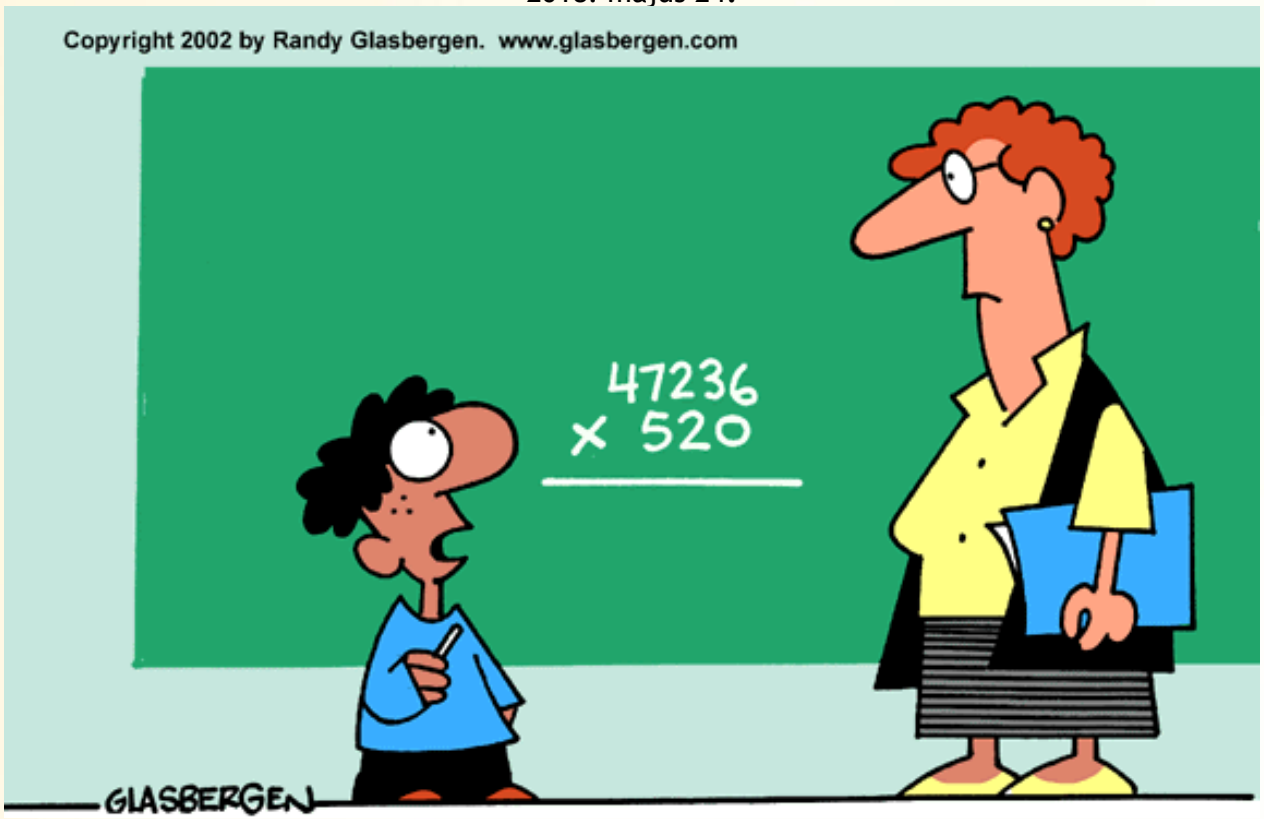
Tolna Megyei Kereskedelmi és Iparkamara

GDPR informatikai feladatok

azaz, amikor a jogászok levonulnak

Tőzsér Zoltán (CISA, CSM, MCP)

2018. május 24.



Mielőtt elkezdenénk, szeretném pontosan tudni hogyan fogják kezelni a személyes adataimat.

TMSI Kft.

- Alakult: 1997 jan. 1.
- Ernst & Young együttműködés 1996-2002
- CISA, CISM, CSM, CNE, MCP,…
- Adatvédelmi audit 2007 óta (Lombard lízing Zrt., Országos Tisztifőorvosi Hivatal (OTH), Volksbank Zrt., …)
- GDPR referenciák (DMRV Zrt, Országos Fordító és Fordításhitelesítő Iroda Zrt.(OFFI), ELTE Origó Nyelvi Centrum Kft, Minerva-Soft Kft., Colas Hungária Zrt.,…)
- in nuce GDPR felkészítő csomag: **2017 november**
- GDPR tanulmány (2018 március)

Fontos korlátozás

- A TMSI Kft. nagy figyelmet fordít a jogszabályoknak való megfelelésre, de cégünk egy informatikai biztonsági tanácsadó cég és nem jogi iroda.
- Az előadásunkban elhangzó és látható bármely információ, észrevétel, megjegyzés vagy vélemény elsősorban informatikai, technikai, esetleg szabályozási jellegű és az üzleti folyamatok javítását célozza. Ugyanakkor ezek semmilyen formában nem minősülnek sem adótanácsadásnak, sem számviteli-, sem jogi tanácsnak vagy véleménynek! Ilyenekre a TMSI Kft. nem hitelesített és nem is jogosult.
- Az előadásunkban található adatokat a legjobb tudásunk szerint megbízható forrásokból szereztük, de csak tájékoztató információként kezelendőek.
- Az előadásunkra való hivatkozás nem lehet alap egy esetleges hatósági, ellenőrzési, törvényességi eljárásban. A jogszabály és az ezzel kialakulóban lévő szemlélet viszonylagos újszerűsége, az ellenőrzések és a jogértelemzés kiforrása miatt egy esetleges későbbi ellenőrzés megállapításait sem lehet előrejelezni.
- Az előadásunk kizárólag gondolatébresztőként szolgálhat az Önök szervezete számára, hogy a megfelelő, erre illetékes, képzett és jogosult szakemberekkel az Önök konkrét helyzetét, eseteit, kérdéseit, tisztázzák. Jogszerű döntéseket csak ilyen konzultációk után lehet hozni.

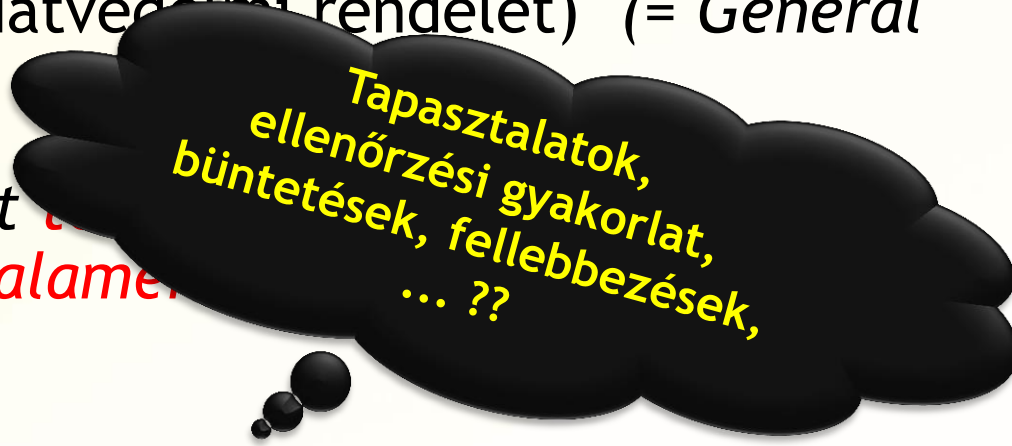
Miről beszélünk?

- *Mi?* • Mi a GDPR?
- *Kit?* • Kit érint?
- *Miért?* • Mik a kockázatok?
- *Mit?* • Mik [illegible]sok?
- [illegible] Hogyan feleljünk meg a követelményeknek?

Informatikai megközelítés/szemlélet!

Mi a GDPR?

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, … (általános adatvédelmi rendelet) *(= General Data Protection Regulation)*



- EU rendelet = *„Ez a rendelet [illegible] közvetlenül alkalmazandó valamel[illegible]*
- Határidők:
  - *„Ez a rendelet az Európai Unió Hivatalos Lapjában való kihirdetését követő huszadik napon lép hatályba.”* (= 2016. április 27. + 20 nap)
  - *„Ezt a rendeletet 2018. május 25-től kell alkalmazni.”*
- Hazai előzmény: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról („Infotörvény”)

Infotörvény módosítás

- A Kormány 2017. aug. 25-én közzétette az Igazságügyi Minisztérium előterjesztését az Infotv. GDPR-el összefüggő módosításával kapcsolatosan (*Infotv_jogharm_modositas_eloterjesztes_170825.pdf*).
- Jogharmonizáció = dereguláció
- Néhány észrevétel:
  - A Javaslat nem egyértelműsíti a papír alapú személyes adatok kezelését.
  - A "kötelező adatkezelés" mint jogalap beleerőltetése a törvénymódosításba? A GDPR-ban található jogalapok között ilyen nem található, a hivatkozott 6. cikk (1) bekezdés c) és e) pontjai nem ilyenek.
  - Rendezi a fordítási hibát a Rendelet 37. cikk (7) vonatkozásában.
  - Olyan többletkötelezettségeket ír elő a GDPR rendelethez képest, amely az eredetiben nem szerepel, azaz a külföldi adatkezelőket nem fogja terhelni. (például az általános.

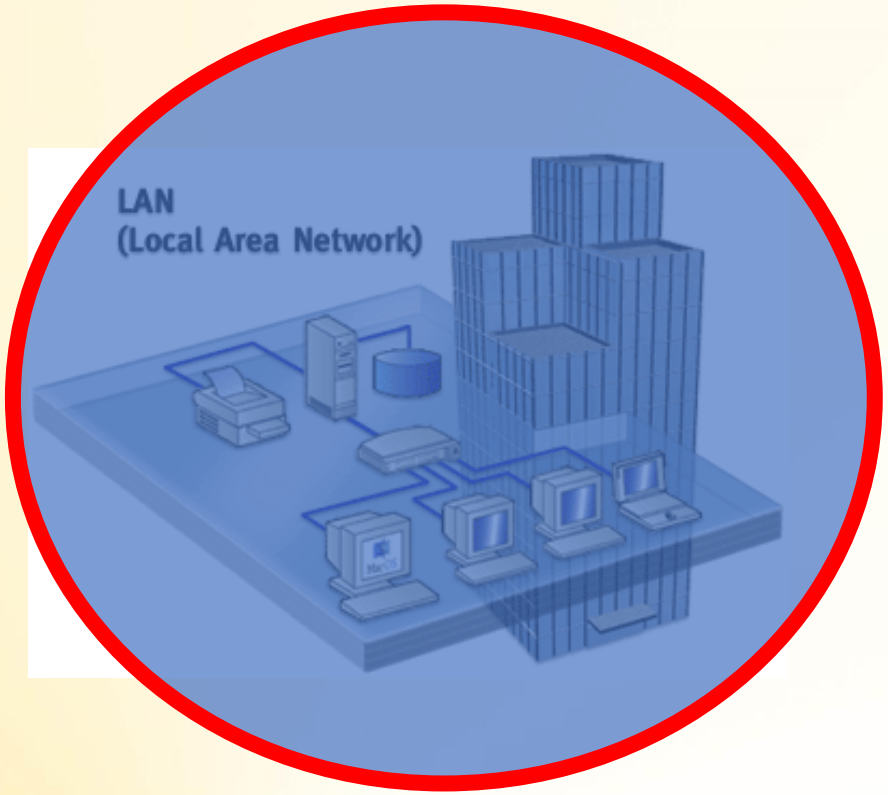
„A hatósági ellenőrzést végző szervek a kis- és középvállalkozásokkal szemben az első esetben előforduló jogsértés esetén – az adó- és vámhatósági eljárást és a felnőttképzési tevékenységet folytató intézmények ellenőrzésére irányuló eljárást kivéve – bírság kiszabása helyett figyelmeztetést alkalmaznak."

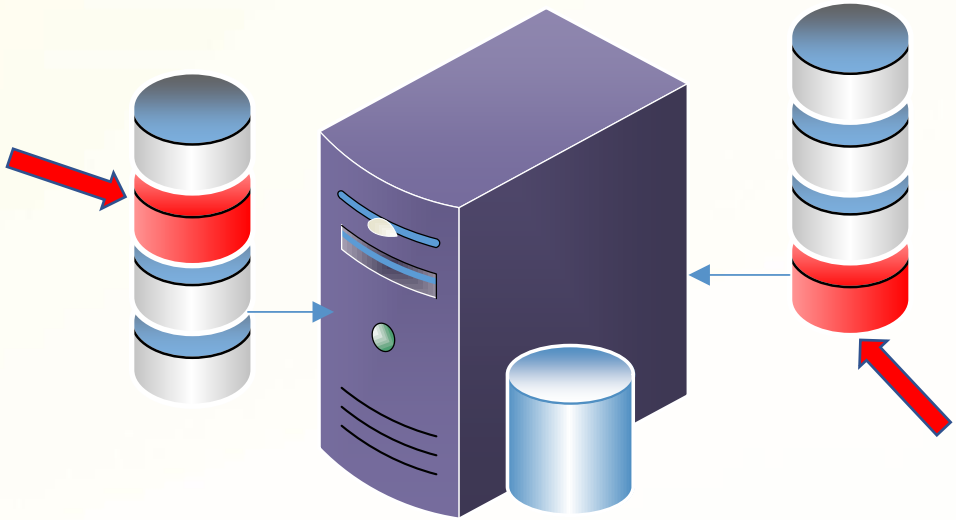
Néhány GDPR-előny

- EU-szintű, egységes adatvédelem
- Jobb adatok = jobb marketing
- Adatbázisok karcsúsítása (az adatok 85%-a redundáns, elavult vagy triviális)
- A hazai multik és nagyvállalatok elindították a beszállítóik érdeklődését
- A zsarolóvírusok gyártói elkezdtek erre specializálódni (magasabb váltságdíj)
- Az adatvédelem megszervezése olcsóbb lehet
- Erősödik a bizalom (pl. online üzleteknél)
- Csökken a kockázat

A GDPR megfelelés versenyelőny lesz!

Műszaki előny





Veszélyforrások 2018

- A legnagyobb IT biztonsági veszélyforrások 2018-ban*:
  - Crime-as-a-service
  - IoT
  - Management elvárások
  - Beszállítói lánc kockázata
  - Szabályozások (GDPR)

** Information Security Forum (ISF)*

A személyes adatok kezelése

Veszélyes üzem!

Felügyeletet ellátó szervek

„Bizottság”

Európai Bizottság

Bizottság

*„93. Cikk: **Bizottsági eljárásrend***
(1) A Bizottság munkáját egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet szerinti bizottság.”

Európai Adatvédelmi Testület

Felügyeleti hatóságok együttműködése

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

Kit érint?

- 2. cikk (1) *„E rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.”*

- 3. cikk (1) *„E rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem.”*
- (2) *„E rendeletet kell alkalmazni **az Unióban tartózkodó érintettek** személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:*
  - *a) áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy*
  - *b) az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve hogy az Unió területén belül tanúsított viselkedésükről van szó.”*

Nekem mi közöm ehhez?

- „Lemásolhatjuk a személyi igazolványát”?
  - Banki ügyintéző
  - Biztosító
  - Autókereskedő
  - Bevásárlóközpont (áruhitel)
- Mobilszolgáltatók (GPS koordináták, besz
- Mobiltelefonok
  - GPS adatgyűjtés+továbbítás,
  - Metaadatok
  - Kamerák, mikrofonok használata
  - Applikációk adatgyűjtése, címlist
- Bankkártya adatok (fizetések k vakoriság, átlagtól eltérő költés,…)
- „Okos” TV kamera (Samsung)
- Szerződtem (pl. lízing), de már e
- Előfizetői (újság, TV, online, …) t obadása
- IP címek (pl. Internetes böngészési szo k elemzése, követése), cookie-k, stb.
- „Zártláncú” kamerák (munkahelyi, bev sárlóközpont, utcai,…)
- Facebook (Zuckerberg-idézet), Google, Skype, . . .

Ha valami ingyenes ott **MI** vagyunk az áru (pl. az adataink)!

A kockázatok

- Presztízsveszteség
- A felügyeleti hatóság … utasításának be nem tartása … legfeljebb 20 000 000 EUR összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeggel sújtható; a kettő közül a magasabb összeget kell kiszabni.

A kockázatok

- NAIH/2016/3398/10/H., OTP Bank Nyrt., 1.000 000-Ft,
  - *„… jogalap hiányában ne kezelje a Panaszos személyes adatait;*
  - *törölje a Panaszos azon adatait, amelyek kezelésére nincs jogalapja, továbbá azokat, amelyek nem szükségesek az adatkezeléshez.”*

- NAIH/2018/412/2/H., Auchan Magyarország Kft., 15.000.000,-Ft
  - „megfelelő jogalap hiányában kezelt személyes adatokat a kamerás megfigyeléssel összefüggésben;
  - „nem nyújtott megfelelő előzetes tájékoztatást az adatkezelésről és annak körülményeiről”
  - „nem tett eleget megfelelően a panaszos felé tájékoztatásadási kötelezettségének.”

