ISOFÓRUM Tavasz - 2018. Konferencia, 2018.04.20.

„A minőségirányítás a vállalati jó működés támogatója.”

Ne feledkezzünk meg az információmenedzsmentről és az adatbiztonságról sem!

AZ INFORMÁCIÓMENEDZSMENT ÉS A GDPR ADATBIZTONSÁG INTEGRÁLÁSA AZ IRÁNYÍTÁSI RENDSZEREKHEZ

Dr. Horváth Zsolt

INFOBIZ

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**!

Egy követelményrendszer szervezeti szinten, elszámoltathatóan és mindig megbízhatóan akkor működik, ha

- ***(dokumentáltan) szabályozott,***
- ***van felelőse,***
- ***tervezett, betartott és felügyelt,***
- ***folyamatosan aktualizált,***
- ***része a szervezet működésének.***

→azaz menedzselt vállalati szinten

Akkor mire van szükség?

A személyes adatok kezelése vonatkozásában:

- **Vállalati szabályozási rendszert kell kialakítani, fenntartani, üzemeltetni, felügyelni és fejleszteni (PDCA)**

…

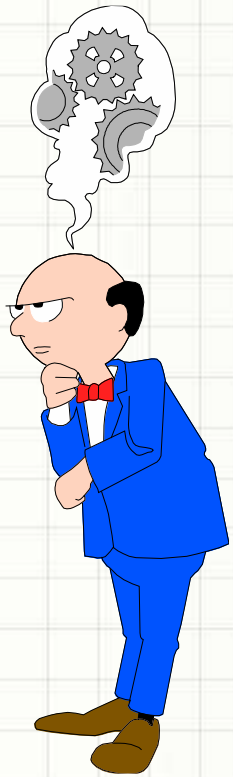
- **Vagy ha már van vállalati irányítási rendszer, akkor … ezeket az új követelményeket oda kell beilleszteni!**

Főbb lépések a személyes adatkezelés rendszerének kiépítéséhez

1. Személyes adatokat tartalmazó adatkörök felmérése
2. Folyamatokban személyes adatok kezelése jelenlegi módjának felmérése
3. Személyes adatok kezelése módjának jogi megfelelési vizsgálata
4. Személyes adatok kezelése módjának biztonsági megfelelési vizsgálata
5. Személyes adatok kezelési folyamatai szabályozásainak *(ha vannak)* módosítása, szükség esetén kialakítása *(megfelelve a vonatkozó GDPR követelményeknek)*
6. Ehhez a szükséges szervezet létrehozása, felelősök, feladataik és hatáskörük szabályozása
7. A szükséges adatvédelmi dokumentációk (nyilvántartások, igazolások, …) létrehozása
8. Az adatkezelés rendszere működésének bevezetése, …

1. Személyes adatokat tartalmazó adatkörök felmérése

- Milyen személyes adatokról van szó egyáltalán?
- Milyen személyes adatokat kezel a szervezet?
- Kiknek a személyes adatai azok? *(alkalmazottak, ügyfelek, ügyfelek ügyfelei, partnerek, stb.)*
- Milyen tömegű személyes adatokról van szó?
- Van-e közöttük különösen érzékeny, illetve különleges adat?



2. Folyamatokban személyes adatok kezelése jelenlegi módjának felmérése

- Hogyan is történik most a személyes adatok kezelése nálunk?
- Milyen folyamataink (tevékenységeink) vannak?
- Szabályozott-e azok működése (dokumentáltan)?
- Történik-e ezekben a folyamatokban személyes adatok kezelése?
- Milyen célból kezeli a folyamat azokat a személyes adatokat?
- Hogyan szabályozottak (a folyamaton belül) a személyes adatok kezeléséhez kapcsolódó tevékenységek?
- Hol és meddig tároltak a személyes adatok – papíron és elektronikusan?
- Hogyan lehet a tárolt személyes adatokhoz hozzáférni papíron, és elektronikusan (fizikailag ill. logikailag)?
- Kik férhetnek hozzá a személyes adatokhoz?

