ISACA BUDAPEST CHAPTER

MÁSODIK SZERDAI ELŐADÁS

SZÖLLŐSI ZOLTÁN, DELOITTE ZRT

GDPR MEGFELELÉS ELSŐ TAPASZTALATAI

2019.03.13.

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

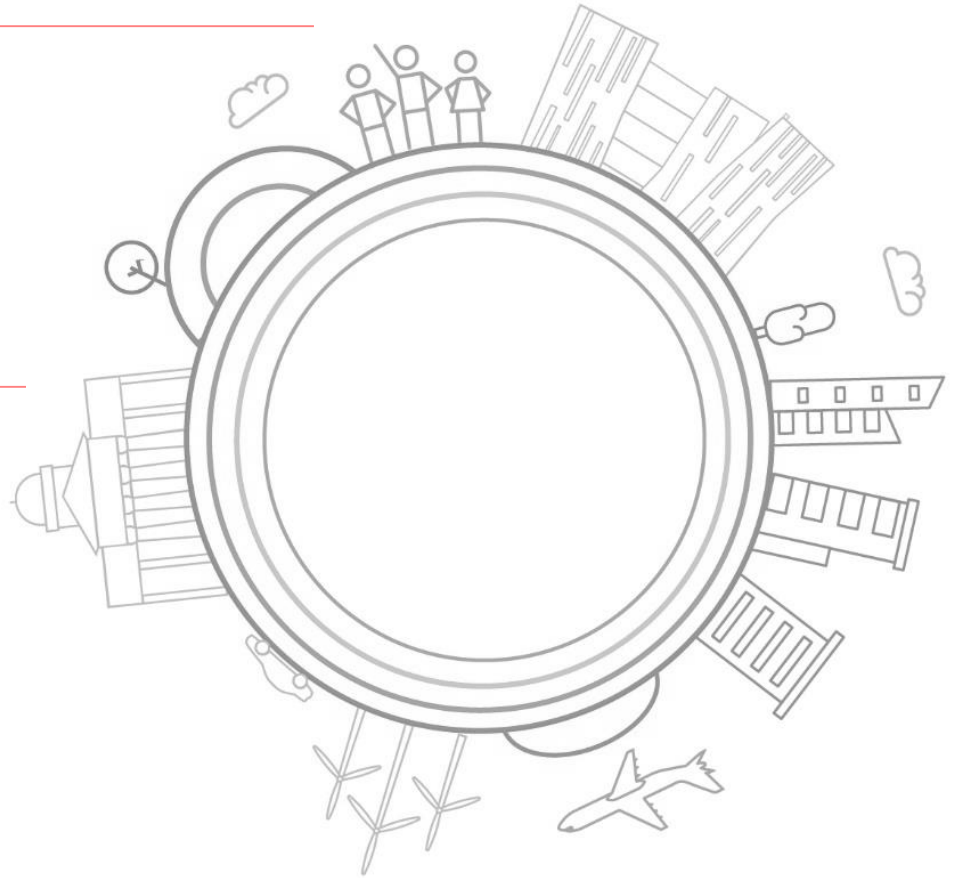
Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

TARTALOM

DELOITTE GDPR GLOBÁLIS FELMÉRÉS

Felmérés résztvevői

11 ország, 2750 kitöltő
(EU-n belül és kívül egyaránt)



Felmérés tárgya

A GDPR hatályba lépésének hatása
a fogyasztói és a vállalati
adatvédelmi hozzáállásra

DELOITTE GDPR GLOBÁLIS FELMÉRÉS EREDMÉNYEI 1/2

Deloitte.

ERŐFORRÁSHIÁNY

- A szervezetek **33%**-a **nem rendelkezik elegendő erőforrással**, hogy teljes mértékben megfeleljen a GDPR elvárásainak.
- A válaszadók **48%**-a **jelentős befektetéseket** hajtott végre az adatvédelmi megfelelés elérése érdekében.
- A válaszadók mindössze **15%**-a gondolja úgy, hogy **sikerült befejeznie a GDPR felkészülési programját**, és minden tekintetben készen áll a GDPR nyújtotta kihívásokra.
- Egyrészt az erőforráshiányból eredően, másrészt a költség minimalizálás érdekében **a GDPR programok** inkább belső megfelelésre és **nem a fogyasztói elégedettségre fókuszáltak.**

A TUDÁS HATALOM

- A megkérdezett fogyasztók **60%**-a **nagyobb figyelmet fordít a személyes adatok biztonságára**, és **50%**-a **hasznot vár cserébe** a személyes adataiért.
- A válaszadó fogyasztók **17%**-a **nem venne igénybe szolgáltatást olyan szolgáltatótól, akiknél adatvédelmi incidensek történnek**. Felértékelődik az adatok etikus használata és fontos szemponttá válik a fogyasztók szolgáltató választása során.

ISACA

DELOITTE GDPR GLOBÁLIS FELMÉRÉS EREDMÉNYEI 2/2

Deloitte.

JELENTŐS FOLYAMATI ÉS TECHNOLÓGIAI BEFEKTETÉSEK

- A válaszadók **70%**-a jelentős **befektetésekről** számolt be a folyamatok átalakítása és a technológiai megoldások alkalmazása terén, annak érdekében, hogy a hosszú távú és hatékony (részben automatizált) GDPR megfelelőség biztosítható legyen.
- A szervezetek **80%-**a **adatszivárgás megelőző rendszer** (DLP) **bevezetését tervezi**, illetve keresik a GDPR megfelelés technológiai támogatásának különböző lehetőségeit.

AZ ADATVÉDELMI ÉRETTSÉG ÉS TUDATOSSÁG JELENTŐSEN NÖVEKEDETT

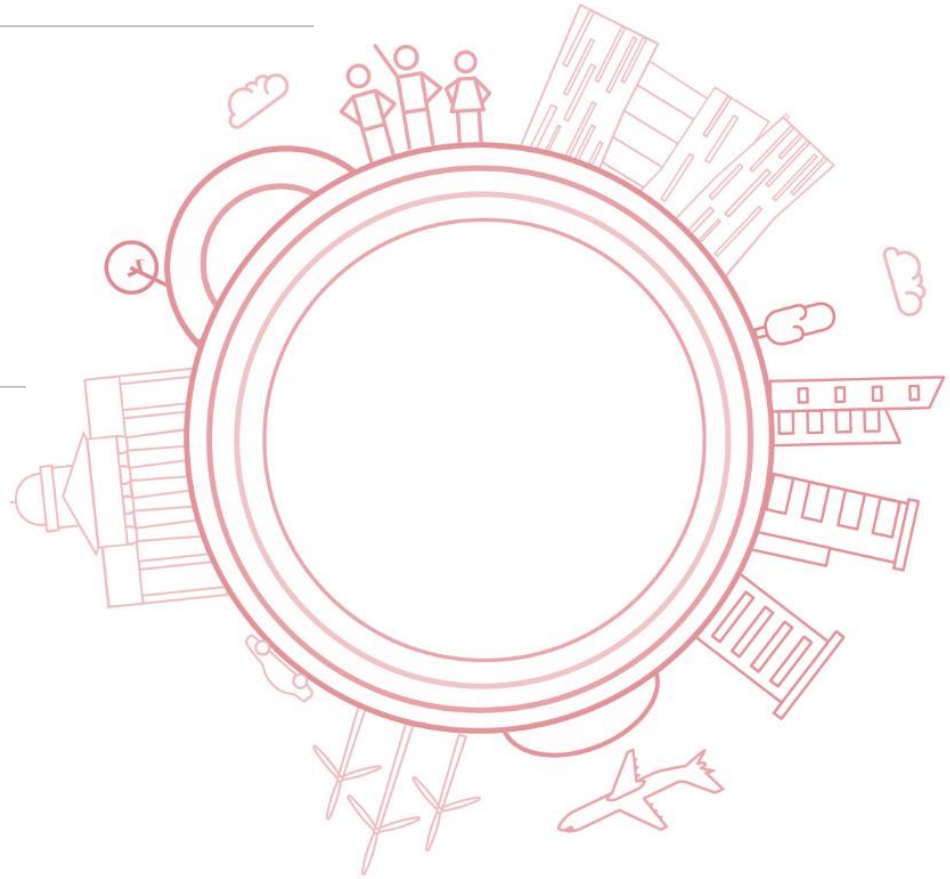
- A válaszadók 59%-a magabiztos abban, hogy középtávon meg tud felelni a GDPR elvárásainak.

ISACA

HATÓSÁGI AKTIVITÁSOK - REGIONÁLIS KITEKINTÉS

Felmérés résztvevői

Közép-európai Deloitte irodák
GDPR szakértői



Felmérés tárgya

A GDPR alkalmazása Közép-Európában (hatósági aktivitások, kihívások, jó gyakorlatok, szektorális kezdeményezések,)

HATÓSÁGI AKTIVITÁSOK - REGIONÁLIS KITEKINTÉS 1/2

Deloitte.

TÁMOGATÁS ÉS POZITÍV HOZZÁÁLLÁS

- A régióban a legtöbb adatvédelmi hatóság ajánlásokkal és konkrét esetek véleményezésével segíti a szervezeteket a GDPR megfelelésben.
- Néhány hatóság tréningeket és kampányokat is tart, fontos hangsúlyt kap az adatvédelmi kultúra és az adatvédelmi felelősség tudatosítása (pl. Lengyelország, Litvánia).
- UK és francia adatvédelmi hatóság aktivitásai jó gyakorlatként szolgálnak, számos jól alkalmazható sablont, eszközt és iránymutatást publikálnak.

A HATÓSÁGI ELLENŐRZÉSEK AZ ADATVÉDELMI BEJELENTÉSEKRE FÓKUSZÁLNAK

- A hatósági ellenőrzések mértéke és mélysége korlátozott, az ellenőri erőforrásokban hiány van.
- Bejelentés alapú vizsgálatok a jellemzőek, átfogó GDPR megfelelőségi vizsgálat csak néhány esetben történt.
- Információbiztonsági szakértők toborzása folyamatos a hatóság oldalán, láthatóan fókuszban vannak a technológiai, e-commerce vállalatok.

ISACA

HATÓSÁGI AKTIVITÁSOK - REGIONÁLIS KITEKINTÉS 2/2

BÍRSÁGOLÁSI GYAKORLAT

- Bírságolási gyakorlat még nem alakult ki, csak kisebb elmarasztalások voltak eddig.
- Nyugat-Európában számos jelentős horderejű adatvédelmi incidens vizsgálata van folyamatban (pl. British Airways, Facebook, Google), amelyek eredménye jelentős hatással lehet a bírságolási gyakorlatra
- November végén megszületett az első német GDPR bírság, amely nem tér el jelentősen az eddigi bírságolási gyakorlattól: kis német közösségimédia-cég -> 20,000 EUR-s büntetés

  330 ezer felhasználó adatai (jelszó, emailcím, stb.) kerültek egy hekkertámadás során illetéktelen kezekbe, a felhasználók adatait titkosítatlanul, szöveges fájlban tárolták

- Súlyos gondatlanság, szándékosság, vagy gyermekek jogainak sérelme esetén várhatóak magasabb bírságok, akár a kkv szektorban is.

MAGYARORSZÁGI HATÓSÁGI STATISZTIKÁK

2018. május 26 - július 25	**840 adatvédelmi megkeresés** érkezett a NAIH-hoz, melynek a fele konzultációs típusú volt.
2018. július 26 - október 31	**802 adatvédelmi megkeresés** érkezett a hatósághoz, ezeknek már mindössze 17 %-a volt konzultáció, a fennmaradó **83% adatvédelmi incidenshez kapcsolódott**

TIPIKUS ADATVÉDELMI HIÁNYOSSÁGOK ÉS KOCKÁZATOK 1/2

Deloitte.

Szabályzati szintű megfelelés	Hozzájárulások használata és kezelése	Adatkezelési nyilvántartás	Adatalanyi jogosultságok
A hazai vállalatok a **GDPR megfelelést** leginkább **szabályzati szinten** valósították meg, a **folyamatokban és rendszerekben korlátozottan** kerültek a változások átvezetésre a GDPR hatályba lépéséig. A GDPR projektek implementációs szakaszát a legtöbb vállalatnál még nem fejezték be.	A GDPR hatályba lépése előtti **hozzájárulások használata**, szükségtelen hozzájárulások bekérése, **„cookie policy”**. Vizibilis támadási felület, konkurencia által is felfedezhető.	**Hiányos, pontatlan**, nem követi a szervezet valódi adatkezelési tevékenységeit, nincs karbantartva. **Hatósági ellenőrzés**eknél kiinduló pontként szolgál.	A fogyasztói megkeresések kezelése nem hatékony, **nincs kialakított folyamat / sablon,** nem kerül mérésre.

ISACA

TIPIKUS ADATVÉDELMI HIÁNYOSSÁGOK ÉS KOCKÁZATOK 2/2

Deloitte.

Információbiztonsági eszközök	Adatvédelmi hatásvizsgálat	Anonimizáció	Adatvédelmi incidenskezelés
Komplex informatikai környezetekben történik a személyes adatkezelés, de nincsenek automatizált megoldások, kontrollok kialakítva, az adatvédelmi incidensek és kockázatok mérséklésére, pl.: • **adat-klasszifikáció** • **adatszivárgás megelőzés** • **jogosultság-kezelés** • **naplóelemzés**	Nem kerültek definiálásra a **magas kockázatú adatkezelési tevékenységek** Nincs adatvédelmi hatásvizsgálati módszertan, sablon Adatvédelmi **hatásvizsgálatok hiányos végrehajtása**, amely könnyen ellenőrizhető a hatóság által	**Deperszonalizáció hiánya** a tesztadatbázisban Az éles adatbázis jogalap nélkül tárolt személyes adatokat tartalmaz **Anonimizációs stratégia és gyakorlat hiánya**	Nincs kialakított folyamat, felelősség-feladat mátrix, intézkedési terv **72 órás incidens bejelentési kötelezettség** betartása kihívást jelent

ISACA

JÖVŐKÉP

Deloitte.

1. **Személyes adatok piaci értéke növekszik**, a fogyasztók hasznot várnak el a személyes adatok megadásáért és használatáért.

2. **Ügyfélbizalom fontos elemévé** válik az **adatvédelem** és a **személyes adatok etikus használata**. Pozitív adatvédelmi megítélés és hírnév versenyelőnnyel jár a piacon. Az adatvédelmi incidensek reputációra gyakorolt negatív hatása könnyen meghaladhatja a bírság egyszeri pénzügyi veszteségét.

3. Súlyos gondatlanság, szándékosság, vagy különleges személyes adatok jogainak sérelme valószínűsíthetően **jelentős bírságokat** fog maga után vonni.

4. **Technológiai támogatás és információbiztonsági eszközök nélkül** hosszú távon nem megvalósítható a komplex IT környezetekben a **GDPR által elvárt szintű adatvédelem.**

5. **E-privacy rendelet** hatályba lépése tovább **erősíti az adatvédelmi elvárásokat és tudatosságot.**

ISACA

KAPCSOLAT

Szöllősi Zoltán
Szenior Menedzser, Deloitte Zrt.

Tel: +3620 910 7644
zszollosi@deloittece.com

Köszönöm a figyelmet!

Deloitte.

A Deloitte név az Egyesült Királyságban “company limited by guarantee” formában alapított Deloitte Touche Tohmatsu Limited („DTTL”) társaságra, tagvállalatainak hálózatára és kapcsolt 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 szakértője segítségével. (Ügyfeleinknek együttműködő 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, 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.