- NAIH/2017/1961/18/H., OMV Hungária Ásványolaj Kft., 18.000.000,-Ft
  - „ a fizető vendégek hangját rögzítő mikrofonok”
  - „töltőállomásokon kiépített elektronikus megfigyelőrendszer”

- NAIH/2018/356/3/H., BKK Budapesti Közlekedési Központ Zrt., 10.000.000,-Ft

A legfontosabb elvárások

•A jelenlegi Infotörvény elvei

- A tisztességes adatkezelés elve *(Infotv. 4. § (1) bekezdés)*
- A célhoz kötöttség elve *(Infotv. 4. § (1) bekezdés)*
- Az adatminimalizálás elve *(Infotv. 4. § (2) bekezdés)*
- Az adatminőség elve *(Infotv. 4. § (4) bekezdés)*
- A személyes adatot törölni kell, ha az adatkezelés célja megszűnt *(Infotv. 17.§ (2) bekezdés)*
- Az érintett jogainak érvényesítése *(Infotv. 5-6., 14-21. §)*
- Az adatbiztonság *(Infotv. 7. §)*
- Adattovábbítás külföldre *(Infotv. 8. §)*

•GDPR adatkezelési elvek (5. cikk)

- jogszerűség, tisztességes eljárás és átláthatóság
- célhoz kötöttség
- adattakarékosság
- pontosság
- korlátozott tárolhatóság
- integritás és bizalmas jelleg
- elszámoltathatóság

A legfontosabb elvárások

•Beépített és alapértelmezett adatvédelem („Privacy by design”)	•Alapértelmezett biztonság	•Adat elszámoltathatóság	•Személyes jogok tiszteletben tartása	•Az adatvédelmi incidens bejelentése
• *„Megfelelő technikai és szervezési védelmi intézkedéseket”* kell végrehajtani (eredendő, állandó és felügyelt védelem a személyes adatok megsemmisítése, elvesztése, terjesztése, változtatása vagy a hozzáférése ellen) • Az adatvédelmi tisztviselő kinevezésének mérlegelése • Megfelelő biztonsági szint biztosítása a kockázatnak megfelelően, és a védelmi eszközöket megfontolása (titkosítások, álnevesítés, ...) • Az adatátvitel minimalizálása és szerződéses biztosítása	• A gyűjtött és tárolt személyes adatok minimalizálása • A tárolás időbeni korlátozása • Az adatkezelő és az érintettek érdekeinek egyensúlya	• Minden személyes adatfeldolgozás azonosítása, dokumentálása és igazolása, akár külső partner igénybevétele esetén is • Adatfeldolgozás csak meghatározott, egyértelmű és törvényes üzleti célra és címzett részére • Kifejezett beleegyezés kérése (vagyis önkéntes "opt-in" az "opt-out" helyett)	• Az érintettek jogainak tiszteletben tartása: • tájékoztatáshoz • hozzáféréshez • javításhoz • kifogásoláshoz • **elfeledtetéshez** • átadáshoz	• Az adatvédelmi incidensek kezelését beilleszteni az információbiztonsági események és incidenskezelés folyamatába • Biztosítani a világos és egyértelmű kommunikációs folyamatokat az adatvédelmi hatóságokkal és az érdekelt felekkel

Személyes adatok

- ***„személyes adat”***: *azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;*

Együtt. Veled

Súgó English

Online Tudakozó

Főoldal

KERESÉS EREDMÉNYE

Keresési feltételek: név szerinti, teljes egyezőségre, minden előfizetőre, **név:** orbán viktor

Összesen: 9 találat 1-9

§ Orbán Viktor	**Cím**: Zomba 7173, Alkotmány utca **Telefon**: (74) 407-894
§ Orbán Viktor	**Cím**: Budaörs 2040, Dráva köz **Telefon**: (30) 309-5787
§ Orbán Viktor	**Cím**: Csorvás 5920, József Attila utca **Telefon**: (30) 501-4008
§ Orbán Viktor	**Cím**: Magyarkeszi 7098, József Attila utca **Telefon**: (20) 324-9130
§ Orbán Viktor	**Cím**: Szekszárd 7100, Benedek Apát utca **Telefon**: (30) 670-6202
§ Orbán Viktor	**Cím**: Gyulakeszi 8286, Balaton utca **Telefon**: (30) 316-4561
§ Orbán Viktor	**Cím**: Garabonc 8747, Garabonc **Telefon**: (30) 462-2256
§ Orbán Viktor	**Cím**: Nagykanizsa 8800, Zemplén Győző utca **Telefon**: (30) 240-5872
§ Orbán Viktor További albejegyzések eléréséhez kattintson az előfizetőre	**Cím**: Szentgotthárd 9970, Árpád utca **Telefon**: (30) 565-7555

Összesen: 9 találat 1-9

KAPCSOLÓDÓ LINKEK

- Ügyintézés
- Szolgáltatási területek
- Tudakozó szolgáltatások
- Telefonkönyv

Mi m

- V
- K
- V
- A
- B
- R

sége.

IN NUCE

Példa (1)

Statisztikai célból érdekel a születési dátumok és a postai irányítószámok összekapcsolása az eladott termékekkel. (pl. egy adott korcsoportban az emberek egy bizonyos földrajzi régióban miből mennyit vásárolnak).

Megkérem Juditot, aki teljes hozzáféréssel rendelkezik a rendszerekhez, hogy gyűjtse ki nekem ezeket az adatokat.

Judit, miközben elkészíti a kivonatot, kezel személyes adatokat?

A. Igen. Annak ellenére, hogy csak bizonyos adatokra van szükség, mivel minden ügyféladathoz teljes hozzáféréssel rendelkezik össze tudja kötni az adatokat a személlyel, ha akarja.

B. Nem. Nem kezel személyes adatokat, mert figyelmen kívül hagy minden információt, csak születési dátumokat, postai irányítószámokat és termékadatokat kér le.

Példa (2)

Judit elküldi nekem a kért adatokat (születési dátumok, postai irányítószámok, eladott termékek).

Ezek személyes adatnak minősülnek?

A. Nem, mert nem tudom összekapcsolni a születési dátumokat és a postai irányítószámokat egy természetes személlyel.

B. Igen, mert az információ egy olyan alkalmazásból származott, amely lehetővé teszi az információ természetes személyhez való kapcsolódását.

C. Esetleg, ha lehetőségem van arra, hogy ezeket az információkat egy magánszemélyhez kössem. Például, ha megadhatom ezeket az információkat olyan alkalmazásban, amely összekapcsolja a kapott adatokat számlaszámokkal, ügyfélszámokkal.

A személyes adatok kategóriái

Általános
(például)

- név
- születési dátum
- postacím
- családi állapot
- helymeghatározó adat (GPS, mobilcella, stb.)
- online azonosító (pl. IP cím, e-mail cím, stb.)
- rögzített telefonbeszélgetés
- utazási adatok
- autóbérlési adatok
- munkaszerződés
- oklevél
- utalási adatok
- hobbi
- video- vagy fényképfelvétel
- ...

Különleges
(például)

- faji vagy etnikai származás
- politikai vélemény
- vallási vagy világnézeti meggyőződés
- szakszervezeti tagság
- genetikai és biometrikus adatok
- az egészségügyi adatok
- szexuális életre vagy szexuális irányultságára vonatkozó személyes adatok
- ...

„A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó **személyes adatok kezelése tilos.**”

9. cikk: A személyes adatok különleges kategóriáinak kezelése

„A … személyes adatok kezelése tilos.”

(2) Az (1) bekezdés **nem alkalmazandó** abban az esetben, ha:

a) az érintett **kifejezett hozzájárulását adta** az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez,…;

b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó **jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges**, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;

c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;

d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet **megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik**, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;

e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket **az érintett kifejezetten nyilvánosságra hozott**;

f) az adatkezelés **jogi igények előterjesztéséhez**, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;

g) az adatkezelés **jelentős közérdek** miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

h) az adatkezelés **megelőző egészségügyi vagy munkahelyi egészségügyi célokból**, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a (3) bekezdésben említett feltételekre és garanciákra figyelemmel;

i) az adatkezelés **a népegészségügy területét érintő olyan közérdekből szükséges**, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;

j) az adatkezelés a 89. cikk (1) bekezdésével összhangban a **közérdekű archiválás** céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan uniós vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

- Az adatkezelés jogszerűsége (6. cikk)

IGAZOLNI!

Adatkezelési célonként!

Lejárat?

Pontos hivatkozást!

Érdekmérlegelés!

Hozzájárulás

„**az érintett hozzájárulását adta** személyes adatainak egy vagy több konkrét célból történő kezeléséhez”

Szerződés teljesítése

„az adatkezelés olyan szerződés teljesítéséhez szükséges, **amelyben az érintett az egyik fél**, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges”

gi kötelezettség

adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges”

Létfontosságú érdek

„az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges”

Közérdek

„az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges”

Jogos érdek

az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek”

Adatkezelő – adatfeldolgozó (4. cikk)

Adatkezelő

az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, **amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza**; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja

28. cikk

Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő **kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak** az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, **megfelelő technikai és szervezési intézkedések végrehajtására**

Adatfeldolgozó

az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel

Példa (3)

From: Krisztián <.Krisztian@ .hu>
Sent: Friday, May 18, 2018 10:33 AM
To: Tozser Zoltan <zoltan.tozser@tmsi.hu>
Cc: Marias Zoltan <zoltan.marias@tmsi.hu>;
Subject: GDPR - Adatfeldolgozói szerződés kiegészítés

From: Tozser Zoltan <zoltan.tozser@tmsi.hu>
Sent: Friday, May 18, 2018 1:25 PM
To: Krisztián <.Krisztian@ .hu>
Cc: Marias Zoltan <zoltan.marias@tmsi.hu>;
Subject: RE: GDPR - Adatfeldolgozói szerződés kiegészítés

From: Krisztián <Krisztian@ .hu>
Sent: Friday, May 18, 2018 1:48 PM
To: Tozser Zoltan <zoltan.tozser@tmsi.hu>
Cc: Marias Zoltan <zoltan.marias@tmsi.hu>;
Subject: RE: GDPR - Adatfeldolgozói szerződés kiegészítés

Kedves Zoltán,

Köszönjük a választ, továbbítottam a jogi osztályunk felé, visszajelzésüket megerősítésnek vették és kérjük a szerződés tervezetet vegyék tárgytalannak.

Üdvözlettel:
Krisztián

Krisztián
IT manager

Adatvédelmi tisztviselő

- Jelenlegi infotörvény: „belső adatvédelmi felelős”
- GDPR: 37. cikk *„(1) Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:*
  - *a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;*
  - *b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik* ***szükségessé****;*
  - *c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.”*
- Kötelező (például): polgármesteri hivatalok, kórházak/klinikák, profilalkotás (bank, biztosító,…), hűségprogramok (vásárlói kártyák), GPS+mobilapp/gépkocsi, „okos” eszközök, online reklámok, közlekedési vállalatok, …
- Egyéb esetben: ajánlott, csak ne ezen a néven.
- Bárki lehet, de összeférhetetlen a: CIO, CISO, CEO, …
- Kiszervezhető, szolgáltatási szerződés keretében

Adatvédelmi hatásvizsgálat

- *35. cikk: „(1) Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő **az adatkezelést megelőzően** hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.”*

- *35. cikk: „(7) A hatásvizsgálat kiterjed legalább:*
  - *a) a tervezett adatkezelési **műveletek módszeres leírására** és **az adatkezelés céljainak ismertetésére**, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;*
  - *b) az adatkezelés céljaira figyelemmel az adatkezelési **műveletek szükségességi és arányossági vizsgálatára**;*
  - *c) az (1) bekezdésben említett, az érintett jogait és szabadságait érintő **kockázatok vizsgálatára**; és*
  - *d) **a kockázatok kezelését célzó intézkedések bemutatására**, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.”*

32. cikk: Az adatkezelés biztonsága

Az adatkezelő és az adatfeldolgozó a **tudomány és technológia állása** és **a megvalósítás költségei**, továbbá **az adatkezelés jellege**, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, **változó valószínűségű és súlyosságú kockázat** figyelembevételével **megfelelő technikai és szervezési intézkedések**et hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja

Álnevesítés
(pszeudonimizálás)
Anonimizálás

A személyes adatok álnevesítése és **titkosítás**a

Név	Álnevesített (Pszeudonimizált)	Anonimizált
Kovács János	qUerDD	XXXXX
László Péter	hjh77GT	XXXXX
Kovács János	qUerDD	XXXXX
Kiss Anna	AL14gT	XXXXX
Nagy Miklós	MMofQL34nn	XXXXX
Kovács János	qUerDD	XXXXX
Rejtő Jenő	P. Howard	XXXXX
Gárdonyi Géza	Göre Gábor	XXXXX
Marie-Henri Beyle	Stendhal	XXXXX

„Harmadik ország”

A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása

45. cikk (1) „Személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására akkor kerülhet sor, ha a Bizottság megállapította, hogy **a harmadik ország**, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet **megfelelő védelmi szintet biztosít**. Az ilyen adattovábbításhoz nem szükséges külön engedély.”

15. cikk (2): „Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, **az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan** a 46. cikk szerinti megfelelő garanciákról.”

28. cikk (3): „….A szerződés vagy más jogi aktus különösen előírja, hogy az **adatfeldolgozó** … **a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli** – **beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is** –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;”

30. cikk (1): (Az adatkezelési tevékenységek nyilvántartása) „… E nyilvántartás a következő információkat tartalmazza:… olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, **ideértve a harmadik országbeli címzetteket** vagy nemzetközi szervezeteket; … **adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk**, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti **továbbítás esetében a megfelelő garanciák leírása;**

• Céges postafiók – magán levelezés

- e-mail cím = személyes adat, GDPR hatálya alá esik
- az adatkezelésről (e-mail cím) a munkáltatónak előzetesen részletes tájékoztatást kell adni, illetve a munkavállaló kérésére külön is tájékoztatni kell az adatkezelésről, továbbá a munkavállaló tiltakozhat az adat kezelésével szemben vagy kérheti azok törlését.

- Nem minősül személyes adatnak a céges email-fiókoknak az a része, ami céges célú levelezés. Ha a munkavállaló a céges e-mail címét személyes magánlevelezésre használja, akkor az ilyen levelei személyes adatnak és magántitoknak minősülnek, és főszabály szerint nem ellenőrizhetők a munkáltató által.

- Ha a munkavállaló a céges email-címmel magánlevelezést folytat, akkor a munkáltató a magánlevelek és címzettjei email-címének is adatkezelője lesz, mivel a saját szerverén történik a levelezés, és biztonsági mentés is készül róla. Ezért erre külön céges szabályzatot kell kidolgozni, ami rögzíti a tárolás, megőrzés szabályait, időtartamát, a törlés szabályait, időpontját, a magánlevelezésre vonatkozó szabályokat és az esetleges munkáltatói ellenőrzés szabályait.
(https://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf)

Az adatvédelmi incidens

- 33. cikk: *„Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.”*

- *Mi számít incidensnek?*
  - *EU rendelet: 4. cikk „12. adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;”*
  - *Infotörvény: 3. § „26. adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.”*

Az adatvédelmi incidens bejelentése

- *Mit kell jelenteni?*
  - *EU rendelet: 33. cikk (3): „Az (1) bekezdésben említett bejelentésben legalább:*
    - *a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;*
    - *b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;*
    - *c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;*
    - *d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.”*

Az adatvédelmi incidens bejelentése

- Ki jelentse?
- Kinek? (az érintetteknek is, ha: „…*az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.”)*
- Hogyan?
- Következmények?

GDPR megfelelési projekt

- Vezetői elkötelezettség
- Adatvédelmi tisztviselő kijelölése és támogatása
- Adatgazdák kijelölése és tréningje
- Tréningek
- Tudatosítás
- Incidenskezelés
- NAIH kapcsolat

- IB politika
- IB stratégia
- IB szabályzat
- Adatkezelési szabályzat
- Egyéb szabályzatok
  - munkautasítások
  - eljárási rendek
  - forgatókönyvek

- SW/HW leltár
- Adatvédelmi hatásvizsgálat (DIA)
- Felhő kezelése
- Zártláncú kamerák
- Közösségi média, böngészési szokások
- Jogosultságkezelés
- SIEM
- SOC
- Jelszókezelés
- Szegmentálás

- DLP
- Titkosítás
- MDM
- Application control
- Web control
- Végpontvédelem
  - vírusvédelem
  - spamszűrés

IN NUCE

Dióhéjban a GDPR: EU általános adatvédelmi rendeletére való felkészülési folyamatát segítő anyagok összesége.

www.tmsi.hu/in-nuce · (+361) 321-0631 · innuce@tmsi.hu

Miért nem jogi kérdés?

- A szervezetek nem tudják hol kezelnek/tárolnak személyes adatokat!
  - Adatleltár, data mapping, adatklasszifikáció/osztályozás, adatáramlási folyamatok, …
- A „hozzájárulás” elektronikus megadásának problémái! Ki adta meg, hogyan igazoljuk ezt, stb.
- Hogyan és hol tároljuk ezeket (pl. felhő, replikálás az anyacéghez, stb.)?
- Hogy lehet ezeket megszüntetni/anonimizálni?
- DLP? BCR? DIA? BCP/DR? SIEM? SOC? …
- Informatikai kockázatelemzés és kockázatkezelés?
- Informatikai incidenskezelés?
- Titkosítás fogalma, szintjei
- Aktuális … alkalmazást kockázatok és te
- K…ség az informatikai (biztonsági) mentése
- Adatok módosítása/törlése a különböző adatbá
- Álnevesítés technikai lehetőségei, opciói, szint
- A szervezetek nem tudnak (főleg nem időben) …
- …

Az „elfeledtetéshez való jog” (VALÓDI törlés) a gyakorlatban

„Észrevételek”

- „Mé[redacted] van.”
- „[redacted]mélyes ad[redacted]

Nincs !

Pl: e-mail-ben? HR/munkaszerződés? IP címek? Cookie-k?
Zártláncú kamerák? Beléptető rendszer?...

Hol vannak személyes adatok?
Hogyan és hol tároljuk ezeket (pl. felhő, replikálás az anyacéghez, stb.)?
Hogy lehet ezeket megszüntetni/anonimizálni?
DLP? BCR? DIA? BCP/DR? SIEM? SOC? ...
Informatikai kockázatelemzés és kockázatkezelés?
Informatikai incidenskezelés?
Adatklasszifikáció?
Titkosítás fogalma, szintjei, módjai?
Aktuális és valós adathalászat kockázatok és technikák?
Különbség az informatikai (biztonsági) mentések és az archiválás között?
Adatok módosítása/törlése a különböző adatbázisokban? Ezek hatása a többi rendszerre?
Álnevesítés technikai lehetőségei, opciói, szintjei?
Az „elfeledtetéshez való jog” (VALÓDI törlés) a gyakorlatban?
...

[redacted] · inhuce@tmsi.hu

• A GDPR IT biztonsággal kapcsolatos előírásai (példák)

Elvek

Adattakarékosság
Pontosság
Korlátozott tárolhatóság
Integritás és bizalmas jelleg
Elszámoltathatóság

Az adatkezelés jogszerűsége

Az érintett hozzájárulását adta személyes adatainak kezeléséhez

A hozzáférés

Rendelkezésre bocsátandó információk
Helyesbítés és törlés
Az elfeledtetéshez való jog
Az adatkezelés korlátozásához való jog
Az adathordozhatósághoz való jog („széles körben használt, géppel olvasható formátumban”)

Az adatkezelő feladatai

„Az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, **változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedések**et hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik.”

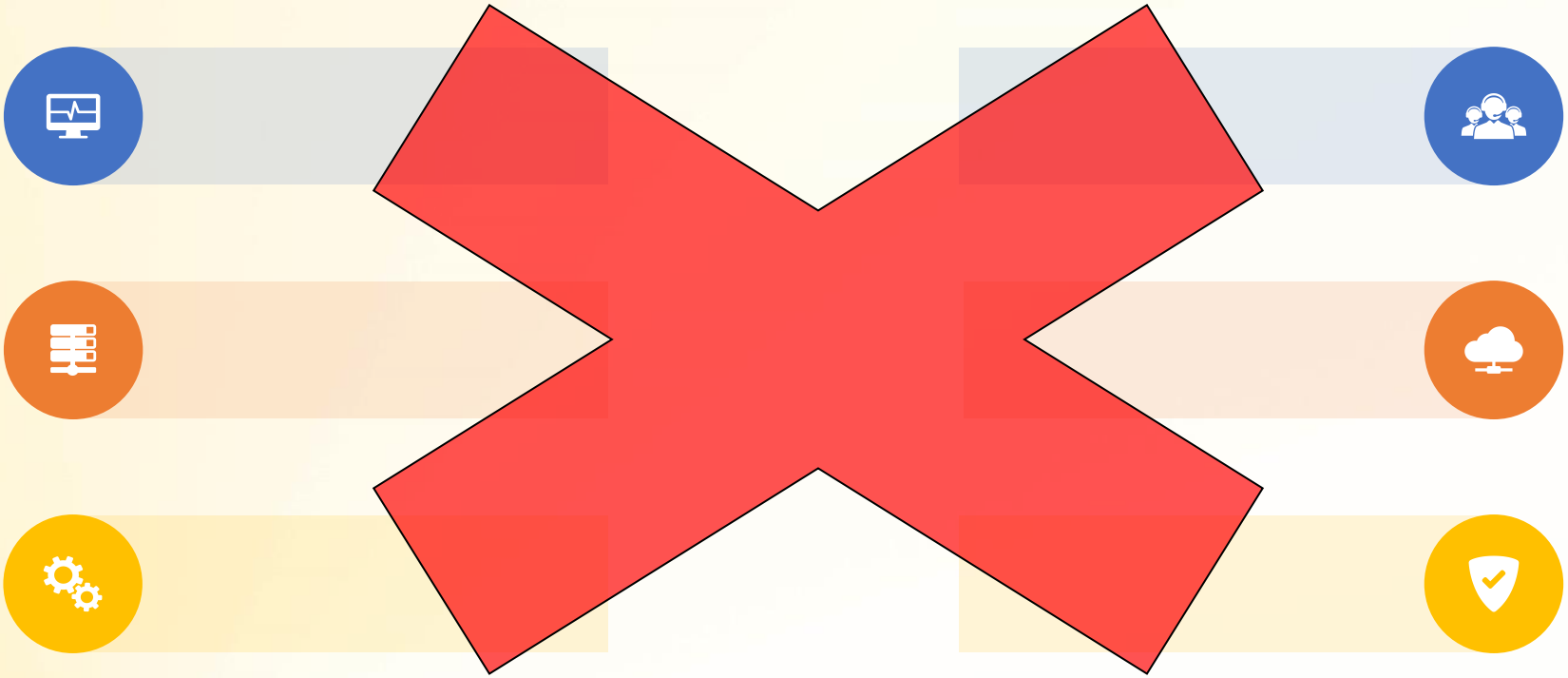
Az adatkezelési tevékenységek nyilvántartása

Minden adatkezelő … a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet.

Adatvédelmi hatásvizsgálat

Ha az adatkezelés valamely típusa, **valószínűsíthetően magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő **az adatkezelést megelőzően hatásvizsgálatot végez** arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

- A GDPR megoldása informatikai eszközzel?



Miért érdemes ezzel foglalkozni?

- Az adatszivárgások 60%-a a beszállítóknál, alvállalkozóknál fordul elő.
- A nagyobb cégek már listázzák a beszállítóikat
  - Megfelelnek ők a GDPR-nek?
  - Lesz nekem belőlük kockázatom?
  - Tudok helyettük megbízhatóbbat, kockázatmentesebbet választani?
  - …

MIÉRT van erre szükség?

- EU rendelet
- Infotörvény
- Elle
- EU-s
- Proj
- …

Saját,
jól felfogott
ÉRDEK!

Gondolkodjunk másként!

- TISZTELJÜK az ügyfelet
- Kezeljük óvatosabban a személyes adatait: ekkor már nem lesz teher
- **Versenyelőny:** ha valakiről tudom hogy tisztességesen, átláthatóan, jogkövetően kezeli a személyes adataimat, világosan és érdemben kommunikál…

10 lépésben a megfelelésig

1. Vezetői elkötelezettség
2. Mennyiben érint bennünket a GDPR?
3. Adatvédelmi tisztviselő kijelölés
4. Mi a jelenlegi helyzetünk ... ettségi fok”)
5. GDPR me... ...lemzése („Gap analysis”)
6. Ad... ...tklasszifikáció, adatfolyamatok)
7. **...ések, hiányosságok pótlása**
   - ...ingek
   - ...s-management tesztelése (bejelentés is)
8. Monitorozás, audit, folyamatos fejlesztés

Minden lépést, eredményt igazolni! („elszámoltathatóság”)

Mi a kötelező?

„Igazolásköteles” technikai vagy szervezeti lépések (**nem minden cikk vonatkozik mindenkire**):

- 5. cikk: a személyes adatok kezelésére vonatkozó elvek (adatkezelési/adatvédelmi/adatminőségi politika és szabályzat, stb.)
- 6. cikk: az adatkezelés jogszerűségének igazolása
- 7., 8. cikk: a hozzájárulások igazolása, különös tekintettel a gyermekek adatainak kezelésére
- 9. cikk: a személyes adatok különleges kategóriáinak kezelése
- 10. cikk: a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése
- 12. cikk: átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések
- 13., 14., 15. cikk: rendelkezésre bocsátandó információk (az érintettek tájékoztatása és a személyes adatokhoz való hozzáférés, eljárások, szabályok, tréningek)
- 16., 17., 18., 19., 20. cikk: helyesbítés és törlés (a helyesbítéshez való jog, „az elfeledtetéshez való jog”, az adatkezelés korlátozásához való jog, értesítési kötelezettség, az adathordozhatósághoz való jog)
- 21. cikk: a tiltakozáshoz való jog gyakorlata
- 22. cikk: automatizált döntéshozatal egyedi ügyekben (profilalkotási gyakorlat, kivételek kezelése)
- 24. cikk: „megfelelő technikai és szervezési intézkedések” végrehajtása, „annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik”

Mi a kötelező (2)?

- 25. cikk: beépített és alapértelmezett adatvédelem igazolása
- 26. cikk: közös adatkezelők
- 27. cikk: úniós képviselő kijelölése
- 28., 29. cikk: harmadik fél kockázatainak kezelése (garanciák kérése és ellenőrzése az alvállalkozóknál, beszállítóknál, szolgáltatóknál)
- 30. cikk: az adatkezelési tevékenységek nyilvántartása (az adatkezelés célja, az érintettek kategóriái, a személyes adatok kategóriái, olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk,…)
- 32. cikk: az adatkezelés biztonsága (álnevesítés, titkosítás, integritás/rendelkezésre állás/elérhetőség igazolása, incidenskezelés: BCP/DRP, rendszeres tesztelés/felmérés/értékelés)
- 33. cikk: az adatvédelmi incidens bejelentése a felügyeleti hatóságnak
- 34. cikk: az érintett tájékoztatása az adatvédelmi incidensről
- 35., 36. cikk: adatvédelmi hatásvizsgálat és előzetes konzultáció
- 37. cikk: adatvédelmi tisztviselő kijelölése
- 38. cikk: az adatvédelmi tisztviselő jogállása
- 39. cikk: az adatvédelmi tisztviselő feladatai
- 45., 46., 48., 49. cikk: adattovábbítás
- 47. cikk: kötelező erejű vállalati szabályok (BCR)
- 89. cikk: a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból folytatott adatkezelésre vonatkozó garanciák és eltérések
- 91. cikk: egyházak és vallási szervezetek létező adatvédelmi szabályai

A többi cikk?

- Független felügyeleti hatóságok
- Illetékesség, feladatok és hatáskörök
- Együttműködés és egységesség
- Európai adatvédelmi testület
- Jogorvoslat, felelősség és szankciók
- …

Stratégia?

Megfelelés vagy védhető állapot kialakítása

GDPR iránti elkötelezettség bemutatása, igazolása

Apró lépések fontossága: biztonságos nyomtatás, „tiszta asztal irányelv” érvénybe léptetése, …

Szabályozási környezet

IT biztonsági intézkedések tervezése, végrehajtása és ezek igazolása
Jogosultságkezelés felülvizsgálata („roles and responsibilities”, „need to know”, admin jogosultságok kontrollja, stb.)
Logelemzés
SIEM

Folyamatos figyelemfelhívás
Folyamatos tréning

Hosszú távú cselekvési terv

Felkészülési stratégia?

- Minden szervezet má
- Mindenki tart valahol
  - használjuk a meglévő
- Más az
  - érintettség,
  - méret,
  - tevékenységi kör,
  - előzmények,
  - érettségi szint,
  - …

Más a kiinduló állapot és más a cél =

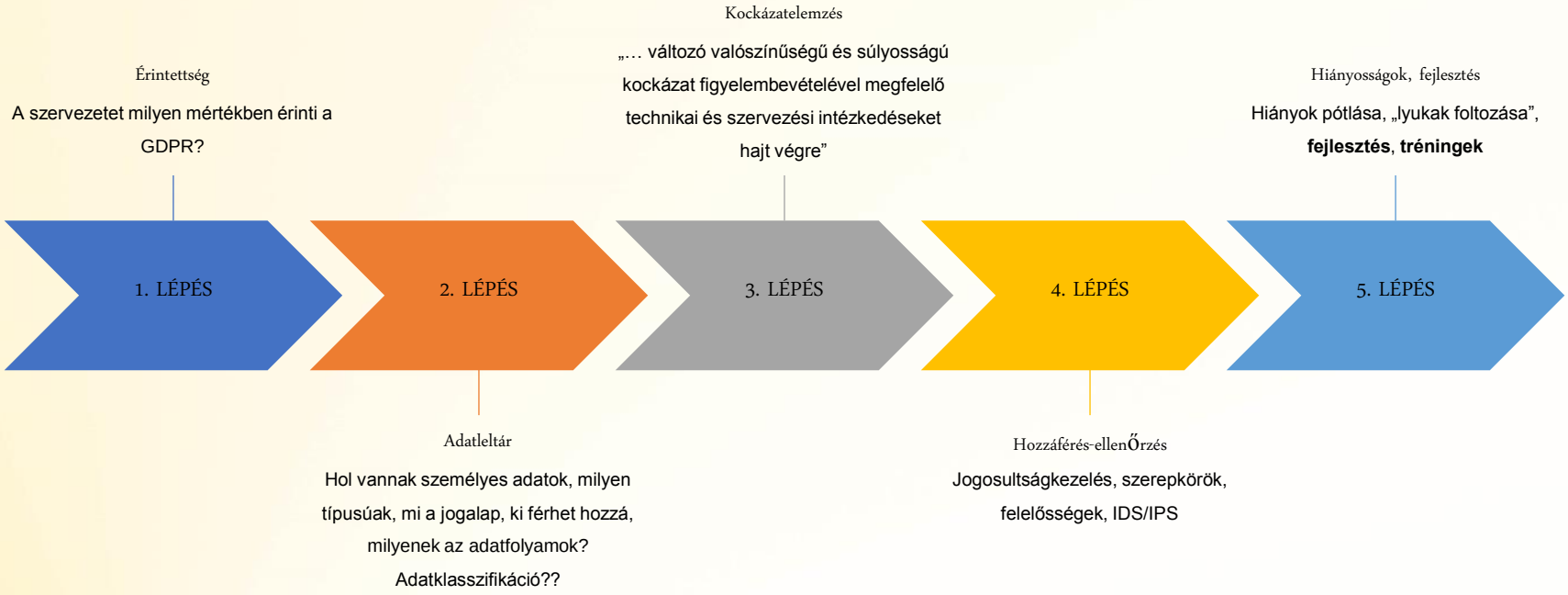
Nem lehet általános receptet/checklistet/szoftvert/… adni

Hogyan kezdjük?

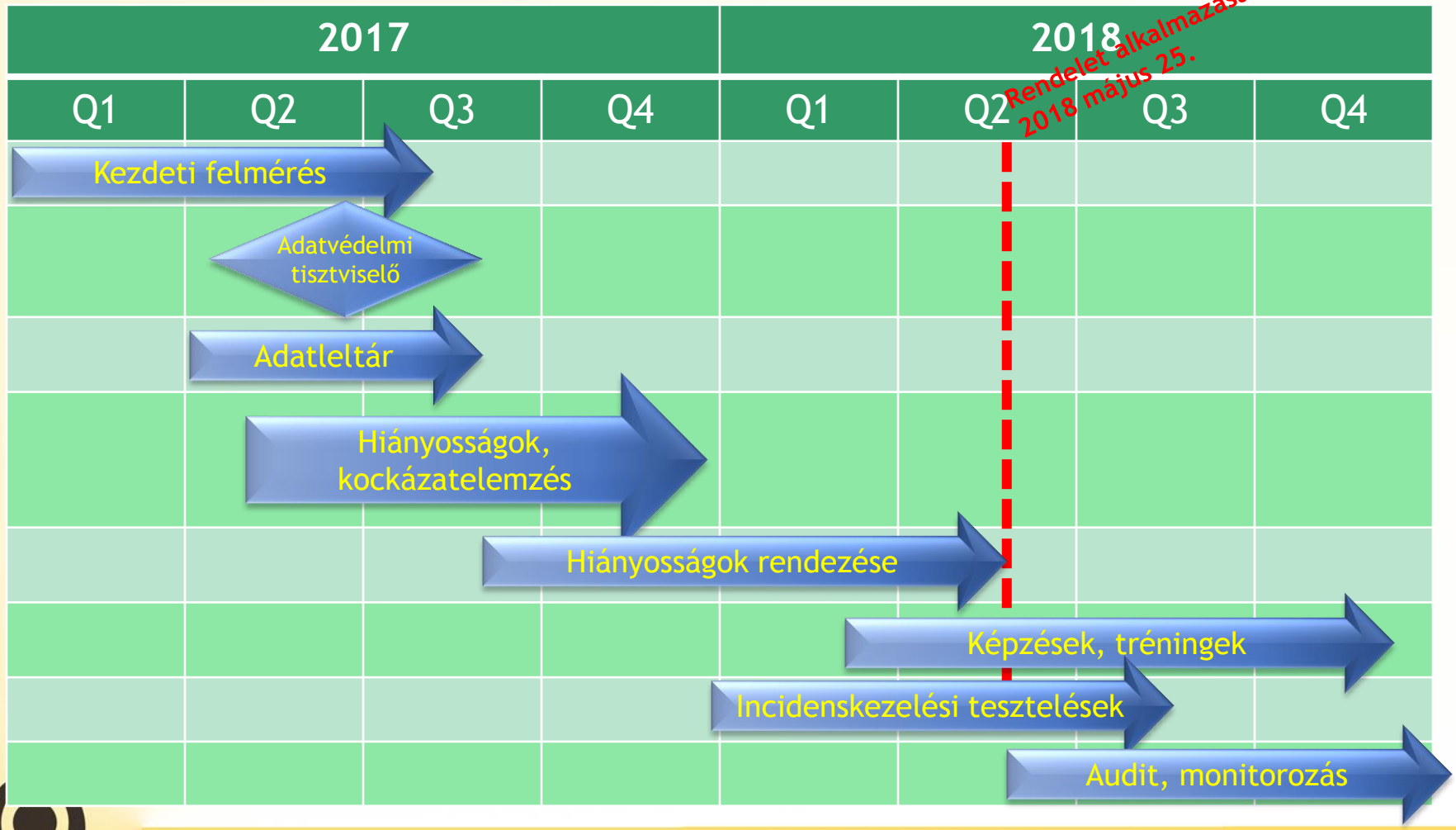
- A GDPR rendelet elvei
  - Jogszerűség, tisztességes eljárás és átláthatóság; célhoz kötöttség; adattakarékosság; pontosság; korlátozott tárolhatóság; integritás és bizalmas jelleg; elszámoltathatóság.
- Az adatkezelési üzleti folyamatokat kell átgondolni
  - „Valóban szükségünk van ezekre a személyes adatokra?”
- NE ☑ alapú egyszeri munka legyen, hanem a szervezet működési folyamatainak szerves része állandóan, hosszú távon

NE a NAIH-nak és a Rendeletnek próbáljunk megfelelni,
próbáljunk értéket/versenyelőnyt teremteni

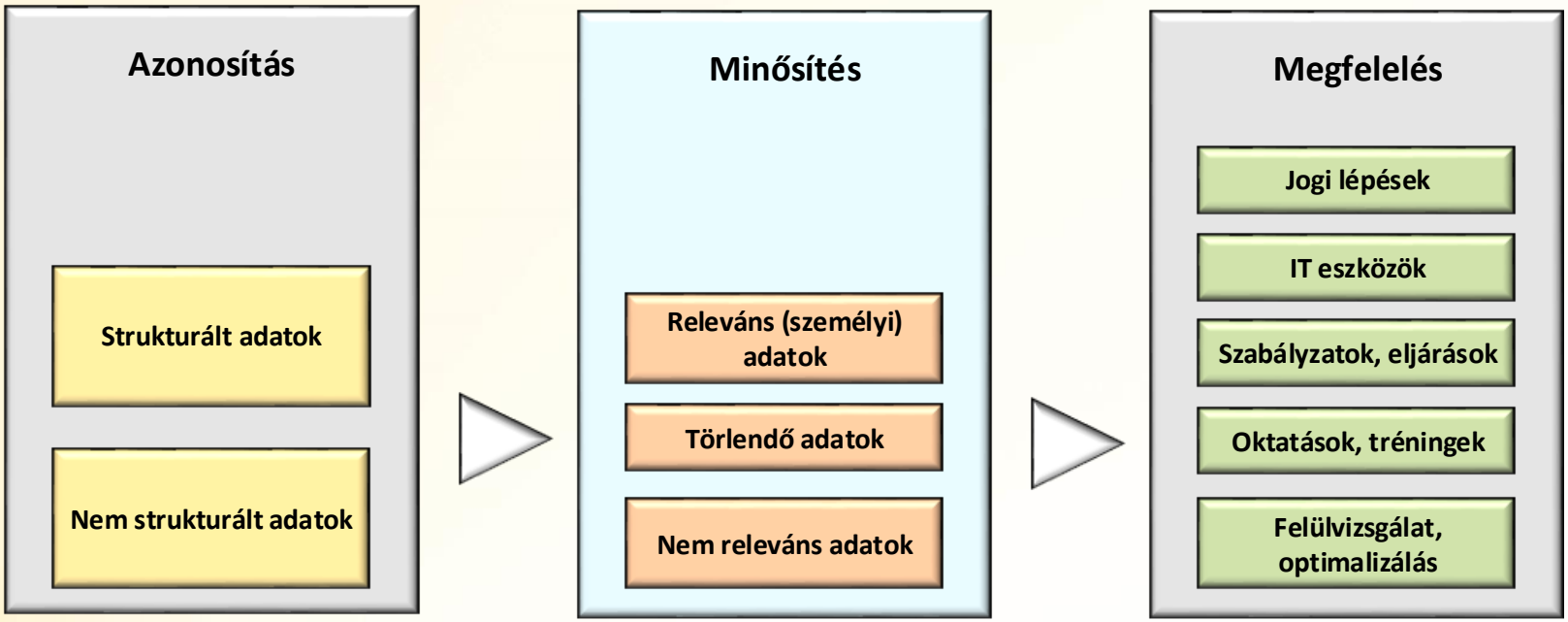
- Első lépések



Megvalósítási ütemezés



Folyamat az adatok szempontjából



A kezdeti munkák

Helyzetfelmérés: GDPR rendelet hatása a szervezetre; a cég kitettségének elemzése; érettségi szint becslése; az érintett üzleti folyamatok azonosítása, megértése; felelősök, technológiák és eszközök elemzése; jelenlegi adatkezelési gyakorlat rövid áttekintése, elemzése (elfogadott szabályok vs. karbantartott/alkalmazott gyakorlatok); kiszervezett tevékenységekkel kapcsolatos szerződéses kapcsolatrendszer felülvizsgálata.

