Deloitte.

Nemzetközi adatvédelmi standard - ISO/IEC 27701

Úton a GDPR tanúsítás felé?

2020. május 21.

Tartalom

Adatvédelem fejlődése

2016. április 27.

GDPR megjelenése

- Rendelet megjelenése
- Szervezetek felkészülése
- Szakmai munkacsoportok kidolgozzák a rendelet gyakorlati alkalmazását

2018. május 25.

GDPR alkalmazása

- 2018. május 25.
- Tagállami szabályozások
- Szervezetek kihívásai és gyakorlati tapasztalatok
- Incidensek kezelése, tudatos adatvédelem
- Bírságolási gyakorlat

2019. augusztus 6.

ISO/IEC 27701

- Részletes adatvédelmi kontrollok kialakítása
- Kontrollok hozzárendelés a GDPR követelményeihez
- Adatvédelmi irányítási keretrendszer a GDPR megfeleléshez

2020-tól

GDPR tanúsítás

- Tanúsítási módszertanok és gyakorlatok kialakítása
- Adatvédelmi hatóságok szakmai közreműködése
- Akkreditáló intézmények
- Tanúsító szervezetek

Mi az ISO/IEC 27701 nemzetközi adatvédelmi standard?

ISO/IEC 27001
Információbiztonsági Menedzsment Rendszer

(IBIR)

⊕

Adatvédelmi kiterjesztés

- Keretrendszer a személyes adatokat kezelő informatikai rendszerek kialakításához, üzemeltetéséhez és folyamatos fejlesztéséhez
- Adatvédelmi iránymutatások az adatkezelők és adatfeldolgozók számára
- Iránymutatások a személyes adatok védelme érdekében

=

ISO/IEC 27701
Adatvédelmi Irányítási Rendszer

(AIR)

Hogyan lehet megszerezni az ISO/IEC 27701 nemzetközi adatvédelmi standard tanúsítványt?

Feltételek:

- ISO/IEC 27001 tanúsítvány
- Kialakított és működő adatvédelmi kontrollok
- Független belső és külső audit

Az időszükséglet függ a szervezet adatkezelési tevékenységeitől, a szervezet méretétől, komplexitásától, informatikai rendszereitől.

ISO/IEC 27701 tanúsítvány

Adatvédelmi irányítási rendszer elemei

A szervezet kontextusa	Vezetés	Tervezés	Támogatás	Működés	Teljesítmény-értékelés	Fejlődés

5 Biztonsági szabályzatok	**6 Információ-biztonság megszervezése**	**7 Emberi erőforrás biztonság**	**8 Vagyonkezelés**
9 Hozzáférés-szabályozás	**10 Titkosítás**	**11 Fizikai és környezeti biztonság**	**Adatkezelők**
12 Üzemeltetés biztonsága	**13 Kommunikáció biztonsága**	**14 Rendszer-fejlesztés, beszerzés, karbantartás**	**Adatfeldolgozók**
15 Beszállítói kapcsolatok	**16 Információ-biztonsági incidenskezelés**	**17 Üzletmenet-folytonosság**	**18 Megfelelőség**

Adatvédelmi Irányítási Rendszer

- szervezet
- szabályzatok
- rendszerek
- folyamatok
- kontrollok
- támogató eszközök

ISO 27001
ISO 27002
ISO 27701

Adatvédelmi irányítási rendszer
Kulcs követelmények

Adatkezelési jogi feltételek

- Adatkezelési nyilvántartás
- Adatkezelési tájékoztatók, jogalapok, hozzájárulások
- Adatalanyi jogosultságok
- Adattovábbítások
- Adatkezelőkkel szemben támasztott követelmények
- Adatfeldolgozókkal szemben támasztott követelmények

Információbiztonsági kontrollok kiterjesztése a személyes adatok kezelésére

- Incidenskezelés
- Adatklasszifikáció
- Adattörlés, anonimizálás, álnevesítés
- Titkosítás
- Hozzáférésmenedzsment
- Naplózás és naplóelemzés
- Adatszivárgások kezelése

Bevezetési megfontolások és kockázatok

Kiknek érdemes?