3. Személyes adatok kezelése módjának jogi megfelelési vizsgálata

- Meghatározott-e a folyamatokban minden személyes adat kezelésének a jogi alapja? *(Kezelhetjük-e egyáltalán ezeket a személyes adatokat?)*
- Teljesülnek-e a folyamatokban a személyes adatok kezelésénél a GDPR által meghatározott alapelvek? – *És a személyes adatok továbbítása, automatizált döntéshozatalhoz való felhasználása esetében, stb. is teljesülnek a kapcsolódó követelmények, alapelvek? (Kezelhetjük-e így ezeket a személyes adatokat?)*
- Biztosítottak-e az érintett személyek számára az adatkezelésükkel kapcsolatos jogaik – és tájékoztatottak-e ők ezekről? *(Tudják-e az érintettek, hogy mit kezelünk őróluk, és ezzel kapcsolatban hogy ők mit tehetnek?)*
- Meghatározottak-e a felelősök, és feladataik, felelősségeik?
- Igazolhatók-e (dokumentáltan) mindezek folyamatos megléte? *(Része-e mindez dokumentáltan szabályozott folyamatnak?)*

→Hiányok megállapítása!

4. Személyes adatok kezelése módjának biztonsági megfelelési vizsgálata

Meghatározott-e a folyamatokban

- minden személyes adat előfordulásának helye? *(papíron, egyéb hagyományos adathordozón, elektronikusan /// eredeti és másodpéldányok helye, …)*
- a személyes adatokat tartalmazó adathordozók tárolása?
- az adatokhoz / adathordozókhoz való hozzáférési lehetőségek és jogosultságok?
- a jogos adatkezelés számára szükséges rendelkezésre állás biztosítása?
- az illetéktelen hozzáférés / módosítás / … általi kár mértéke, azok kockázata?
- a magas kockázatok esetére szükséges adatbiztonsági intézkedések?
- az (esetleges) incidensek esetén a teendők?

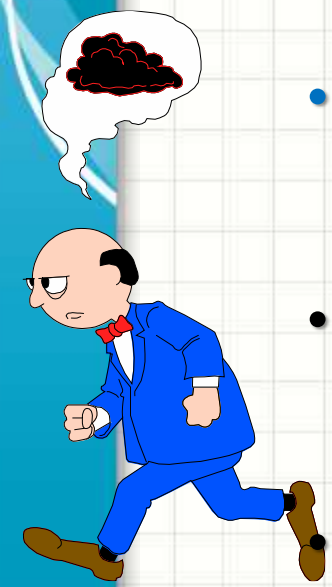
Igazolhatók-e (dokumentáltan) mindezek folyamatos megléte? *(Része-e mindez dokumentáltan szabályozott folyamatnak?)*

→Hiányok megállapítása!

5. Személyes adatok kezelési folyamatai szabályozásainak kialakítása, módosítása

A feltárt hiányok pótlása, kijavítása:

- adatkezeléshez a jogi alap hiányzik → *adat NEM kezelhető!*
- adatkezelés alapelvei sérülnek, érintettek jogai nem biztosítottak → *ezek biztosítása a folyamatban / tevékenységben, adminisztratív vagy technikai intézkedéssel, szabályozottan*
- érintettek nem tájékoztatottak a jogaikról → *érintettek számára elérhető tájékoztatás készítése a jogaikról és azok gyakorlásának lehetőségeiről*
- adatbiztonsági veszélyek, kockázatok nem ismertek → *információbiztonsági fenyegetések és gyengepontok feltárása, kockázatok felmérése*
- adatbiztonsági intézkedések nincsenek, nem megfelelőek → *szükséges adminisztratív vagy technikai intézkedések kidolgozása, bevezetése*