Meglévő IT technológiák áttekintése (pl. titkosítás, BCP/DR tervek, DLP megoldások, stb.); a vonatkozó adatok, adatbázisok azonosítása, előfordulási helyeinek és formáinak elemzése; egyéb elérhető erőforrások azonosítása (emberek, folyamatok, technológiák és eszközök).

Adatvédelmi tisztviselő szükségességének elemzése.

Adatleltár/adattérkép/data mapping/adatklasszifikáció, adatfolyamok; **kockázatelemzés** (*„Aki mindent véd, semmit sem véd”*).

A kezdeti prioritások meghatározása; a későbbi munkák különböző megközelítési módjának kiválasztása (kockázatelemzési/projekt management/jogi/… stb. alapú); az üzleti területek és folyamatok tulajdonosainak/vezetőinek tájékoztatása, tréningje.

Első lépések - eredmény

Cselekvési terv

- Eredménytermék:
  - **Mit!**
- Általában **nem** eredménytermék ebben a fázisban:
  - **Hogyan?**
  - **Mikor?**
  - **Költség?**
  - **Felelősök?**
  - …

Cselekvési terv

- Eredménytermék lehet a különböző GDPR munkacsoportok kialakítása, például:
  - Jogi
  - Üzleti (folyamatok)
  - Informatikai
  - Biztonsági
- Feladatok és felelősségi körök meghatározása
- Együttműködési formák, csatornák meghatározása

Cselekvési terv

- A GDPR felkészülés (is) csapatsport (jog/IT/HR/Marketing/PR/…)
- Az első tréningeket gyorsan és olcsón
- QuickWin (önbizalom erősítés, csapatépítés)
- **Ne próbáljuk meg azonnal tökéletesre írni !**

Cselekvési terv - minta

Ssz.	Report	Cél, fejlesztendő terület	Téma	Kockázat mértéke (1-5)	Időtáv	Felelős	Határidő
1.	3.2	Dokumentáció	Adatkezelési tájékoztató módosítása, publikálása	2	Rövid	Pató Pál	2017. december
2.	2.1	Folyamatok	Okmányok fénymásolásának megszüntetése	4	Rövid	Pató Pál	2017. december
3.	3.3	Dokumentáció	Új szerződésekhez használt formanyomtatványok, űrlapok aktualizálása az adatvédelmi elveknek megfelelően	2	Közép	Dr. Jogász János	2018. február
4.	3.5	Dokumentáció	A meglévő adatkezelési és adattovábbítási szerződések módosítása a belső adatvédelmi szabályzatnak megfelelően	3	Közép	Dr. Jogász János	2018. február
5.	5.2	Képzés	Adatvédelmi tisztviselő, adatgazdák, érintett kollégák képzése	2	Közép	Tréner Tamás	2018. április
6.	4.12	Informatika	Biztonsági mentések titkosítása	1	Hosszú	Rendszer Gazda	2018. május
7.	4.15	Informatika	Incidenskezelő (SIEM) rendszer üzembe helyezés	3	Hosszú	Rendszer Gazda	2018. december
8.							

Néhány kérdés

(„adatok” = személyes adatok)

- Gyűjtünk, tárolunk, vagy feldolgozunk személyes adatokat?
- Gyűjtünk, tárolunk, vagy feldolgozunk érzékeny személyes adatokat?
- Mely üzleti folyamataink használnak személyes adatokat? Ezeket mely informatikai rendszerek támogatják?
- Vannak adatgazdáink? A képzésük, jogosultságuk megfelelő?
- Van adatvédelmi felelősünk? A képzése, jogosultsága megfelelő?
- Van adatklasszifikációs rendszerünk?
- Van friss kockázatelemzésünk?
- Ki visz be adatokat a rendszereinkbe?
- Hogyan férünk hozzá az adatokhoz?
- Hogyan használjuk az adatokat?
- Ki használ személyes adatot?
- Hogyan biztosítjuk az adatokat?
- Ki törölhet adatokat, mikor és hogyan? Ez valódi törlés?
- Ki archiválhat adatokat és hogyan? Mindenki érti a különbséget a biztonsági mentés és az archiválás között?
- Hogyan mozognak az adatok a rendszerek között?
- Hogyan mentjük az adatokat?
- Hogyan tudunk egyes személyes adatokat elérni, kiadni?
- Az adatmentéseket hogyan óvjuk, és ellenőrizzük?
- Hogyan adunk át adatot harmadik félnek?
- Küldünk-e külföldre adatokat? Küldünk az EU-n kívülre adatokat?
- Hogyan kezeljük az adatkezelésünkkel kapcsolatos megkereséseket, kéréseket?
- Hogyan kezeljük az adatokkal kapcsolatos incidenseket?
- A fejlesztéseinkben hogyan kezeljük az adatbiztonságot? („Privacy by design”)
- Hogy néz ki az üzleti folyamatok, szabványok, céges szokások fejlesztése?

Öt KOMOLY kérdés a felkészülés során

1. Milyen személyes adatokat kezelünk, és hol találhatók ezek?
2. Ki kezelheti ezeket az adatokat, és ki fért eddig hozzá valójában?
3. Ellenőrzésünk alatt van a személyes adatok tárolási helye?
4. Azonnal észleljük a jogosulatlan hozzáférést, vagy adatszivárgást?
5. A pozitív gyakorlatunkat hitelt érdemlően tudjuk igazolni?

Leggyakoribb (??) kihívás

- „Milyen személyes adatokat kezelnek rólam, és hogyan?”
  - 15. cikk: *„Az érintett hozzáférési joga”*
  - 16. cikk *„A helyesbítéshez való jog”*
  - 17. cikk *„A törléshez való jog („az elfeledtetéshez való jog”)”*
  - 18. cikk *„Az adatkezelés korlátozásához való jog”*
  - 19. cikk *„A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség”*
  - 20. cikk *„Az adathordozhatósághoz való jog”*
  - 21. cikk *„A tiltakozáshoz való jog”*
  - 22. cikk *„Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást”*
- *„Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet …”*

Ügyfélkapcsolat
(az érintett jogai)

… az érintett részére a személyes adatok kezelésére vonatkozó, … valamennyi információt és … minden egyes tájékoztatást **tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa**

Folyamatot kialakítani:

- A hozzájárulások beszerzésére és annak **igazolására**
- Ügyfelek kéréseinek, megkereséseinek kezelésére (pl. adatszolgáltatás)
- Adatok módosításának kezelésére
- Az „elfeledtetéshez való jog” gyakorlására
- …

Leggyakoribb (??) kihívás

- 12. cikk **Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések**
- *„Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, … valamennyi információt és … minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében.”*
- = a felhasználó nyelvén! (EU 24 hivatalos nyelv + félhivatalos + bevándorló+ egyéb…)

Leggyakoribb (??) kihívás

- Ki intézi ezeket a kéréseket?
  - Adatvédelmi tisztviselő
  - Fordítási hiba! 37. cikk, Az adatvédelmi tisztviselő kijelölése
    - *„(7) Az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a felügyeleti hatósággal közli.”*
    - *„(7) The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.”*
    - *„(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.”*
    - *„(7) Voditelj obrade ili izvršitelj obrade objavljuje kontaktne podatke službenika za zaštitu podataka i priopćuje ih nadzornom tijelu.”*
    - *„(7) El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.”*

- Megfontolásra érdemes pontok

Hol érkeznek a cégbe személyes adatok?

- ügyfélszolgálat
- porta (belépőkártyák, személyi igazolványok,…) **MÁS a papíralapú megőrizhetőség és más az elektronikus!**
- call center (rögzített felvétel?)
- szerződésekben szereplő kapcsolattartók
- tenderekben szereplő személyes adatok
- GPS adatok, IP címek, cookie-k/sütik, stb.

Hol kezelnek személyes adatokat?

- papíralapú
- elektronikus
    - strukturált adatok
    - nem strukturált adatok (!!)

Hova továbbítják a személyes adatokat?

- személyes adatok továbbítása harmadik félnek
    - posta
    - telekommunikációs cégek
    - követeléskezelők
    - marketing cégek (dm levél küldő szerverek)
    - google adwords
- személyes adatok továbbítása külföldre?
- személyes adatok továbbítása EU-n kívülre?

Informatikai GDPR költségvetés 2018*	Belsős opció?	2017 (tény)	JAN	FEB	MÁR	ÁPR	MÁJ	JÚN	JÚL	AUG	SZEP	OKT	NOV	DEC	Összesen	DIFF	Megjegyzések
SZOFTVER (GDPR)																	
Végpontvédelmi szoftver frissítése (application control, web control, stb.)		3 200 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	3 800 000 Ft	- Ft	- Ft	- Ft	- Ft	3 800 000 Ft	15,79%	
Adatklasszifikációt segítő szoftver		- Ft	2 500 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 500 000 Ft	100,00%	
DLP szoftver		- Ft	- Ft	- Ft	3 000 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	3 000 000 Ft	100,00%	
SIEM rendszer	✔	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	5 000 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	5 000 000 Ft	100,00%	
Titkosító szoftver		- Ft	- Ft	2 000 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 000 000 Ft	100,00%	
MDM (mobil eszközök védelmét biztosító) szoftver		- Ft	- Ft	- Ft	- Ft	2 800 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 800 000 Ft	100,00%	
Anonimizálási fejlesztések a különböző adatbázisokban		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	3 500 000 Ft	- Ft	- Ft	3 500 000 Ft	100,00%	
Egyéb szoftver (SOC, IDM, ...)		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	3 000 000 Ft	- Ft	3 000 000 Ft	100,00%	
Szoftverköltségek összesen		**3 200 000 Ft**	**2 500 000 Ft**	**2 000 000 Ft**	**3 000 000 Ft**	**2 800 000 Ft**	**- Ft**	**5 000 000 Ft**	**- Ft**	**3 800 000 Ft**	**- Ft**	**3 500 000 Ft**	**3 000 000 Ft**	**- Ft**	**25 600 000 Ft**	**87,50%**	
HARDVER (GDPR)																	
FireEye		- Ft	- Ft	- Ft	- Ft	- Ft	3 500 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	3 500 000 Ft	100,00%	
SIEM szerver		- Ft	650 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	650 000 Ft	100,00%	
Hardverköltségek összesen		**- Ft**	**650 000 Ft**	**- Ft**	**- Ft**	**- Ft**	**3 500 000 Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**4 150 000 Ft**	**100,00%**	
SZEMÉLYI KIADÁSOK - GDPR tanácsadás																	
Szabályzatok módosítása	✔	600 000 Ft	- Ft	400 000 Ft	- Ft	600 000 Ft	- Ft	- Ft	- Ft	1 500 000 Ft	- Ft	300 000 Ft	- Ft	- Ft	2 800 000 Ft	78,57%	
GDPR hiányosságok elemzése	✔	- Ft	650 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	650 000 Ft	100,00%	
Adatklasszifikáció	✔	- Ft	- Ft	2 500 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 500 000 Ft	100,00%	
Adatvagyon felmérés		- Ft	- Ft	- Ft	1 800 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	1 800 000 Ft	100,00%	
Incidenskezelési eljásárok fejlesztése, SIEM rendszer bevezetés	✔	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 500 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 500 000 Ft	100,00%	
Szoftver- és hardverleltár	✔	- Ft	2 500 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 500 000 Ft	100,00%	
Informatikai kockázatelemzés		- Ft	- Ft	- Ft	- Ft	- Ft	2 450 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 450 000 Ft	100,00%	
Adatvédelmi hatásvizsgálat az új CRM rendszerre	✔	- Ft	- Ft	800 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	800 000 Ft	100,00%	
Jogosultsági rendszer felülvizsgálata, módosítása		- Ft	- Ft	- Ft	800 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	800 000 Ft	100,00%	
Anonimizálás lehetőségei a különböző adatbázisokban	✔	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	0,00%	
Biztonsági mentések és archiválás rendszerének fejlesztése	✔	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	1 500 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	1 500 000 Ft	100,00%	
Egyéb tanácsadók		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	0,00%	
Utazás, szállás		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	0,00%	
Személyi kiadások összesen		**3 800 000 Ft**	**6 950 000 Ft**	**5 700 000 Ft**	**5 600 000 Ft**	**6 200 000 Ft**	**9 450 000 Ft**	**7 500 000 Ft**	**1 500 000 Ft**	**5 300 000 Ft**	**- Ft**	**7 300 000 Ft**	**6 000 000 Ft**	**- Ft**	**61 500 000 Ft**	**93,82%**	
TRÉNING, TOVÁBBKÉPZÉS																	
Kötelező (adatvédelmi tisztviselő képzése)	✔	- Ft	- Ft	- Ft	300 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	300 000 Ft	100,00%	
Kötelező (adatgazdák képzése)	✔	- Ft	- Ft	50 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	50 000 Ft	100,00%	
Felhasználói tréningek (adatvédelem és IT biztonság)	✔	80 000 Ft	90 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	90 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	180 000 Ft	55,56%	
Tudatosító kampányok (adatvédelem és IT biztonság)	✔	- Ft	- Ft	- Ft	- Ft	28 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	28 000 Ft	- Ft	- Ft	56 000 Ft	100,00%	
Opcionális		30 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	30 000 Ft	- Ft	- Ft	- Ft	- Ft	30 000 Ft	0,00%	
Könyvek, újságok, segédanyagok		30 000 Ft	44 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	44 000 Ft	31,82%	
Tréning, továbbképzés összesen		**140 000 Ft**	**134 000 Ft**	**50 000 Ft**	**300 000 Ft**	**28 000 Ft**	**- Ft**	**- Ft**	**90 000 Ft**	**30 000 Ft**	**- Ft**	**28 000 Ft**	**- Ft**	**- Ft**	**660 000 Ft**	**78,79%**	
ONLINE SZOLGÁLTATÁSOK																	
Felhő alapú szolgáltatások		2 500 000 Ft	100 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	100 000 Ft	-2400,00%	
Webfejlesztés (webshop módosítása)		300 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	1 500 000 Ft	- Ft	- Ft	- Ft	1 500 000 Ft	80,00%	
Webfejlesztés (céges honlap módosítás)		200 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	250 000 Ft	- Ft	250 000 Ft	20,00%	
Online marketing rendszer módosításai		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	0,00%	
Online szolgáltatások összesen		**3 000 000 Ft**	**100 000 Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**- Ft**	**250 000 Ft**	**- Ft**	**1 850 000 Ft**	**-62,16%**	
EGYÉB KÜLSŐ SZOLGÁLTATÁSOK																	
Jogi iroda (adatvédelmi szakjogász)		600 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	70 000 Ft	840 000 Ft	28,57%	
Fizikai biztonsági szolgáltatások (szerverközpont védelem)		600 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	30 000 Ft	360 000 Ft	-66,67%	
Etikus hack		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	2 500 000 Ft	2 500 000 Ft	100,00%	
Biztonsági kamerák átszervezése, átszerelése		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	670 000 Ft	- Ft	- Ft	- Ft	- Ft	- Ft	670 000 Ft	100,00%	
Adatvédelmi audit		- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	- Ft	3 500 000 Ft	- Ft	- Ft	- Ft	- Ft	3 500 000 Ft	100,00%	
Egyéb külső szolgáltatások összesen		**1 200 000 Ft**	**100 000 Ft**	**100 000 Ft**	**100 000 Ft**	**100 000 Ft**	**100 000 Ft**	**100 000 Ft**	**770 000 Ft**	**3 600 000 Ft**	**100 000 Ft**	**100 000 Ft**	**100 000 Ft**	**2 600 000 Ft**	**7 870 000 Ft**	**84,75%**	
Összes Informatikai GDPR kiadás (tervezet)		**11 340 000 Ft**	**10 434 000 Ft**	**7 850 000 Ft**	**9 000 000 Ft**	**9 128 000 Ft**	**13 050 000 Ft**	**12 600 000 Ft**	**2 360 000 Ft**	**12 730 000 Ft**	**100 000 Ft**	**10 928 000 Ft**	**9 350 000 Ft**	**2 600 000 Ft**	**100 130 000 Ft**		

** A belső munkaerő bérköltségével itt nem számolva*

Félreértés:„Teljes GDPR felkészítés”!!

- Ilyet senki nem vállalhat, mert nem tud rá garanciát adni!
  - Casco a 6M Ft-os autóra (100e Ft/év)
  - Casco a 60MFt-os autóra = ??
  - Casco a HAT MILLIÁRD forintos autóra???

A GDPR megfelelés nem egy állapot, hanem egy folyamat!

Félreértés: általános

”A rendelet túl általánosan/tágan fogalmaz!”

Példa: 32. cikk „Az adatkezelés biztonsága”

58 szó!

1) Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

   a) a személyes adatok álnevesítését és titkosítását;

   b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

   c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

   d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

Félreértés: általános

32. cikk „Az adatkezelés biztonsága”

Figyelembe kell venni (elemezni):

- a tudomány és technológia állása,
- a megvalósítás költségeit,
- az adatkezelés jellegét,
- az adatkezelés hatókörét,
- az adatkezelés körülményeit,
- az adatkezelés céljait,
- a természetes személyek jogaira és szabadságaira jelentett kockázatokat,

hogy megfelelő technikai és szervezési intézkedéseket hajtsunk végre,

hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantáljuk.

Ilyen technikai és szervezési intézkedés lehet például:

a) a személyes adatok álnevesítése és titkosítása,

b) a rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása (integritás, rendelkezésre állás, ellenálló képesség),

c) incidens esetén a rendelkezésre állást kellő időben vissza lehessen állítani (BCP/DRP),

d) az intézkedések rendszeres tesztelése, felmérése és értékelése.