- Személyes adatokat kezelő és/vagy feldolgozó szervezetek (nagy volumen vagy különleges személyes adatok)
- Retail szegmensben szolgáltató vállalatok (a személyes adatok védelme a fogyasztói döntés alapját képezheti)
- Magas foglalkoztatotti létszám és szenzitív adatok

Miért jó?

- Bizalmat épít az ügyfelekben és munkavállalókban
- Márkaérték növelése
- Vállalatvezetés számára bizonyosságot ad az adatvédelem megfelelőségéről
- Harmadik feleknek demonstrálja a szervezet adatvédelmi felkészültségét

Mik a kockázatok?

- Nem jelent automatikus GDPR megfelelést, incidensek történhetnek
- Bevezetett folyamatok, kontrollok fenntartása szükséges
- Erőforrásigény, költségek érettségtől, komplexitástól függ
- Éves belső és külső auditok által azonosított hiányosságok kezelése szükséges

ISO/IEC 27701 bevezetés és tanúsítás folyamata

1. Eltéréselemzés és akcióterv (1-3 hónap)*

Eltéréselemzés a jelenlegi adatvédelmi irányítási rendszer és az ISO 27701 standard közti eltérések feltárása érdekében és akcióterv készítése a szükséges intézkedésekre.

Azonosított eltérések és szükséges akciók

2. Akcióterv megvalósítása (3-12 hónap)*

Akcióterv megvalósítása az ISO 27701 standardnak való megfelelés érdekében

ISO 27701 standardnak megfelelő működés

3. Belső ellenőrzés (1-3 hónap)*

Az adatvédelmi irányítási rendszer független belső ellenőrzése és a fennmaradt hiányosságok feltárása

Fennmaradó adatvédelmi hiányosságok és javítási terv

4. Tanúsítás (1-3 hónap)

Független külső auditor által végzett tanúsítás

ISO 27701 tanúsítvány

*Az időszükséglet függ a szervezet méretétől, komplexitásától és az adatvédelmi érettségtől.

