGYELMÜKET!