

Deloitte.



GDPR webinar

2017. szeptember 27.

Agenda

Kiket érint elsősorban a felkészülés?

A felkészülés javasolt lépései

Gyakorlati tapasztalatok

Kérdések

Kiket érint elsősorban a felkészülés?

Kiket érint elsősorban a felkészülés?

Minden olyan cégre vonatkozik, ami személyes adatokat kezel, például:

- Munkavállalók adatai
- Természetes személy (magánszemély) ügyfél adatai
- Harmadik személyek adatai (pl. kezes, kedvezményezett, károsult)

Különösen érintett szektorok:

- Pénzügyi (bankok, biztosítók, befektetési szolgáltatók)
- Szolgáltatóipar, vendéglátóipar
- Szolgáltatóközpontok
- Gyógyszeripar
- Hűségprogramokat működtető cégek
- Munkaerőtoborzással foglalkozó cégek
- Média, telekommunikációs és közszolgáltató cégek

Ha cége nem felel meg az előírásoknak, akkor maximum 20.000.000 Euróig vagy a cégcsoport globális éves árbevételének 4%-ig terjedő bírságot szabhat ki a NAIH

A felkészülés javasolt lépései

A felkészülés javasolt lépései

1.

GDPR megfelelést felmérő eltérés-elemzés elkészítése (folyamat, jog és informatikai kontroll szinten)

2.

Akcióterv egyes eltérések kezelésére (kockázati szinthez, optimális erőforrás-kihasználásához igazítva)

3.

Akcióterv implementációja

Néhány magas prioritású feladat

1

Magánszemély ügyfeladataira vonatkozó megkeresés belső folyamatainak és informatika háttérének kialakítása

2

Adatkezelési jogalapok felülvizsgálata és a hozzájáruló nyilatkozatok újra beszerzése

3

Adatkezelési tevékenységek nyilvántartásának elkészítése

4

Adatfeldolgozói és kiszervezési szerződések felülvizsgálata és újratárgyalása

5

Adatvédelmi hatásvizsgálatokkal kapcsolatos módszertan implementálása és a támogató folyamatok, sablonok kialakítása

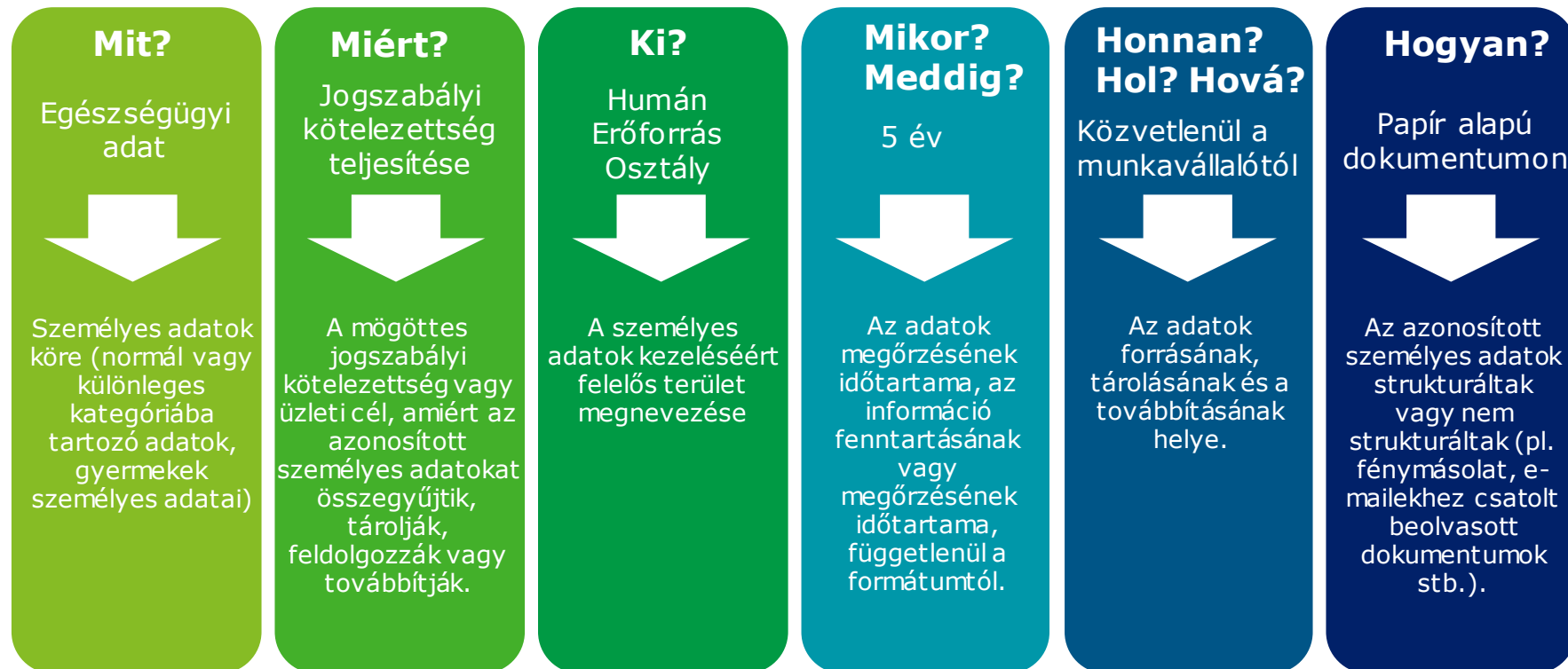
Gyakorlati tapasztalatok

Adatáramlások felmérése – Adattérkép készítése

MIT?, MIÉRT?, KI?, MIKOR?, HOL?, HOGYAN?

Két fő lépés:

- Személyes adat cégen belüli definiálása
- Személyes adatok felmérése



Gyakorlati tapasztalatok

Adatmegőrzési korlátok és gyakorlati érvényesítésük

Nem világos, mikor milyen adatot/adatelemet milyen célból, milyen alapon, mennyi ideig tárolunk/tárolhatunk

- Alapvető üzleti cél, marketing, tudományos kutatás, különleges adatok (nemi, etnikai, vallási, világnézeti, politikai stb.)

Informatikai eszközökkel nincs (megfelelően) támogatva ezek nyilvántartása

- Master Data Management

Adatok informatikai rendszerekben, adathordozókon történő megőrzése illetve az adathordozók megsemmisítése nem kielégítő sem szabályzati, sem gyakorlati szinten

**Jogszályban
előre
meghatározott
vagy egyéb
jogszályi
felhatalmazásból
következő,
valamint egyéni
hozzájáruláson
alapuló megőrzési
idők „egyvelege”**

Milyen megoldásokat célszerű mérlegelni a személyes adatok törlése esetén?

Adathordozó esetén

- Fizikai megsemmisítés
- Olvashatatlaná tétel
- Adatok végleges törlése (felülírás)

Adat esetén

- Üzleti entitás minden adatelemének törlése (pl. teljes tábla-/rekord-struktúra)
- Egyedi rekordok törlése

Deperszonalizáció / anonimizálás

- nem feltétlenül törlés, hanem felismerhetetlenné transzformálás
- Részleges adattörlés, adatmódosítás (átírás), összekeverés, adatkapcsolatok megszüntetése stb.

Privacy-Enhancing Technologies, Secure-by-design és Privacy-by-design a gyakorlatban

Privacy Enhancing Technologies

ICT technológiák, megoldások, melyek növelik a személyes adatok biztonságát.

Privacy-by-Design

Eljárások, módszerek, technikák alkalmazása a folyamatokban és IT rendszerekben az adatok megfelelő biztonságú kezeléséhez.

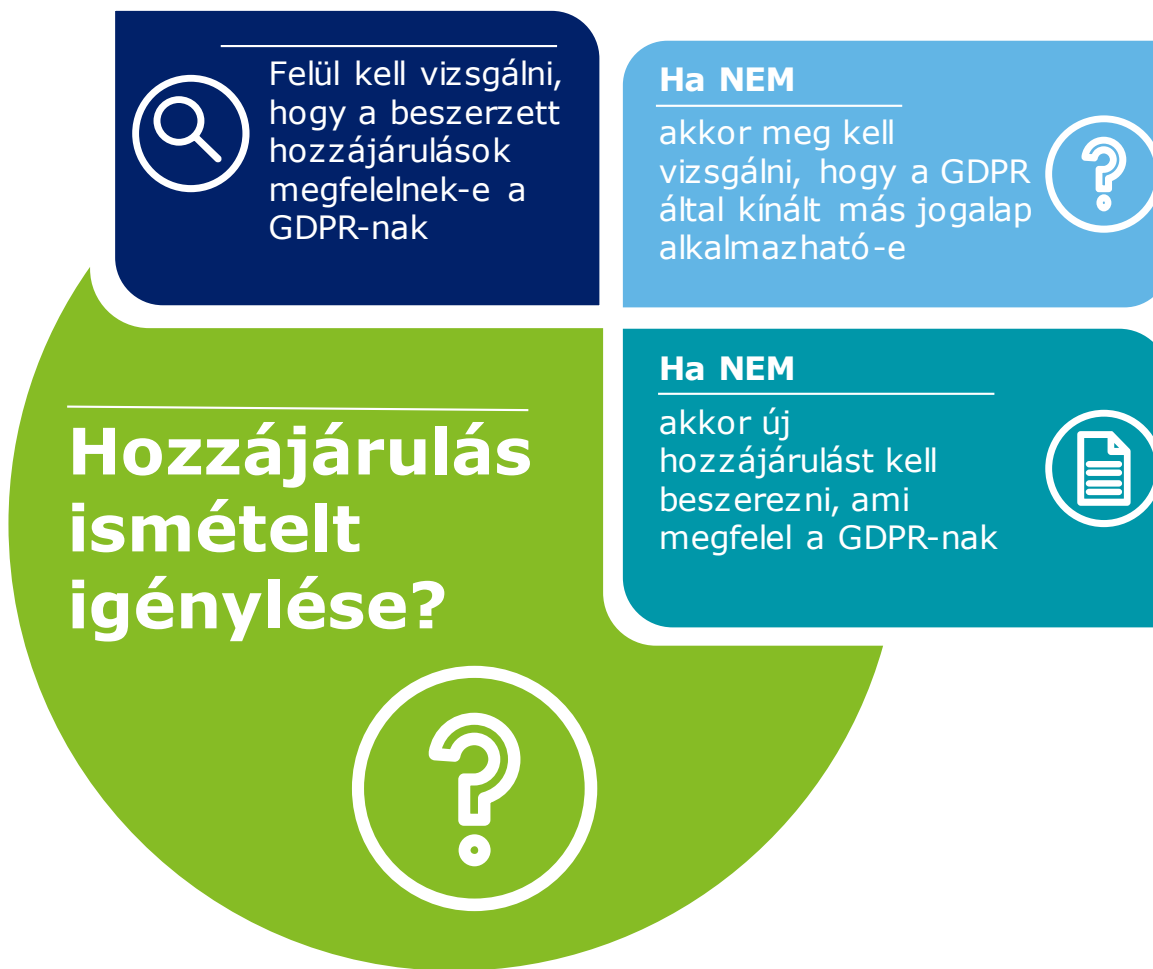
Secure-by-Design

Szoftverek esetén olyan tervezési és fejlesztési gyakorlat, amely biztosítja 3 alapelv érvényesülését: bizalmasság, sérthetetlenség, rendelkezésre állás.

Privacy-by-Default

Nem lehet alapértelmezés az adatkezelésbe való beleegyezés, a természetes személy kifejezett nyilatkozata szükséges.

Tényleg újra kell kérni hozzájárulást az adatkezeléshez?



Ki legyen az adatvédelmi tisztviselő?

Az adatvédelmi tisztviselő lehet szervezeten belüli es külsős tanácsadó is. Ennek megállapításához szükséges, hogy a szervezet ismerje a személyes adatkezeléssel érintett folyamatait.



1 Belső adatvédelmi tisztviselő

választása esetén az adatvédelmi tisztviselőnek szervezetileg közvetlenül a legfelső vezetés alá kell tartoznia.

2 Külsős adatvédelmi tisztviselő

feladatkört betöltő személyként akár ügyvéd, ügyvédi iroda vagy tanácsadó is megbízható.

Ki alkalmas az adatvédelmi tisztviselői feladatok ellátására?

Az adatvédelmi tisztviselő rendelkezzen „rátermettséggel és az adatvédelmi jog és gyakorlat szakértői szintű ismeretével”.

Kérdések

A Deloitte név az Egyesült Királyságban "company limited by guarantee" formában alapított Deloitte Touche Tohmatsu Limited („DTTL”) társaságra, tagvállalatainak hálózatára és kapcsoló vállalkozásaira utal. A DTTL és valamennyi tagvállalata önálló, egymástól elkülönülő jogi személy. A DTTL (vagy „Deloitte Global”) nem nyújt szolgáltatásokat ügyfelek számára. A DTTL és tagvállalatai jogi struktúrájának részletes bemutatását a következő link alatt találja: www.deloitte.hu/magunkrol.

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 500 hazai és külföldi számkértője segítségével. (Ügyfeleinknek egyéttműködő ügyvédi irodánk, a Deloitte Legal Erdős 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, a melyekért 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 megfelelést sem. A Deloitte Magyarország cégei nem felelnek a szolgáltatásaik piacképességére, vagy adott célra való alkalmassága, jogtisztasága, versenyképessége, biztonságára és pontosságára 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 a datokból fakadó vagy azokkal összefüggő károk vonatkozásában. Minden itt nem szabályozott kérdésre vonatkozó szerződés irányadó.

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