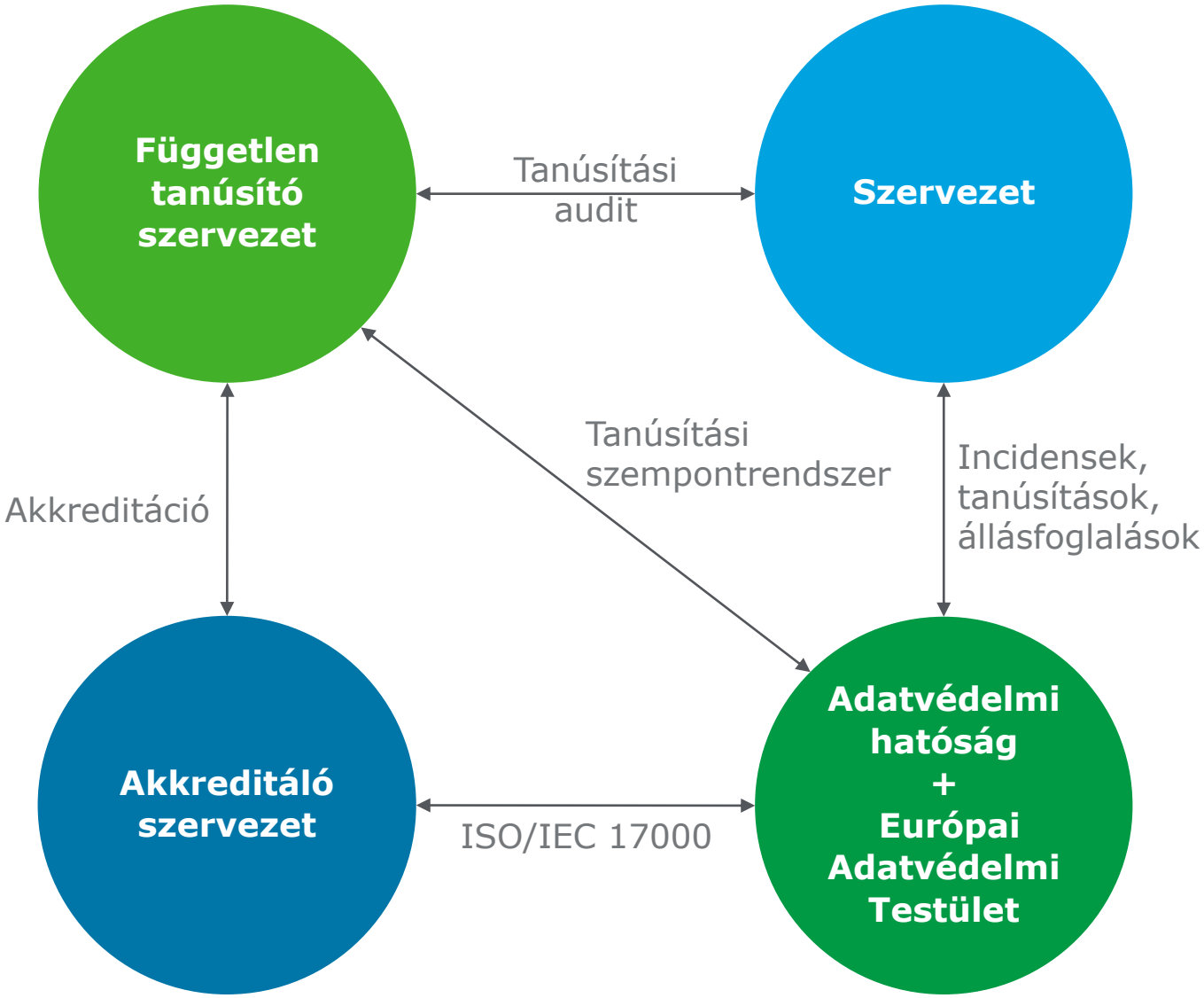
GDPR tanúsítási lehetőségek

Adatvédelmi Irányítási Rendszer tanúsítása (ISO/IEC 27701)

Adatkezelési tevékenységek tanúsítása

A szervezet GDPR megfelelése biztosított

GDPR tanúsítás szereplői



Kapcsolat

Szöllősi Zoltán

Igazgató
Technológiai tanácsadás
zszollosi@deloittece.com
+36209107644

Bánczi Lea

Ügyvéd
Jogi tanácsadás
E-mail: lbanczi@deloittece.com
Telefon: +36202296253

Deloitte.

A Deloitte név egy vagy több Deloitte Touche Tohmatsu Limited („DTTL”) társaságra, a tagvállalatok globális hálózatára és azok kapcsolt vállalkozásaira utal (együttesen: a „Deloitte szervezet”). A DTTL (vagy „Deloitte Global”) és valamennyi tag- és kapcsolt vállalata önálló, egymástól elkülönülő jogi személy, melyek harmadik felek irányába egymás nevében nem vállalnak kötelezettségeket. A DTTL, valamint annak tag- és kapcsolt vállalatai kizárólag saját tetteikért és mulasztásaikért felelnek. A DTTL ügyfelek számára nem nyújt szolgáltatásokat. További információ a deloitte.hu/magunkról webhelyen olvasható.