Mi az in nuce?

- in nuce *(ejtsd: in núce) latin eredetű kifejezés, jelentése: dióhéjban, röviden.*
- GDPR rendelet 88 oldal, 99 cikk: „dióhéjban”
- Első megjelenés: 2017 nov. 16!

Kinek jó az in nuce?

- Kevés
  - és egyszerű üzleti folyamat,
  - informatikai célrendszer,
  - kiszervezett tevékenység,
  - alkalmazott.

- A levelezés központosított, managelhető.
- Mikrovállalkozások, KKV-k, multik beszállítói, háziorvosi rendelők, iskolák, …

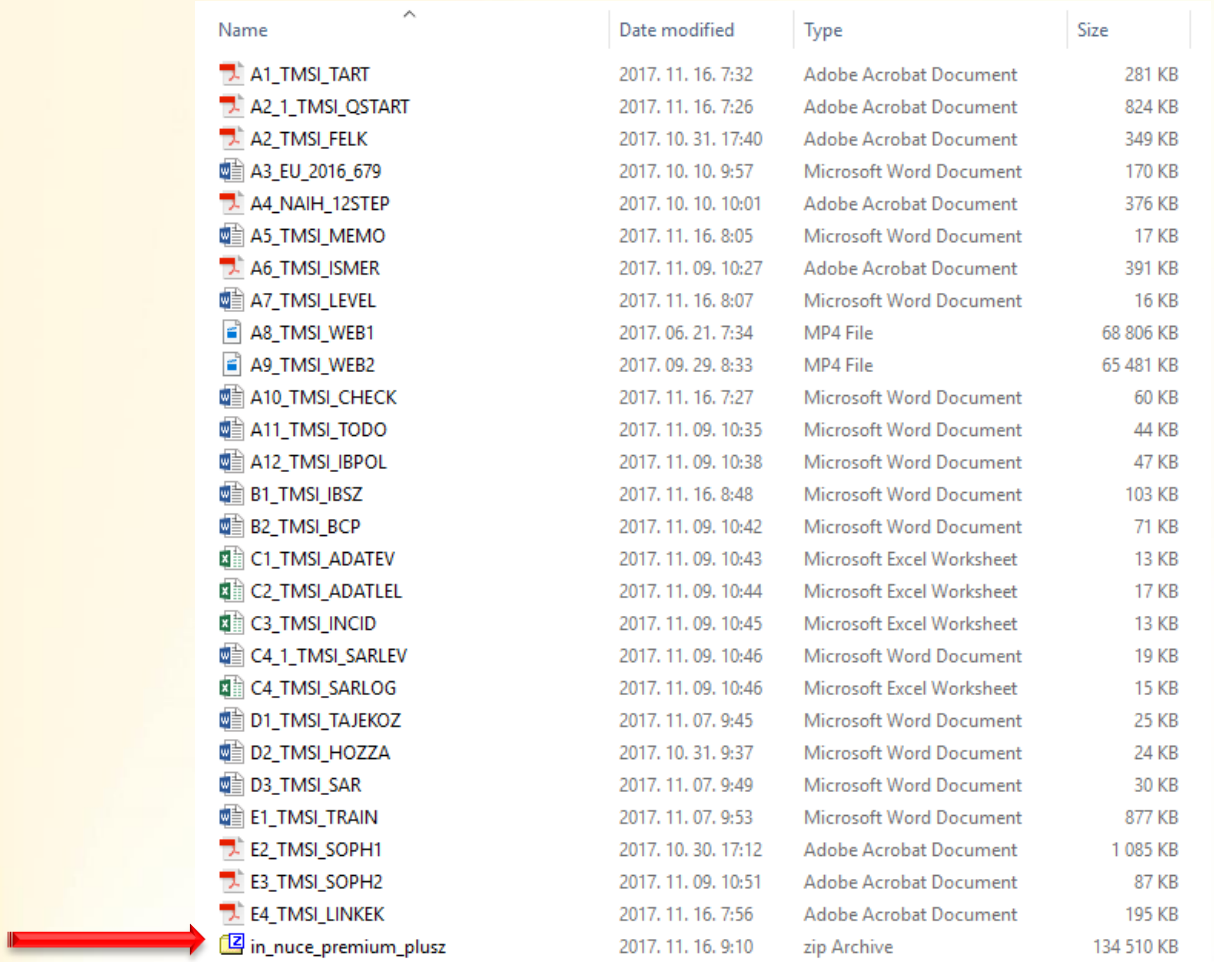
„in nuce” tartalomjegyzék

#	Azonosító	Leírás	Formátum	Alap	Prémium	Prémium plusz
A1	TMSI_TART	Tartalomjegyzék, a mellékelt dokumentumok jegyzéke és rövid leírása	PDF	✓	✓	✓
A2	TMSI_FELK	Legfontosabb lépések vizuálisan	PDF	✓	✓	✓
A2.1	TMSI_QSTART	Első lépések, rövid felkészülési útmutató	PDF	✓	✓	✓
A3	EU_2016/679	Az EU rendelet teljes szövege	DOC	✓	✓	✓
A4	NAIH_12STEP	A NAIH rövid grafikus iránymutatása	PDF	✓	✓	✓
A5	TMSI_MEMO	Vezetőket tájékoztató levél	DOC	✓	✓	✓
A6	TMSI_ISMER	GDPR ismertető vezetőknek	PDF	✓	✓	✓
A7	TMSI_LEVEL	GDPR tájékoztató levél az alkalmazottaknak	DOC	✓	✓	✓
A8	TMSI_WEB1	GDPR alapok, PPT/video ismertető (53 perc)	MP4	✓	✓	✓
A9	TMSI_WEB2	Hogyan kezdjük? PPT/video ismertető (55 perc)	MP4	✓	✓	✓
A10	TMSI_CHECK	Kérdőív, checklist	DOC	×	✓	✓
A11	TMSI_TODO	Cselekvési terv	DOC	✓	✓	✓
A12	TMSI_IBPOL	Informatikai biztonsági politika	DOC	×	✓	✓
		Szabályzatok				
B1	TMSI_IBSZ	Informatikai biztonsági szabályzat, benne	DOC	✓	✓	✓
B1.1	TMSI_IBSZ	Kockázatelemzési eljárásrend	DOC	×	×	✓
B1.2	TMSI_IBSZ	Adatkezelési eljárásrend	DOC	✓	✓	✓
B1.3	TMSI_IBSZ	Adatvédelmi hatásvizsgálati eljárásrend	DOC	×	×	✓
B1.4	TMSI_IBSZ	Jogosultságkezelés	DOC	×	×	✓
B1.5	TMSI_IBSZ	Adatmentési eljárásrend	DOC	✓	✓	✓
B1.6	TMSI_IBSZ	Incidenskezelési eljárásrend	DOC	✓	✓	✓
B1.7	TMSI_IBSZ	Adatkezelési kérés- és panaszkezelés	DOC	✓	✓	✓
B1.8	TMSI_IBSZ	Oktatás, számítógéphasználati elvek	DOC	×	✓	✓
B1.9	TMSI_IBSZ	Ellenőrzési eljárásrend	DOC	✓	✓	✓
B2	TMSI_BCP	Üzletmenet-folytonossági terv (BCP)	DOC	×	×	✓
		Nyilvántartások				
C1	TMSI_ADATEV	Az adatkezelési tevékenységek nyilvántartása	XLS	✓	✓	✓
C2	TMSI_ADATLEL	Nyilvántartás a személyes adatok kezeléséről (adatleltár)	XLS	✓	✓	✓
C3	TMSI_INCID	Az adatvédelmi incidensek nyilvántartása	XLS	×	✓	✓
C4	TMSI_SARLOG	Az érintettek/adatalanyok kéréseinek naplója	XLS	×	✓	✓
C4.1	TMSI_SARLEV	Az adatalanyok kéréseire adott válaszlevél	DOC	×	×	✓
		Honlap				
D1	TMSI_TAJEKOZ	Adatkezelési tájékoztató honlapra	DOC	✓	✓	✓
D2	TMSI_HOZZA	Adatkezelési hozzájárulási űrlap	DOC	×	✓	✓
D3	TMSI_SAR	Adatkezelési kérelmi űrlap	DOC	×	×	✓
		Egyéb				
E1	TMSI_TRAIN	Belső adatkezelési figyelemfelkeltő tréning (teszt kérdésekkel)	DOC	×	×	✓
E2	TMSI_SOPH1	GDPR általános ismertető (Sophos Whitepaper)	PDF	✓	✓	✓
E3	TMSI_SOPH2	Rövid titkosítási útmutató (Sophos Whitepaper, angolul)	PDF	✓	✓	✓
E4	TMSI_LINKEK	Linkek nyitott forráskódú (ingyenes) szoftverekhez amelyek segítséget jelenthetnek a GDPR-hez	PDF	✓	✓	✓

A mindenkor aktuális lista elérhetősége:
https://tmsi.hu/in-nuce/

IN NUCE

in nuce



Name	Date modified	Type	Size
A1_TMSI_TART	2017. 11. 16. 7:32	Adobe Acrobat Document	281 KB
A2_1_TMSI_QSTART	2017. 11. 16. 7:26	Adobe Acrobat Document	824 KB
A2_TMSI_FELK	2017. 10. 31. 17:40	Adobe Acrobat Document	349 KB
A3_EU_2016_679	2017. 10. 10. 9:57	Microsoft Word Document	170 KB
A4_NAIH_12STEP	2017. 10. 10. 10:01	Adobe Acrobat Document	376 KB
A5_TMSI_MEMO	2017. 11. 16. 8:05	Microsoft Word Document	17 KB
A6_TMSI_ISMER	2017. 11. 09. 10:27	Adobe Acrobat Document	391 KB
A7_TMSI_LEVEL	2017. 11. 16. 8:07	Microsoft Word Document	16 KB
A8_TMSI_WEB1	2017. 06. 21. 7:34	MP4 File	68 806 KB
A9_TMSI_WEB2	2017. 09. 29. 8:33	MP4 File	65 481 KB
A10_TMSI_CHECK	2017. 11. 16. 7:27	Microsoft Word Document	60 KB
A11_TMSI_TODO	2017. 11. 09. 10:35	Microsoft Word Document	44 KB
A12_TMSI_IBPOL	2017. 11. 09. 10:38	Microsoft Word Document	47 KB
B1_TMSI_IBSZ	2017. 11. 16. 8:48	Microsoft Word Document	103 KB
B2_TMSI_BCP	2017. 11. 09. 10:42	Microsoft Word Document	71 KB
C1_TMSI_ADATEV	2017. 11. 09. 10:43	Microsoft Excel Worksheet	13 KB
C2_TMSI_ADATLEL	2017. 11. 09. 10:44	Microsoft Excel Worksheet	17 KB
C3_TMSI_INCID	2017. 11. 09. 10:45	Microsoft Excel Worksheet	13 KB
C4_1_TMSI_SARLEV	2017. 11. 09. 10:46	Microsoft Word Document	19 KB
C4_TMSI_SARLOG	2017. 11. 09. 10:46	Microsoft Excel Worksheet	15 KB
D1_TMSI_TAJEKOZ	2017. 11. 07. 9:45	Microsoft Word Document	25 KB
D2_TMSI_HOZZA	2017. 10. 31. 9:37	Microsoft Word Document	24 KB
D3_TMSI_SAR	2017. 11. 07. 9:49	Microsoft Word Document	30 KB
E1_TMSI_TRAIN	2017. 11. 07. 9:53	Microsoft Word Document	877 KB
E2_TMSI_SOPH1	2017. 10. 30. 17:12	Adobe Acrobat Document	1 085 KB
E3_TMSI_SOPH2	2017. 11. 09. 10:51	Adobe Acrobat Document	87 KB
E4_TMSI_LINKEK	2017. 11. 16. 7:56	Adobe Acrobat Document	195 KB
in_nuce_premium_plusz	2017. 11. 16. 9:10	zip Archive	134 510 KB

IN NUCE

Dióhéjban a GDPR: EU általános adatvédelmi rendeletére való felkészülési folyamatát segítő anyagok összesége.

www.tmsi.hu/in-nuce · (+361) 321-0631 · innuce@tmsi.hu

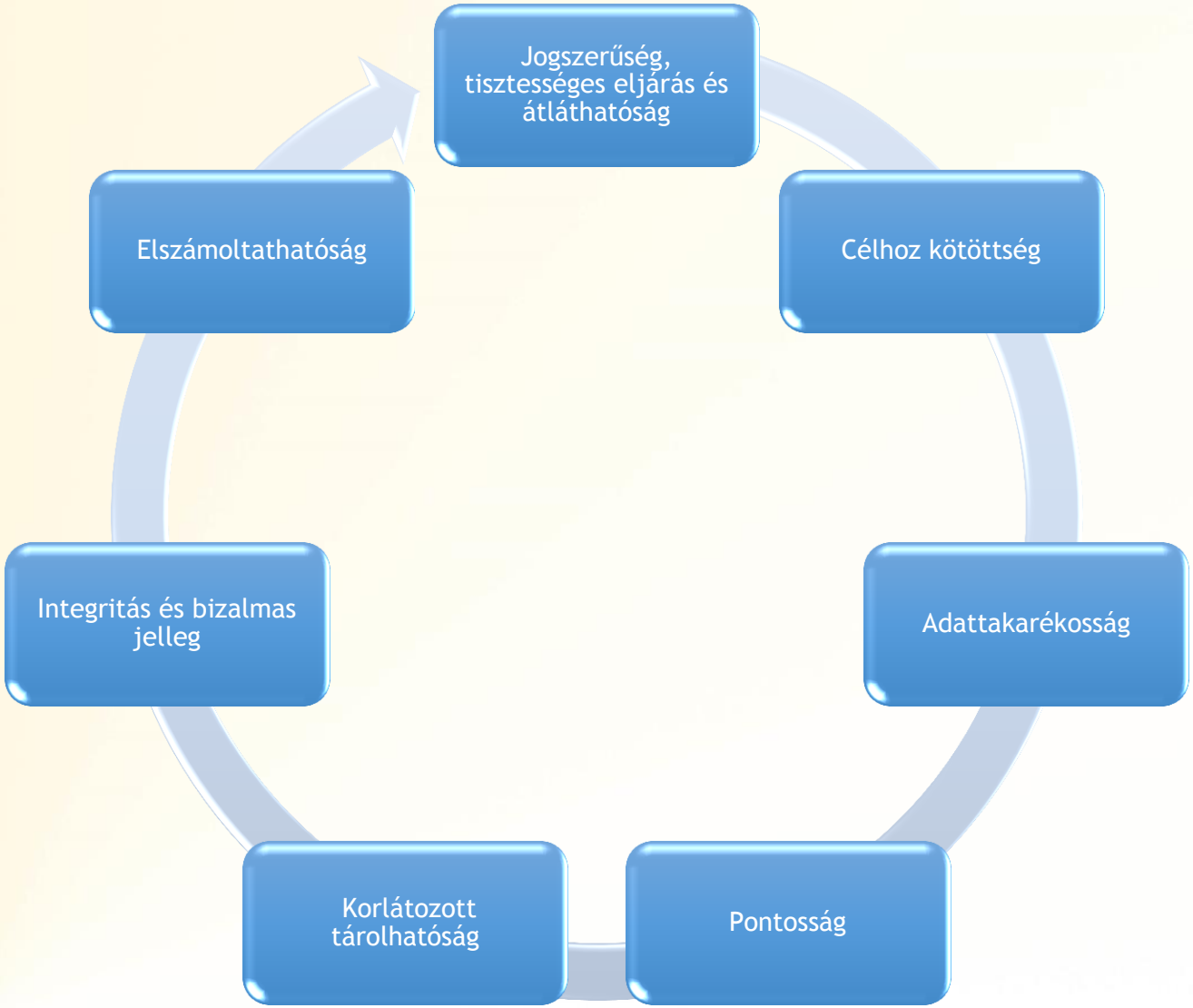
Miért ebben a struktúrában?

- A GDPR-ből a G = általános!
  (**általános** adatvédelmi rendelet)

Nincs technológia előírva,
nincs kötelező szabályozási struktúra,

elvek és elvárások vannak!

Elvek


Jogszerűség, tisztességes eljárás és átláthatóság
Célhoz kötöttség
Adattakarékosság
Pontosság
Korlátozott tárolhatóság
Integritás és bizalmas jelleg
Elszámoltathatóság

Azonosító	Leírás	Formátum			
TMSI_FELK	Legfontosabb lépések vizuálisan	PDF	✓	✓	✓

Azonosító	Leírás	Formátum			
TMSI_QSTART	Első lépések, rövid felkészülési útmutató	PDF	✓	✓	✓

2 Érintettség elemzése

HA a szervezet vezetősége felől megkaptuk a teljes támogatást, akkor először is azt kell első lépésben tisztázni, hogy a szervezet érintett-e a GDPR kérdésében, milyen mértékben és hogyan.

Nagy valószínűséggel érintett, például: munkaszerződésekben szereplő személyes adatok, e-mail-ekben előforduló személyes adatok, feljegyzésekben/táblázatokban/papír alapon/ stb. előforduló személyes adatok, honlapunk elhelyez-e „sütiket" a látogatót gépén, rögzítünk-e mobiltelefonos- vagy más helymeghatározós adatokat, van-e beléptető- vagy kamera-rendszerünk stb.

Ehhez a fázishoz a következő dokumentumokat javasoljuk segédeszközként:

- TMSI_LEVEL GDPR tájékoztató levél az alkalmazottaknak
- TMSI_WEB1 GDPR alapok, video ismertető (53 perc)
- TMSI_WEB2 Hogyan kezdjük? video ismertető (55 perc)

3 Adatvédelmi felelős kijelölése

HA a szervezetünk érintett, azaz kezelünk személyes adatokat, akkor érdemes megfontolni egy adatvédelmi felelős kijelölését.

A GDPR rendelet adatvédelmi tisztviselő kinevezését írja elő (37. cikk) az alábbi esetekben:

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
*b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, **amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé**;*
c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Ennek a cikknek az értelmezése még elég képlékeny, de ha úgy érezzük, hogy egy adatvédelmi megbízott segítségünkre lehet hosszú távon, akkor bízzunk meg ezzel külső szakértőt (a rendelet erre lehetőséget ad), vagy nevezzünk ki valakit a szervezeten belülről. 37. cikk, 5. pont: *„Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a ... feladatok ellátására való alkalmasság alapján kell kijelölni."*

Ugyanakkor, ha nem vagyunk a kinevezésre kötelezettek, de szükségét érezzük egy ilyen felelősnek, akkor talán az lenne a praktikusabb megoldás, ha megbíznánk valakit ezekkel a feladatokkal, de NEM adatvédelmi tisztviselőnek hívnánk (hanem pl. adatkezelési felelős). Ez esetben ugyanis lenne felelősünk, de nem lenne alanya a rendeletnek.

Ehhez a fázishoz a következő dokumentumokat javasoljuk segédeszközként:

- EU_2016/679 Az EU rendelet teljes szövege

4 Érettségi fok, hiányosságok elemzése

Ha található nálunk személyes adat, akkor nagyon nagy vonalakban meg kell vizsgálni a szervezet „érettségi fokát". Azaz, például:

- Milyen (digitális és papír alapú) személyes adatokat kezelünk, és hol találhatók ezek?
- Ki kezelheti ezeket az adatokat, és ki fért eddig hozzá valójában?
- Ellenőrzésünk alatt van a személyes adatok tárolási helye? (pl. használunk-e felhő alapú tárolást?)
- Azonnal észleljük a jogosulatlan hozzáférést, vagy adatszivárgást?
- A pozitív gyakorlatunkat hitelt érdemlően tudjuk igazolni?

Csak egy ilyen alapfelmérés, és az ott felmerülő hiányosságok megfogalmazása után tudunk pontos tervet vázolni a megfelelőség elérésére. Csak ezek után tudunk idő- és erőforrásigényeket tervezni, pontos cselekvési tervet összeállítani.

Ehhez a fázishoz a következő dokumentumokat javasoljuk segédeszközként:

- TMSI_IBSZ Informatikai biztonsági szabályzat
- TMSI_CHECK Kérdőív
- TMSI_TODO Cselekvési terv

5 Adatleltár, adatfolyam felmérése

A gyakorlati munka kezdetén meg kell állapítani, hogy **hol kezelünk és tárolunk a rendelet által érintett személyes adatokat.**

A papír alapú dokumentumok felmérése általában az egyszerűbb feladat, hiszen egy kisebb szervezetben ez könnyebben áttekinthető, felmérhető, rendbe tehető.

Az elektronikusan tárolt személyes adatok összeírása egyrészt az üzleti folyamatok elemzésével (Ki kezel személyes adatokat? Kitől kapja ezeket? Kinek továbbítja ezeket a cégen belül és kívül? Az elektronikus levelezésekben mikor fordulhatnak elő ilyen adatok?), másrészt a különböző tárolók átnézésével történhet. Ez utóbbi átnézés történhet manuálisan, és különböző célszoftverek segítségével, az adatmennyiség és a komplexitás függvényében.

Ehhez a fázishoz a következő dokumentumokat javasoljuk segédeszközként:

- TMSI_ADATEV Az adatkezelési tevékenységek nyilvántartása
- TMSI_ADATLEL Nyilvántartás a személyes adatok kezelésről (adatleltár minta).
- TMSI_LINKEK Linkek szoftverekhez, amelyek segítséget jelenthetnek a GDPR-hez

Azonosító	Leírás	Formátum			
EU_2016/679	Az EU rendelet teljes szövege	DOC	✓	✓	✓

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)

(EGT-vonatkozású szöveg)

AZ EUROPAI PARLAMENT ES AZ EUROPAI UNIO TANACSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 16. cikkére,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére (1),

tekintettel a Régiók Bizottságának véleményére (2),

rendes jogalkotási eljárás keretében (3),

mivel:

(1) A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

(2) A természetes személyek személyes adataik kezelésével összefüggő védelméhez kapcsolódó elvek és szabályok a természetes személyek állampolgárságától és lakóhelyétől függetlenül tiszteletben tartják e természetes személyek alapvető jogait és szabadságait, különösen, ami a személyes adataik védelméhez való jogukat illeti. Ez hozzájárul a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség, valamint a gazdasági unió megteremtéséhez, a gazdasági és társadalmi fejlődéshez, a belső piacon belüli gazdaságok erősödéséhez és konvergenciájához, valamint a természetes személyek jólétéhez.

(3) A 95/46/EK európai parlamenti és tanácsi irányelv (4) célja, hogy harmonizálja az adatkezelési tevékenységek tekintetében a természetes személyek alapvető jogainak és szabadságainak védelmét, valamint, hogy biztosítsa a személyes adatok tagállamok közötti szabad áramlását.

(4) A személyes adatok kezelését az emberiség szolgálatába kell állítani. A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal. Ez a rendelet minden alapvető jogot tiszteletben tart, és szem előtt tartja a Chartában elismert és a Szerződésekben rögzített szabadságokat és elveket, különösen ami a magán- és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához és a személyes adatok védelméhez, a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a véleménynyilvánítás szabadságához és a tájékozódás szabadságához, a vállalkozás szabadságához, a hatékony jogorvoslathoz és a tisztességes eljáráshoz, és a kulturális, vallási és nyelvi sokféleséghez való jogot illeti.

(5) A belső piac működéséből eredő gazdasági és társadalmi integráció lényegesen megnövelte a személyes adatok határokon átnyúló áramlását. Megnövekedett az állami és a magánszereplők, köztük a természetes személyek, egyesületek és a vállalkozások között Unió-szerte zajló személyes adatok cseréje. Az uniós jog együttműködésre és személyes adatok cseréjére kötelezi tagállamok nemzeti hatóságait annak érdekében, hogy képesek legyenek feladataikat ellátni, illetve hogy más tagállam hatóságai nevében eljárjanak.

(6) A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét.

(7) E fejlemények egy olyan szilárd és az eddiginél következetesebb uniós adatvédelmi keretet igényelnek, amelyet erős kikényszeríthetőség támogat, hiszen a bizalom megteremtése fontos a digitális gazdaság belső piaci fejlődéséhez. A természetes személyek számára biztosítani kell, hogy saját személyes adataik felett maguk rendelkezzenek. A természetes személyek, a gazdasági szereplők és a közhatalmi szervek számára a jogbiztonságot és a gyakorlati biztonságot fokozni kell.

(8) Ha e rendelet úgy rendelkezik, hogy a benne foglalt szabályokat tagállami jog által pontosítani, illetve korlátozni lehet, a tagállamok e rendelet egyes elemeit beépíthetik a nemzeti jogukba, ha az a koherencia biztosításához, valamint ahhoz szükséges, hogy a nemzeti rendelkezések a hatályuk alá tartozó személyek számára érthetők legyenek.

(9) A 95/46/EK irányelv célkitűzései és elvei továbbra is érvényesek, azonban az irányelv nem akadályozta meg sem azt, hogy az Unió tagállamaiban az adatvédelem végrehajtása széttagolt módon valósuljon meg, sem a jogbizonytalanságot, sem pedig azt, hogy széles körben az a benyomás alakuljon ki, hogy természetes személy védelme – különösen az online tevékenységek esetében – jelentős kockázatoknak van kitéve. Az a tény, hogy a személyes adatok kezelése tekintetében a természetes személyek jogai és szabadságai egyes tagállamokban eltérő szintű védelmet élveznek, különösen, ami személyes adatok védelméhez való jogot illeti, a személyes adatok Unióban történő szabad áramlásának útjában állhat. Ebből eredően ezek az eltérések a gazdasági tevékenységek uniós szinten való folytatásának akadályát képezhetik, torzíthatják a versenyt, és hátráltathatják a hatóságokat az uniós jog szerinti feladataik ellátásában. A jogok és szabadságok védelmi szintjében mutatkozó ilyen eltérések a 95/46/EK irányelv végrehajtásában és alkalmazásában fennálló eltérésekre vezethetők vissza.

(10) A természetes személyek következetes és magas szintű védelmének biztosítása és a személyes adatok Unión belüli áramlása előtti akadályok elhárítása érdekében a természetes személyeknek az ilyen adatok kezelésével összefüggésben fennálló jogait és szabadságait minden tagállamban azonos szintű védelemben kell részesíteni. A természetes személyeknek a személyes adataik kezeléséhez kapcsolódó alapvető jogai és szabadságai védelmére vonatkozó szabályok következetes és egységes alkalmazását az Unió egész területén biztosítani kell. A tagállamok számára lehetővé kell tenni, hogy az e rendeletben foglalt szabályok alkalmazását pontosító nemzeti rendelkezéseket tartsanak fenn vagy vezessenek be, ha a személyes adatok kezelésére jogi kötelezettség teljesítéséhez, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges. A 95/46/EK irányelvet végrehajtó általános és horizontális adatvédelmi jogszabályokhoz kapcsolódóan a tagállamok számos ágazatspecifikus jogszabályt hoztak azokon a területeken, ahol konkrétabb rendelkezésekre van szükség. Ez a rendelet a tagállamok számára mozgásteret biztosít ahhoz, hogy pontosítsák a benne meghatározott szabályokat, ideértve a személyes adatok különleges kategóriáira („különleges adatok") vonatkozókat is. Ennyiben tehát ez a rendelet nem zárja ki olyan tagállami jog elfogadását, amely meghatározza a különleges adatkezelési helyzetek körülményeit, ezen belül pontosabban megállapítja, hogy milyen feltételek mellett jogszerű a személyes adatok kezelése.

(11) Ahhoz, hogy a személyes adatok az Unió egész területén hatékony védelemben részesüljenek, az érintettek jogait, valamint a személyes adatokat kezelő, illetve az adatkezelést meghatározó személyek kötelezettségeit megerősíteni és részletesen meghatározni szükséges, ugyanakkor pedig az egyes tagállamokban a személyes adatok védelmére vonatkozó szabályok betartásának ellenőrzéséhez és biztosításához egyenértékű hatáskört is biztosítani szükséges, és a jogsértőkre azonos szankciókat kell alkalmazni.

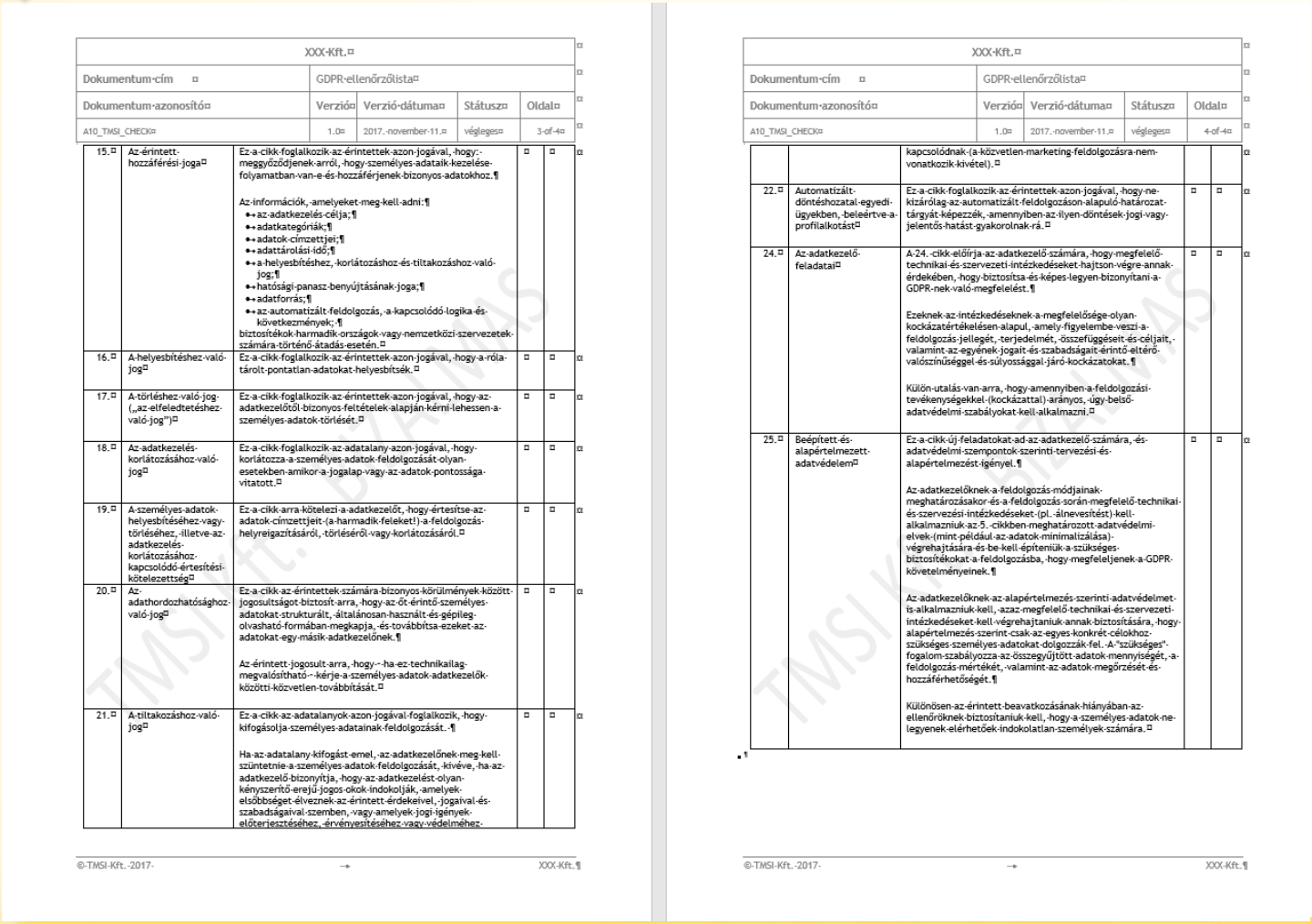
(12) Az EUMSZ 16. cikkének (2) bekezdése felhatalmazza az Európai Parlamentet és a Tanácsot a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályok megállapítására.

(13) A természetes személyek egységes, uniós-szintű védelmének biztosítása, valamint a személyes adatok belső piacon való szabad áramlását akadályozó eltérések megelőzése érdekében rendelettel kell biztosítani a jogbiztonságot és az áttekinthetőséget valamennyi tagállam gazdasági szereplői részére – beleértve a mikro-, kis- és középvállalkozásokat is –, továbbá rendelettel kell biztosítani a természetes személyek részére minden tagállamban azonos szintű, jogi úton érvényesíthető jogokat és kötelezettségeket, az adatkezelők és adatfeldolgozók számára azonos felelősséget, a személyes adatok kezelésének következetes nyomon követését, valamennyi tagállamban azonos szankciók alkalmazását, és a különböző tagállamok felügyeleti hatóságai közötti hatékony együttműködést. A belső piac megfelelő működése érdekében a személyes adatok Unión belüli szabad áramlását a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból nem szabad korlátozni vagy megtiltani. A mikro-, kis- és középvállalkozások sajátos helyzetének figyelembevétele érdekében a 250 főnél kevesebb személyt foglalkoztató szervezetek esetében e rendelet a nyilvántartás vezetése tekintetében eltérést tartalmaz. Emellett, e rendelet alkalmazása során az uniós intézményeket és szerveket, és a tagállamokat és azok felügyeleti hatóságait ösztönözni kell, hogy vegyék figyelembe a mikro-, kis- és középvállalkozások sajátos szükségleteit. A mikro-, kis- és középvállalkozások fogalma kapcsán a 2003/361/EK bizottsági ajánlás (5) mellékletének 2. cikkét kell alapul venni.

(14) A természetes személyeket a személyes adataik kezelésével kapcsolatban e rendelet alapján nyújtott védelem állampolgárságuktól és lakóhelyüktől függetlenül megilleti. E rendelet hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre, illetve amely különösen olyan vállalkozásokra vonatkozik, amelyeket jogi

Azonosító	Leírás	Formátum			
NAIH_12STEP	A NAIH rövid grafikus iránymutatása	PDF	✓	✓	✓

Azonosító	Leírás	Formátum			
TMSI_MEMO	Vezetőket tájékoztató levél	DOC	✓	✓	✓
TMSI_ISMER	GDPR ismertető vezetőknek	PDF	✓	✓	✓
TMSI_LEVEL	GDPR tájékoztató levél az alkalmazottaknak	DOC	✓	✓	✓
TMSI_WEB1	GDPR alapok, PPT/video ismertető (53 perc)	MP4	✓	✓	✓
TMSI_WEB2	Hogyan kezdjük? PPT/video ismertető (55 perc)	MP4	✓	✓	✓
TMSI_CHECK	Kérdőív, checklist	DOC	✗	✓	✓



XXX-Kft.

Dokumentum-cím	GDPR-ellenőrzőlista			
Dokumentum-azonosító	Verzió	Verzió-dátuma	Státusz	Oldal
A10_TMSI_CHECK	1.0	2017.-november-11.	végleges	3-of-4

15.	Az-érintett-hozzáférési-joga	Ez-a-cikk-foglalkozik-az-érintettek-azon-jogával,-hogy:-meggyőződjenek-arról,-hogy-személyes-adataik-kezelése-folyamatban-van-e-és-hozzáférjenek-bizonyos-adatokhoz. Az-információk,-amelyeket-meg-kell-adni: • az-adatkezelés-célja; • adatkategóriák; • adatok-címzettjei; • adattárolási-idő; • a-helyesbítéshez,-korlátozáshoz-és-tiltakozáshoz-való-jog; • hatósági-panasz-benyújtásának-joga; • adatforrás; • az-automatizált-feldolgozás,-a-kapcsolódó-logika-és-következmények; biztosítékok-harmadik-országok-vagy-nemzetközi-szervezetek-számára-történő-átadás-esetén.		
16.	A-helyesbítéshez-való-jog	Ez-a-cikk-foglalkozik-az-érintettek-azon-jogával,-hogy-a-róla-tárolt-pontatlan-adatokat-helyesbítsék.		
17.	A-törléshez-való-jog-(„az-elfeledtetéshez-való-jog")	Ez-a-cikk-foglalkozik-az-érintettek-azon-jogával,-hogy-az-adatkezelőtől-bizonyos-feltételek-alapján-kérni-lehessen-a-személyes-adatok-törlését.		
18.	Az-adatkezelés-korlátozásához-való-jog	Ez-a-cikk-foglalkozik-az-adatalany-azon-jogával,-hogy-korlátozza-a-személyes-adatok-feldolgozását-olyan-esetekben-amikor-a-jogalap-vagy-az-adatok-pontossága-vitatott.		
19.	A-személyes-adatok-helyesbítéséhez-vagy-törléséhez,-illetve-az-adatkezelés-korlátozásához-kapcsolódó-értesítési-kötelezettség	Ez-a-cikk-arra-kötelezi-a-adatkezelőt,-hogy-értesítse-az-adatok-címzettjeit-(a-harmadik-feleket!)-a-feldolgozás-helyreigazításáról,-törléséről-vagy-korlátozásáról.		
20.	Az-adathordozhatósághoz-való-jog	Ez-a-cikk-az-érintettek-számára-bizonyos-körülmények-között-jogosultságot-biztosít-arra,-hogy-az-őt-érintő-személyes-adatokat-strukturált,-általánosan-használt-és-gépileg-olvasható-formában-megkapja,-és-továbbítsa-ezeket-az-adatokat-egy-másik-adatkezelőnek. Az-érintett-jogosult-arra,-hogy-–-ha-ez-technikailag-megvalósítható-–-kérje-a-személyes-adatok-adatkezelők-közötti-közvetlen-továbbítását.		
21.	A-tiltakozáshoz-való-jog	Ez-a-cikk-az-adatalanyok-azon-jogával-foglalkozik,-hogy-kifogásolja-személyes-adatainak-feldolgozását. Ha-az-adatalany-kifogást-emel,-az-adatkezelőnek-meg-kell-szüntetnie-a-személyes-adatok-feldolgozását,-kivéve,-ha-az-adatkezelő-bizonyítja,-hogy-az-adatkezelést-olyan-kényszerítő-erejű-jogos-okok-indokolják,-amelyek-elsőbbséget-élveznek-az-érintett-érdekeivel,-jogaival-és-szabadságaival-szemben,-vagy-amelyek-jogi-igények-előterjesztéséhez,-érvényesítéséhez-vagy-védelméhez-		

©-TMSI-Kft.-2017- XXX-Kft.

XXX-Kft.

Dokumentum-cím	GDPR-ellenőrzőlista			
Dokumentum-azonosító	Verzió	Verzió-dátuma	Státusz	Oldal
A10_TMSI_CHECK	1.0	2017.-november-11.	végleges	4-of-4

		kapcsolódnak-(a-közvetlen-marketing-feldolgozásra-nem-vonatkozik-kivétel).		
22.	Automatizált-döntéshozatal-egyedi-ügyekben,-beleértve-a-profilalkotást	Ez-a-cikk-foglalkozik-az-érintettek-azon-jogával,-hogy-ne-kizárólag-az-automatizált-feldolgozáson-alapuló-határozat-tárgyát-képezzék,-amennyiben-az-ilyen-döntések-jogi-vagy-jelentős-hatást-gyakorolnak-rá.		
24.	Az-adatkezelő-feladatai	A-24.-cikk-előírja-az-adatkezelő-számára,-hogy-megfelelő-technikai-és-szervezeti-intézkedéseket-hajtson-végre-annak-érdekében,-hogy-biztosítsa-és-képes-legyen-bizonyítani-a-GDPR-nek-való-megfelelést. Ezeknek-az-intézkedéseknek-a-megfelelősége-olyan-kockázatértékelésen-alapul,-amely-figyelembe-veszi-a-feldolgozás-jellegét,-terjedelmét,-összefüggéseit-és-céljait,-valamint-az-egyének-jogait-és-szabadságait-érintő-eltérő-valószínűséggel-és-súlyossággal-járó-kockázatokat. Külön-utalás-van-arra,-hogy-amennyiben-a-feldolgozási-tevékenységekkel-(kockázattal)-arányos,-úgy-belső-adatvédelmi-szabályokat-kell-alkalmazni.		
25.	Beépített-és-alapértelmezett-adatvédelem	Ez-a-cikk-új-feladatokat-ad-az-adatkezelő-számára,-és-adatvédelmi-szempontok-szerinti-tervezési-és-alapértelmezést-igényel. Az-adatkezelőknek-a-feldolgozás-módjainak-meghatározásakor-és-a-feldolgozás-során-megfelelő-technikai-és-szervezési-intézkedéseket-(pl.-álnevesítést)-kell-alkalmazniuk-az-5.-cikkben-meghatározott-adatvédelmi-elvek-(mint-például-az-adatok-minimalizálása)-végrehajtására-és-be-kell-építeniük-a-szükséges-biztosítékokat-a-feldolgozásba,-hogy-megfeleljenek-a-GDPR-követelményeinek. Az-adatkezelőknek-az-alapértelmezés-szerinti-adatvédelmet-is-alkalmazniuk-kell,-azaz-megfelelő-technikai-és-szervezeti-intézkedéseket-kell-végrehajtaniuk-annak-biztosítására,-hogy-alapértelmezés-szerint-csak-az-egyes-konkrét-célokhoz-szükséges-személyes-adatokat-dolgozzák-fel.-A-"szükséges"-fogalom-szabályozza-az-összegyűjtött-adatok-mennyiségét,-a-feldolgozás-mértékét,-valamint-az-adatok-megőrzését-és-hozzáférhetőségét. Különösen-az-érintett-beavatkozásának-hiányában-az-ellenőröknek-biztosítaniuk-kell,-hogy-a-személyes-adatok-ne-legyenek-elérhetőek-indokolatlan-személyek-számára.		

©-TMSI-Kft.-2017- XXX-Kft.

IN NUCE

Dióhéjban a GDPR: EU általános adatvédelmi rendeletére való felkészülési folyamatát segítő anyagok összesége.

www.tmsi.hu/in-nuce · (+361) 321-0631 · innuce@tmsi.hu

Azonosító	Leírás	Formátum			
TMSI_TODO	Cselekvési terv	DOC	✓	✓	✓

A·CsT·felülvizsgálatára·az·alábbiak·szerint·kerül·sor:¶

- → évente·egy·alkalommal,·a·belső·felülvizsgálatok·során,¶
- → minden·olyan·esetben,·amikor·a·leírtakhoz·képest·jelentős·változás·történik.¶

A·mindenkori·felülvizsgálat·végrehajtása·az·Informatikai·felelős·feladatát·jelenti.¶

1.3 → Kapcsolódó·dokumentumok¶

A·CsT·elkészítéséhez·felhasznált·dokumentumok¶

- → EU·rendelet·[1]¶

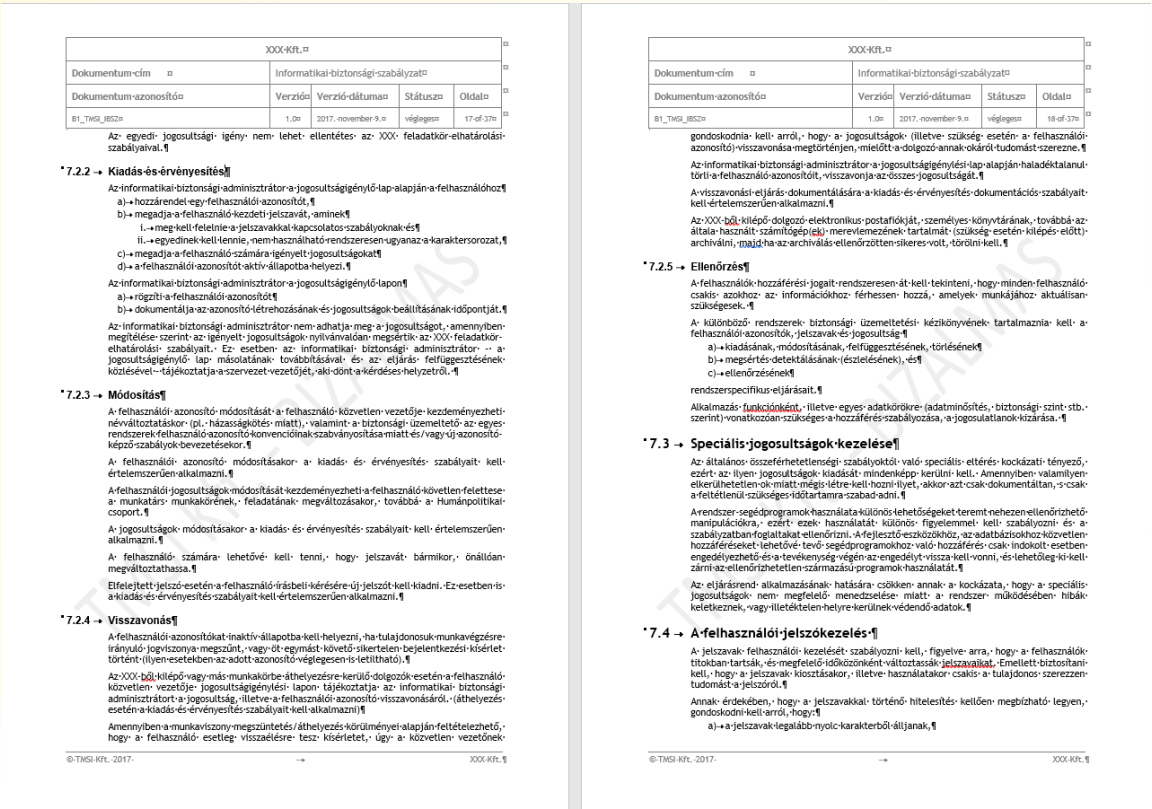
2 → Cselekvési·terv¶

Az·XXX·vezetése·elkötelezett,·hogy·olyan·összetett·és·biztonságos·informatikai·környezetet·alakítson· ki· és· működtessen,· mely· segítségével· kellő· biztonsággal,· ugyanakkor· rugalmassággal·tudja·kezelni·a·reá·bízott·és·saját·információkat.·¶

Ennek·érdekében,·ezeket·a·stratégiai·célokat·az·alábbi·ütemezéssel·kívánja·megvalósítani:¶

Sorszám:	Cél	Felelős	Határidő
1.	Informatikai·politika·kialakítása,·elfogadása	Kovács·János	2017.·december
2.	Adatvédelmi·tisztviselő·kijelölése	Igazgató	2017.·december
3.	Az·XXX·adatvagyonának·felmérése,·adatosztályozás	Kovács·János	2018.·január
4.	Informatikai·(biztonsági)·szabályzat·felülvizsgálata,·elfogadása	Kovács·János	2018.·január
5.	Nyilvános·adatkezelési·anyagok·(tájékoztató,·űrlapok,·stb.)·módosítása,·publikálása	Kovács·János	2018.·január
6.	Az·adatkezelési·tevékenységek·nyilvántartása	Kovács·János	2018.·január
7.	Informatikai·kockázatelemzés	Kovács·János	2018.·február
8.	Szabályzat·az·[illegible]·adatainak·kérésének·	Kovács·János	2018.·január
9.	[illegible]	Kovács·János	2018.·március
10.	[illegible]	Kovács·János	2018.·április
11.	Ada[illegible]	Kovács·János	2018.·január
12.	Új·szer[illegible]	Kovács·János	2018.·január
13.	[illegible]	Kovács·János	2018.·május
14.	A[illegible]	Kovács·János	2018.·május
15.	[illegible]	Kovács·János	2018.·június
16.	A[illegible]	Kovács·János	2018.·július
17.	[illegible] növelése	Kovács·János	2018.·július
18.	Kül[illegible]	Kovács·János	2018.·július
19.	[illegible]	Kovács·János	2018.·március
20.	[illegible] bevezetése	Kovács·János	2018.·április

Azonosító	Leírás	Formátum			
TMSI_IBSZ	Informatikai biztonsági szabályzat, benne	DOC	✓	✓	✓
TMSI_IBSZ	Kockázatelemzési eljárásrend	DOC	✗	✗	✓
TMSI_IBSZ	Adatkezelési eljárásrend	DOC	✓	✓	✓
TMSI_IBSZ	Adatvédelmi hatásvizsgálati eljárásrend	DOC	✗	✗	✓
TMSI_IBSZ	Jogosultságkezelés	DOC	✗	✗	✓
TMSI_IBSZ	Adatmentési eljárásrend	DOC	✓	✓	✓
TMSI_IBSZ	Incidenskezelési eljárásrend	DOC	✓	✓	✓
TMSI_IBSZ	Adatkezelési kérés- és panaszkezelés	DOC	✓	✓	✓
TMSI_IBSZ	Oktatás, számítógéphasználati elvek	DOC	✗	✓	✓
TMSI_IBSZ	Ellenőrzési eljárásrend	DOC	✓	✓	✓



XXX-Kft.

Dokumentum-cím	Informatikai-biztonsági-szabályzat			
Dokumentum-azonosító	Verzió	Verzió-dátuma	Státusz	Oldal
B1_TMSI_IBSZ	1.0	2017.-november-9.	végleges	17-of-37

Az egyedi jogosultsági igény nem lehet ellentétes az XXX feladatkör-elhatárolási szabályaival.

7.2.2 Kiadás-és-érvényesítés

Az informatikai-biztonsági-adminisztrátor-a-jogosultságigénylő-lap-alapján-a-felhasználóhoz

a) hozzárendel-egy-felhasználói-azonosítót,
b) megadja-a-felhasználó-kezdeti-jelszavát, aminek
   i. meg-kell-felelnie-a-jelszavakkal-kapcsolatos-szabályoknak-és
   ii. egyedinek-kell-lennie, -nem-használható-rendszeresen-ugyanaz-a-karaktersorozat,
c) megadja-a-felhasználó-számára-igényelt-jogosultságokat
d) a-felhasználói-azonosítót-aktív-állapotba-helyezi.

Az-informatikai-biztonsági-adminisztrátor-a-jogosultságigénylő-lapon

a) rögzíti-a-felhasználói-azonosítót
b) dokumentálja-az-azonosító-létrehozásának-és-jogosultságok-beállításának-időpontját.

Az-informatikai-biztonsági-adminisztrátor-nem-adhatja-meg-a-jogosultságot, -amennyiben-megítélése-szerint-az-igényelt-jogosultságok-nyilvánvalóan-megsértik-az-XXX-feladatkör-elhatárolási-szabályait. Ez- esetben- az- informatikai- biztonsági- adminisztrátor- -- a- jogosultságigénylő- lap- másolatának- továbbításával- és- az- eljárás- felfüggesztésének- közlésével- -tájékoztatja-a-szervezet-vezetőjét, -aki-dönt-a-kérdéses-helyzetről.

7.2.3 Módosítás

A-felhasználói-azonosító-módosítását-a-felhasználó-közvetlen-vezetője-kezdeményezheti-névváltoztatáskor-(pl.-házasságkötés-miatt), -valamint-a-biztonsági-üzemeltető-az-egyes-rendszerek-felhasználó-azonosító-konvencióinak-szabványosítása-miatt-és/vagy-új-azonosító-képző-szabályok-bevezetésekor.

A- felhasználói- azonosító- módosításakor- a- kiadás- és- érvényesítés- szabályait- kell- értelemszerűen-alkalmazni.

A-felhasználói-jogosultságok-módosítását-kezdeményezheti-a-felhasználó-követlen-felettese-a- munkatárs- munkakörének, -feladatának- megváltozásakor, -továbbá- a- Humánpolitikai-csoport.

A- jogosultságok- módosításakor- a- kiadás- és- érvényesítés- szabályait- kell- értelemszerűen-alkalmazni.

A- felhasználó- számára- lehetővé- kell- tenni, -hogy- jelszavát- bármikor, -önállóan-megváltoztathassa.

Elfelejtett-jelszó-esetén-a-felhasználó-írásbeli-kérésére-új-jelszót-kell-kiadni. -Ez-esetben-is-a-kiadás-és-érvényesítés-szabályait-kell-értelemszerűen-alkalmazni.

7.2.4 Visszavonás

A-felhasználói-azonosítókat-inaktív-állapotba-kell-helyezni, -ha-tulajdonosuk-munkavégzésre-irányuló- jogviszonya- megszűnt, -vagy- őt- egymást- követő- sikertelen- bejelentkezési- kísérlet- történt- (ilyen-esetekben-az-adott-azonosító-véglegesen-is-letiltható).

Az-XXX-ből-kilépő-vagy-más-munkakörbe-áthelyezésre-kerülő-dolgozók-esetén-a-felhasználó-közvetlen- vezetője- jogosultságigénylési- lapon- tájékoztatja- az- informatikai- biztonsági-adminisztrátort-a-jogosultság, -illetve-a-felhasználói-azonosító-visszavonásáról. -(áthelyezés-esetén-a-kiadás-és-érvényesítés-szabályait-kell-alkalmazni)

Amennyiben-a-munkaviszony-megszüntetés/áthelyezés-körülményei-alapján-feltételezhető, -hogy- a- felhasználó- esetleg- visszaélésre- tesz- kísérletet, -úgy- a- közvetlen- vezetőnek-

XXX-Kft.

Dokumentum-cím	Informatikai-biztonsági-szabályzat			
Dokumentum-azonosító	Verzió	Verzió-dátuma	Státusz	Oldal
B1_TMSI_IBSZ	1.0	2017.-november-9.	végleges	18-of-37

gondoskodnia- kell- arról, -hogy- a- jogosultságok- (illetve- szükség- esetén- a- felhasználói-azonosító)-visszavonása-megtörténjen, -mielőtt-a-dolgozó-annak-okáról-tudomást-szerezne.

Az-informatikai-biztonsági-adminisztrátor-a-jogosultságigénylési-lap-alapján-haladéktalanul-törli-a-felhasználó-azonosítóit, -visszavonja-az-összes-jogosultságát.

A-visszavonási-eljárás-dokumentálására-a-kiadás-és-érvényesítés-dokumentációs-szabályait-kell-értelemszerűen-alkalmazni.

Az-XXX-ből-kilépő-dolgozó-elektronikus-postafiókját, -személyes-könyvtárának, -továbbá-az-általa-használt-számítógép(ek)-merevlemezének-tartalmát-(szükség-esetén-kilépés-előtt)-archiválni, -majd-ha-az-archiválás-ellenőrzötten-sikeres-volt, -törölni-kell.

7.2.5 Ellenőrzés

A-felhasználók-hozzáférési-jogait-rendszeresen-át-kell-tekinteni, -hogy-minden-felhasználó-csakis- azokhoz- az- információkhoz- férhessen- hozzá, -amelyek- munkájához- aktuálisan-szükségesek.

A- különböző- rendszerek- biztonsági- üzemeltetési- kézikönyvének- tartalmaznia- kell- a-felhasználói-azonosítók, -jelszavak-és-jogosultság

a) kiadásának, -módosításának, -felfüggesztésének, -törlésének
b) megsértés-detektálásának-(észlelésének), -és
c) ellenőrzésének

rendszerspecifikus-eljárásait.

Alkalmazás- funkciónként, -illetve- egyes- adatkörökre- (adatminősítés, -biztonsági- szint- stb.- szerint)-vonatkozóan-szükséges-a-hozzáférés-szabályozása, -a-jogosulatlanok-kizárása.

7.3 Speciális-jogosultságok-kezelése

Az- általános- összeférhetetlenségi- szabályoktól- való- speciális- eltérés- kockázati- tényező, -ezért- az- ilyen- jogosultságok- kiadását- mindenképp- kerülni- kell. - Amennyiben- valamilyen-elkerülhetetlen-ok-miatt-mégis-létre-kell-hozni-ilyet, -akkor-azt-csak-dokumentáltan, -s-csak-a-feltétlenül-szükséges-időtartamra-szabad-adni.