6. Adatvédelmi szervezet létrehozása, felelősök, feladataik és hatáskörük szabályozása

- Az adatvédelem szervezetének, felelőseinek létrehozása, a szervezet keretein belül (adatvédelmi tisztviselő)
- Az adatvédelem felügyelete, ellenőrzése feladatainak definiálása
- Működési (operatív) folyamatok szabályozásában módosítások végrehajtása – a személyes adatok kezelésének szükséges módosításaival
- Ezek egységes, dokumentált szabályozása – integrálva a szervezet működési szabályozási rendszerébe

- **Keretrendszerbe illesztési lehetőségek:**
  - *ISO rendszerhez illesztés (ISO 27001, ISO 9001, …)*
  - *Magatartási kódex alkalmazása*
  - *Adatvédelmi auditon való részvétel*

7. A szükséges adatvédelmi dokumentációk

GDPR által meghatározott, (főképp kifelé is kommunikálandó) nyilvántartások, igazolások létrehozása, fenntartása, aktualizálása

- Adatkezelések nyilvántartása *(csak megfelelő feltételek teljesülésekor kötelező, de egyébként sem tiltott…)*
- Érintettek tájékoztatása a személyes adataik kezeléséről, az ezzel kapcsolatos jogaikról és jogaik gyakorlásának lehetőségeiről
- Incidensek esetén hatóság és érintettek tájékoztatása

- Az adatkezelés megfelelő és szabályozott működését előíró és igazoló dokumentáció *(ami ellenőrzéskor bemutatható a Hatóságnak)*

8. Az adatkezelés rendszere működésének bevezetése

És ha mindez elkészült, akkor

- hivatalosan életbe kell léptetni,
- *a felelősöket a feladataikkal meg kell bízni,*
- *a folyamatokban résztvevőket oktatni kell,*
- *az érintetteket tájékoztatni kell,*
- *a folyamatokat működtetni, ellenőrizni, felügyelni kell.*

… de ez ismerős → IBIR (ISO/IEC 27001)!

Mit csinálunk az ISO/IEC 27001 szerinti IBIR (Információ-biztonsági Irányítási Rendszer) kiépítésekor?

- Felmérjük a folyamatokban kezelt adatköröket;
- Meghatározzuk azok kezelésére vonatkozó (külső és belső) követelményeket;
- Felmérjük azok (jelenlegi) kezelési folyamatait, és az alapján azok információbiztonsági kockázatait
- Kialakítjuk (létrehozzuk / módosítjuk) kockázatarányosan az adatkezelési folyamatok szabályozásait (ha vannak), – megfelelve az adatkezelési külső és belső követelményeknek.
- Létrehozzuk ehhez a szükséges információbiztonsági szervezetet (felelősöket), feladataikat és hatáskörüket szabályozása.
- Bevezetjük az IBIR működéshez szükséges nyilvántartásokat, igazolásokat létrehozása, bevezetjük az IBIR-t …

… de ez ismerős → IBIR (ISO/IEC 27001)!

Mit csinálunk az ISO/IEC 27001 szerinti IBIR (Információ-biztonsági Irányítási Rendszer) kiépítésekor – hogy megfeleljünk a GDPR-nak?

- Az IBIR érvényességi területébe vegyük bele a személyes adatokat;
- Az IB politika tartalmazza a személyes adatok megfelelő kezelését és a GDPR-nak való megfelelést;
- A megfelelési követelmények között jelenjenek meg a GDPR általi elvárások;

… és akkor

- a személyes adatokra vonatkozó hatásvizsgálatok, kockázati felmérések
- az IBIR struktúrájában meghatározott (figyelembe véve az elvárásokat), bevezetett, üzemeltetett, felügyelt és folyamatos karbantartott intézkedések

a követelményeknek – azaz a személyes adatok vonatkozásában – a GDPR jogszabálynak fognak megfelelni;