Magyarországon a szolgáltatásokat a Deloitte Könyvvizsgáló és Tanácsadó Kft. (Deloitte Kft.), a Deloitte Üzletviteli és Vezetési Tanácsadó Zrt. (Deloitte Zrt.) és a Deloitte CRS Kft. nyújtja (melyek közös neve "Deloitte Magyarország"). Mindhárom társaság a Deloitte Central Europe Holdings Limited tagvállalata. A Deloitte Magyarország négy szakmai területen - könyvvizsgálat, tanácsadás, adó- és jogi, valamint kockázati tanácsadási területeken - tölt be kiemelkedő szerepet az országban, és kínál szolgáltatásokat több mint 750 hazai és külföldi szakértője segítségével. (Ügyfeleinknek együttműködő ügyvédi irodánk, a Deloitte Legal Göndöcz és Társai Ügyvédi Iroda nyújtja a jogi tanácsadási szolgáltatásokat.)

A jelen dokumentum és a benne foglalt valamennyi információ a Deloitte Magyarország társaságaitól származik és célja, hogy bizonyos témakör(ök)ben általános információkkal szolgáljon, de nem tárgyalja az adott témakör(öke)t annak teljességében. A jelen dokumentumban megadott információk nem minősülnek számviteli, adóügyi, jogi, befektetési, tanácsadási illetve egyéb szakmai szolgáltatásnak. Ezek az információk nem képezhetik ügyfeleink üzleti döntéseinek kizárólagos alapját. Ügyfeleinket arra kérjük, hogy pénzügyeiket vagy üzletvitelüket befolyásoló bármely döntésük meghozatala, vagy a döntésnek megfelelő magatartás tanúsítása előtt kérjék képzett szakmai tanácsadóink véleményét.

Jelen anyagok és a bennük foglalt információk tájékoztató jellegűek és esetlegesen hibákat is tartalmaznak, amelyekért a Deloitte Magyarország sem kifejezetten, sem hallgatólagosan nem vállal felelősséget, és amelyek nem minősülnek a Deloitte Magyarország állásfoglalásának. Az előzőek érintése nélkül a Deloitte Magyarország nem garantálja az anyagoknak és / vagy a bennük foglalt információknak a hibamentességét, továbbá a teljesítés vagy a minőség valamennyi egyedi kritériumának való megfelelőséget sem. A Deloitte Magyarország cégei nem felelnek a szolgáltatásaik piacképességére, vagy adott célra való alkalmassága, jogtisztasága, versenyképessége, biztonsága és pontossága vonatkozásában.

Ügyfelünk a jelen anyagot és a benne foglalt információkat a saját felelősségére használja, és teljes mértékben felelősséget vállal a jelen dokumentum és a benne foglalt információk használatából eredő következményekért, esetleges veszteségekért. A Deloitte Magyarország cégei nem vonhatók felelősségre jelen dokumentum, vagy a benne foglalt információk felhasználásával kapcsolatosan felmerülő közvetlen, közvetett, járulékos, következményes, büntető jellegű vagy bármilyen egyéb kárért, valamint egyéb veszteségért sem, legyen az szerződéses, jogszabály szerinti vagy magánjogi (például gondatlanságból fakadó).

A fent írtaktól eltérően amennyiben az információk és az anyagok kifejezetten az Ügyfél és a Deloitte Magyarország között létrejött szerződés végleges teljesítéseként kerülnek átadásra, a Deloitte Magyarország felelősséget vállal azért, hogy a szolgáltatásnyújtás és - amennyiben van - az elkészült termék szerződésszerű. A Deloitte Magyarország rögzíti, hogy az anyagok és az információk kizárólag a szerződésben meghatározott személyek / szervezetek számára készülnek és célokra alkalmasak. A Deloitte Magyarország minden felelősséget kizár az Ügyfél által rendelkezésre bocsátott dokumentumokból, anyagokból, információkból és adatokból fakadó vagy azokkal összefüggő károk vonatkozásában. Minden itt nem szabályozott kérdésre a vonatkozó szerződés irányadó.

Ha a fenti rendelkezések bármelyike bármilyen okból nem érvényesíthető, a többi rendelkezés továbbra is hatályban marad és alkalmazandó.