Kapcsolatok ISO/IEC 27001:2013 esetén

Az ISO/IEC 27001 szerinti Információbiztonsági Irányítási Rendszer (IBIR) célja

- a szervezet által **kezelt adatok / információk** vonatkozásában
- azok **információbiztonsága** (= bizalmassága + sértetlensége + rendelkezésre állása) **elvesztése vagy sérülése következtében**
- **lehetséges károk minimalizálására**,
- a fennálló **kockázatokkal arányos** mértékben
- **védelmi intézkedések** meghatározása és bevezetése,
- majd azok bevonása **a szervezet menedzsmentrendszerébe** (szabályozottan, PDCA-nak megfelelve).

(A személyes adatok is az összes adatok részét képezik.)

A védelmi kontrollok: *a kockázatok alapján a gyakorlatban működtetettek, valamint segítségképpen csekklista a szabvány „A melléklete”.*

Előnyök az IBIR alkalmazásakor!

- **Nemzetközi ‚best practice' alapú egységes menedzsment-rendszer**
- Nemzetközi szabványalapon **tanúsítható**
- **Módszert ad**, az alapján **menedzseli és kézben tartja az információbiztonsági követelményeknek megfelelő teljes működést** – minden tekintetben
- **Egységes rendszerben** (összhang, szinergiák kihasználása, rendszerszemlélet, hatékonyság) **kezeli mindegyik előirányzott adat-kategória** biztonságára vonatkozó követelményeket. (Adatkategóriákra példák: személyes adatok, üzleti titkok, nemzeti minősített adatok, egyéb titok-kategóriák, stb…)

→ Az ilyen, a GDPR-t figyelembe vevő, tanúsított IBIR mindenben meg tud felelni a GDPR követelményeinek, illetve *(az előírások állandó és teljes betartása esetén)* az adatvédelmi auditnak és a hatósági ellenőrzéseknek!

Kapcsolatok ISO 9001:2015 esetén

- **Megfelelés a vonatkozó jogszabályi követelményeknek** *(pl. GDPR is)*
- **Tevékenységek folyamat alapú szabályozása, szabályozott működése**
- **Dokumentált információk** *(adatvagyon)*
  - *ismerete és kezelésük szabályozása*
  - *fenntartása: benne a bizalmasság, sértetlenség, rendelkezésre állás (= információ biztonsága) követelményeivel*
- **Kockázatok felmérése** olyan tényezőkre, amelyek bekövetkezése jelentős kárt jelenthet a szervezetnek *(pl. az információk biztonságának sérülése)*, **és** magas kockázatok esetén azok **kezelésére intézkedések** *(pl. adatbiztonsági intézkedések)* bevezetése
- **Menedzsmentrendszerben** való kezelés, fenntartás, ellenőrzés és fejlesztés (**PDCA**)

Miben segít egy már bevezetett ‚ISO rendszer'?

- 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*

Keretrendszerbe illesztési lehetőségek

ÖNKÉNTESSÉG

ISO 9001 (MIR) rendszeren belül

- *Meglévő folyamatalapúság, menedzsmentrendszer kereteinek használata*
- *Többi szakmai feladatot végig kell csinálni*

ISO 27001 (IBIR) rendszeren belül

- *IBIR érvényességi területbe ‚személyes adatok kezelése' felvétele*
- *IBIR teljes módszertanának alkalmazása – figyelemmel a GDPR elvárások teljesítésére*

‚Magatartási kódex' alkalmazása *(még nincs)*

- Ágazati vagy egyéb jellemző cégcsoportra vonatkozó intézkedés-gyűjtemény, NAIH által elfogadott, külső megfelelési igazolás lehetséges (lesz)
- Kódexben meghatározott intézkedések alkalmazása

‚Adatvédelmi audit'-on való részvétel *(még nincs)*

- Bevezetés saját módszerrel, saját erőből
- Tanúsítható (lesz), NAH és NAIH által akkreditált tanúsító szervezetek által

KÉRDÉSEK?