A-rendszer-segédprogramok-használata-különös-tehetőségeket-teremt-nehezen-ellenőrizhető-manipulációkra, -ezért- ezek- használatát- különös- figyelemmel- kell- szabályozni- és- a-szabályzatban-foglaltakat-ellenőrizni. -A-fejlesztő-eszközökhöz, -az-adatbázisokhoz-közvetlen-hozzáféréseket-lehetővé-tevő-segédprogramokhoz- való-hozzáférés- csak- indokolt- esetben-engedélyezhető-és-a-tevékenység-végén-az-engedélyt-vissza-kell-vonni, -és-lehetőleg-ki-kell-zárni-az-ellenőrizhetetlen-származású-programok-használatát.

Az- eljárásrend- alkalmazásának- hatására- csökken- annak- a- kockázata, -hogy- a- speciális-jogosultságok- nem- megfelelő- menedzselése- miatt- a- rendszer- működésében- hibák-keletkeznek, -vagy-illetéktelen-helyre-kerülnek-védendő-adatok.

7.4 A-felhasználói-jelszókezelés

A- jelszavak- felhasználói- kezelését- szabályozni- kell, -figyelve- arra, -hogy- a- felhasználók-titokban-tartsák, -és-megfelelő-időközönként-változtassák-jelszavaikat. -Emellett-biztosítani-kell, -hogy- a- jelszavak- kiosztásakor, -illetve- használatakor- csakis- a- tulajdonos- szerezzen-tudomást-a-jelszóról.

Annak- érdekében, -hogy- a- jelszavakkal- történő- hitelesítés- kellően- megbízható- legyen, -gondoskodni-kell-arról, -hogy:

a) a-jelszavak-legalább-nyolc-karakterből-álljanak,

Azonosító	Leírás	Formátum			
TMSI_BCP	Üzletmenet-folytonossági terv (BCP)	DOC	✖	✖	✓

6 → Kapacitástervezés

Az XXX-nek meg kell tervezni a folyamatos működéshez szükséges információ-feldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.

6.1 → Az alapfeladatok és alapfunkciók folyamatossága

Az alapfeladatok és alapfunkciók folyamatosságát úgy kell megtervezni, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő, fenntartható legyen a folyamatosság az elektronikus információs rendszer elsődleges feldolgozó-vagy tárolási helyszínén történő teljes helyreállításáig.

Ezek a visszaállítási célkitűzések (RTO-k) az 1. számú mellékletben vannak rendszerenként pontosítva.

6.2 → Tartalék eszközök

Az XXX jelenleg merevlemezekből rendelkezik tartalékokkal. A tartalék szerver, illetve switch beszerzése rövid távon tervezett.

Az XXX az informatikai rendszerek működésfolytonossága szempontjából kritikus elemként azonosította az alábbi informatikai eszközöket:

Visszaállítási prioritás/sorrend	Támogatott üzleti folyamat
1.	LAN/WAN hálózat
2.	Tűzfal
3.	Active Directory központi címtár
4.	Exchange
5.	Számlázó rendszer
6.	Főkönyvi rendszer

6.3 → Tartalék feldolgozási helyszín

Az XXX:

- kijelöl egy tartalék feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésére, a tartalék helyszínen újra kezdhesse, vagy folytathassa;
- biztosítja, hogy a működés újrakezdéséhez vagy folytatásához szükséges eszközök és feltételek a tartalék feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak;
- biztosítja, hogy a tartalék feldolgozási helyszín informatikai biztonsági intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.

A tartalék feldolgozási helyszínre vonatkozóan olyan megállapodásokat kell kötni, intézkedéseket kell bevezetni, amelyek a szervezet rendelkezésre állási követelményeivel

(köztük a helyreállítási idő célokkal) összhangban álló szolgáltatás-prioritási rendelkezéseket tartalmaznak.

Az XXX úgy készíti fel a tartalék feldolgozási helyszínt, hogy az a visszaállítási célkitűzésekben meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.

Az XXX a Budapest, Benczúr utca 43. telephelyen található géptermet jelöli ki biztonsági feldolgozási helyszínként, ahol az elektronikus információs rendszer mentéseinek másolatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja. Ez a helyszín elkülönül az elsődleges feldolgozás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

6.4 → Biztonsági tárolási helyszín

Az XXX a Budapest, Naspolya u. 23. központi telephelyen található géptermet jelöli ki biztonsági tárolási helyszínként, ahol az elektronikus információs rendszer mentéseinek másolatát az elsődleges helyszínnel azonos módon, és biztonsági feltételek mellett tárolja.

Ez a helyszín elkülönül az elsődleges tárolás helyszínétől, az azonos veszélyektől való érzékenység csökkentése érdekében.

6.5 → Tartalék kommunikációs vonalak

Az XXX tartalék infokommunikációs szolgáltatásokat létesít, erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az elektronikus információs rendszer alapfunkcióit, vagy meghatározott műveletek számára azok meghatározott időtartamon belüli újrakezdését, amennyiben az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

Olyan tartalék infokommunikációs szolgáltatásokat kell igénybe venni, melyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét (pl. alternatív technológiára épülnek).

Azonosító	Leírás	Formátum			
TMSI_ADATEV	Az adatkezelési tevékenységek nyilvántartása	XLS	✓	✓	✓
TMSI_ADATLEL	Nyilvántartás a személyes adatok kezeléséről (adatleltár)	XLS	✓	✓	✓
TMSI_INCID	Az adatvédelmi incidensek nyilvántartása	XLS	✗	✓	✓
TMSI_SARLOG	Az érintettek/adatalanyok kéréseinek naplója	XLS	✗	✓	✓
TMSI_SARLEV	Az adatalanyok kéréseire adott válaszlevél	DOC	✗	✗	✓

C12

2016/679 EU rendelet

30. cikk: Az adatkezelési tevékenységek nyilvántartása

(1) Minden adatkezelő és - ha van ilyen - az adatkezelő képviselője a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet.

"Az ebben a bekezdésben foglalt kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira é
a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó szem

Szám	Az adatkezelő neve és elérhetősége	Az adatkezelés céljai	Az érintettek kategóriái	A személyes adatok kategóriái	Címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják (ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket)	A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk (a harmadik ország vagy a nemzetközi szervezet azonosítása)	A különböző ad előirányzott ha
1.	XXX Kft., 70-1234567, info@xxx.hu	Hírlevél küldés	Szerződött ügyfelek: felnőtt magánszemélyek	Név, keresztnév, e-mail cím	A jelzett adatokat nem adjuk tovább harmadik félnek.	A jelzett adatokat nem adjuk tovább harmadik félnek.	Minden jelzett automatikusan
2.	XXX Kft., 70-1234567, info@xxx.hu	Szerződéses kötelezettségek teljesítése	Szerződött ügyfelek: felnőtt magánszemélyek	Név, keresztnév, e-mail cím, telefonszám, postai cím.	A jelzett adatokat fizetési késedelm esetén követelésbehajtónak átadhatjuk.	A jelzett adatokat nem adjuk tovább harmadik félnek.	A jelzett adato lezárása után 1

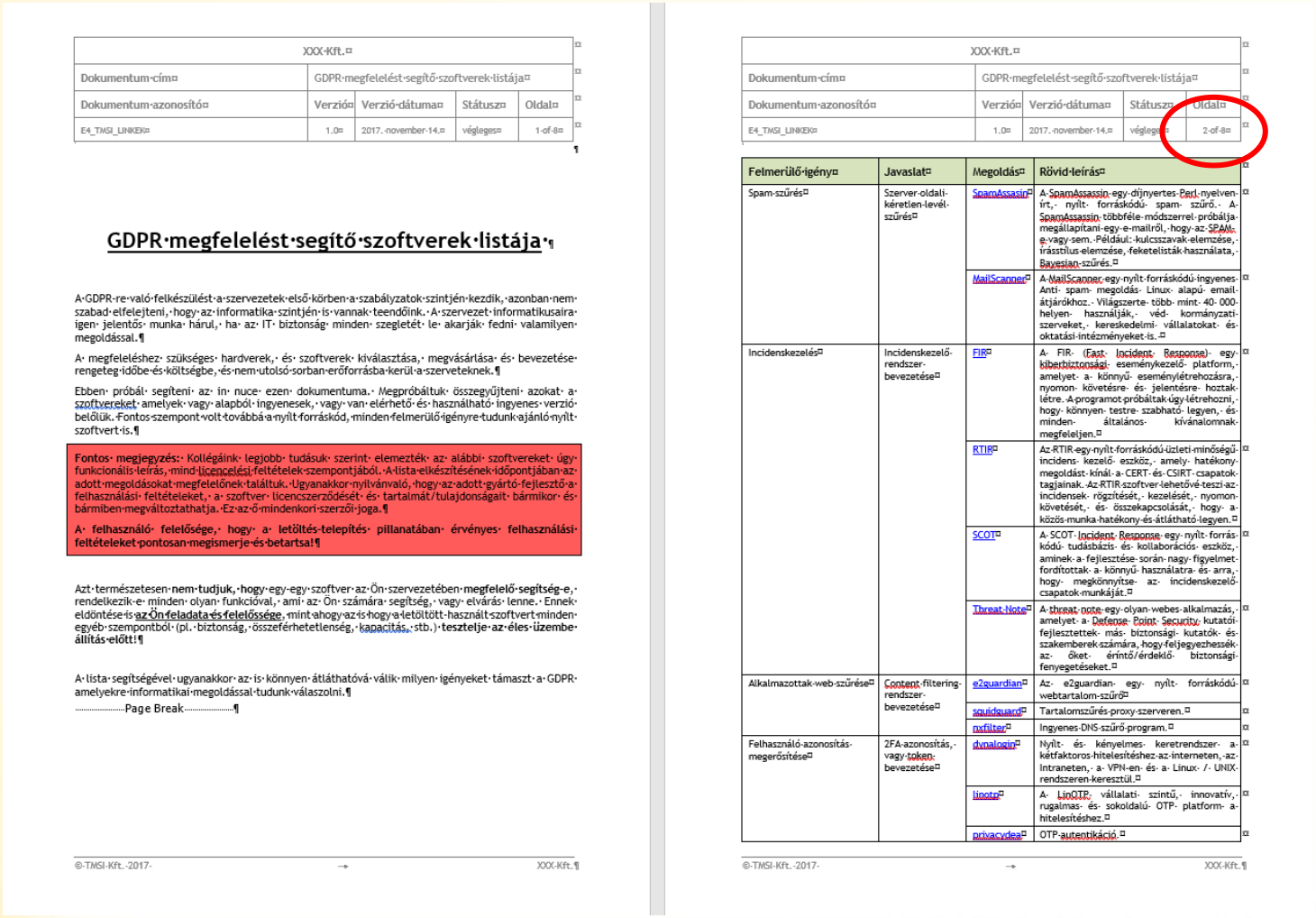
Azonosító	Leírás	Formátum			
TMSI_TAJEKOZ	Adatkezelési tájékoztató honlapra	DOC	✓	✓	✓
TMSI_HOZZA	Adatkezelési hozzájárulási űrlap	DOC	×	✓	✓
TMSI_SAR	Adatkezelési kérelmi űrlap	DOC	×	×	✓

ÉRINTETT KÉRELMI ŰRLAP

1. A kérelmező adatai

2. Az eljáró adatai

Azonosító	Leírás	Formátum			
TMSI_TRAIN	Belső adatkezelési figyelemfelkeltő tréning (teszt kérdésekkel)	DOC	✗	✗	✓
TMSI_SOPH1	GDPR általános ismertető (Sophos Whitepaper)	PDF	✓	✓	✓
TMSI_SOPH2	Rövid titkosítási útmutató (Sophos Whitepaper, angolul)	PDF	✓	✓	✓
TMSI_LINKEK	Linkek nyitott forráskódú (ingyenes) szoftverekhez amelyek segítséget jelenthetnek a GDPR-hez	PDF	✓	✓	✓



XXX-Kft.

Dokumentum-cím	GDPR-megfelelést-segítő-szoftverek-listája			
Dokumentum-azonosító	Verzió	Verzió-dátuma	Státusz	Oldal
E4_TMSI_LINKEK	1.0	2017.-november-14.	végleges	1-of-8

GDPR-megfelelést-segítő-szoftverek-listája

A-GDPR-re-való-felkészülést-a-szervezetek-első-körben-a-szabályzatok-szintjén-kezdik,-azonban-nem-szabad-elfelejteni,-hogy-az-informatika-szintjén-is-vannak-teendőink.-A-szervezet-informatikusaira-igen-jelentős-munka-hárul,-ha-az-IT-biztonság-minden-szegletét-le-akarják-fedni-valamilyen-megoldással.

A-megfeleléshez-szükséges-hardverek,-és-szoftverek-kiválasztása,-megvásárlása-és-bevezetése-rengeteg-időbe-és-költségbe,-és-nem-utolsó-sorban-erőforrásba-kerül-a-szervezeteknek.

Ebben-próbál-segíteni-az-in-nuce-ezen-dokumentuma.-Megpróbáltuk-összegyűjteni-azokat-a-szoftvereket-amelyek-vagy-alapból-ingyenesek,-vagy-van-elérhető-és-használható-ingyenes-verzió-belőlük.-Fontos-szempont-volt-továbbá-a-nyílt-forráskód,-minden-felmerülő-igényre-tudunk-ajánló-nyílt-szoftvert-is.

Fontos-megjegyzés:-Kollégáink-legjobb-tudásuk-szerint-elemezték-az-alábbi-szoftvereket-úgy-funkcionális-leírás,-mind-licencelési-feltételek-szempontjából.-A-lista-elkészítésének-időpontjában-az-adott-megoldásokat-megfelelőnek-találtuk.-Ugyanakkor-nyilvánvaló,-hogy-az-adott-gyártó-fejlesztő-a-felhasználási-feltételeket,-a-szoftver-licencszerződését-és-tartalmát/tulajdonságait-bármikor-és-bárhiben-megváltoztathatja.-Ez-az-ő-mindenkori-szerzői-joga.

A-felhasználó-felelősége,-hogy-a-letöltés-telepítés-pillanatában-érvényes-felhasználási-feltételeket-pontosan-megismerje-és-betartsa!

Azt-természetesen-**nem-tudjuk,-hogy**-egy-egy-szoftver-az-Ön-szervezetében-**megfelelő-segítség-e,**-rendelkezik-e-minden-olyan-funkcióval,-ami-az-Ön-számára-segítség,-vagy-elvárás-lenne.-Ennek-eldöntése-is-**az-Ön-feladata-és-felelőssége**,-mint-ahogy-az-is-hogy-a-letöltött-használt-szoftvert-minden-egyéb-szempontból-(pl.-biztonság,-összeférhetetlenség,-kapacitás,-stb.)-**tesztelje-az-éles-üzembe-állítás-előtt!**

A-lista-segítségével-ugyanakkor-az-is-könnyen-átláthatóvá-válik-milyen-igényeket-támaszt-a-GDPR-amelyekre-informatikai-megoldással-tudunk-válaszolni.

Page Break

XXX-Kft.

Dokumentum-cím	GDPR-megfelelést-segítő-szoftverek-listája			
Dokumentum-azonosító	Verzió	Verzió-dátuma	Státusz	Oldal
E4_TMSI_LINKEK	1.0	2017.-november-14.	végleges	2-of-8

Felmerülő-igény	Javaslat	Megoldás	Rövid-leírás
Spam-szűrés	Szerver-oldali-kéretlen-levél-szűrés	SpamAssassin	A-SpamAssassin-egy-díjnyertes-Perl-nyelven-írt,-nyílt-forráskódú-spam-szűrő.-A-SpamAssassin-többféle-módszerrel-próbálja-megállapítani-egy-e-mailről,-hogy-az-SPAM-e-vagy-sem.-Például:-kulcsszavak-elemzése,-írásstílus-elemzése,-feketelisták-használata,-Bayesian-szűrés.
		MailScanner	A-MailScanner-egy-nyílt-forráskódú-ingyenes-Anti-spam-megoldás-Linux-alapú-email-átjárókhoz.-Világszerte-több-mint-40-000-helyen-használják,-véd-kormányzati-szerveket,-kereskedelmi-vállalatokat-és-oktatási-intézményeket-is.
Incidenskezelés	Incidenskezelő-rendszer-bevezetése	FIR	A-FIR-(Fast-Incident-Response)-egy-kiberbiztonsági-eseménykezelő-platform,-amelyet-a-könnyű-eseménylétrehozásra,-nyomon-követésre-és-jelentésre-hoztak-létre.-A-programot-próbáltak-úgy-létrehozni,-hogy-könnyen-testre-szabható-legyen,-és-minden-általános-kívánalomnak-megfeleljen.
		RTIR	Az-RTIR-egy-nyílt-forráskódú-üzleti-minőségű-incidens-kezelő-eszköz,-amely-hatékony-megoldást-kínál-a-CERT-és-CSIRT-csapatok-tagjainak.-Az-RTIR-szoftver-lehetővé-teszi-az-incidensek-rögzítését,-kezelését,-nyomon-követését,-és-összekapcsolását,-hogy-a-közös-munka-hatékony-és-átlátható-legyen.
		SCOT	A-SCOT-Incident-Response-egy-nyílt-forráskódú-tudásbázis-és-kollaborációs-eszköz,-aminek-a-fejlesztése-során-nagy-figyelmet-fordítottak-a-könnyű-használatra-és-arra,-hogy-megkönnyítse-az-incidenskezelő-csapatok-munkáját.
		Threat-Note	A-threat-note-egy-olyan-webes-alkalmazás,-amelyet-a-Defense-Point-Security-kutatói-fejlesztettek-más-biztonsági-kutatók-és-szakemberek-számára,-hogy-feljegyezhessék-az-őket-érintő/érdeklő-biztonsági-fenyegetéseket.
Alkalmazottak-web-szűrése	Content-filtering-rendszer-bevezetése	e2guardian	Az-e2guardian-egy-nyílt-forráskódú-webtartalom-szűrő
		squidguard	Tartalomszűrés-proxy-szerveren.
		nxfilter	Ingyenes-DNS-szűrő-program.
Felhasználó-azonosítás-megerősítése	2FA-azonosítás,-vagy-token-bevezetése	dvnalogin	Nyílt-és-kényelmes-keretrendszer-a-kétfaktoros-hitelesítéshez-az-interneten,-az-Intraneten,-a-VPN-en-és-a-Linux-/-UNIX-rendszeren-keresztül.
		linotp	A-LinOTP,-vállalati-szintű,-innovatív,-rugalmas-és-sokoldalú-OTP-platform-a-hitelesítéshez.
		privacydea	OTP-autentikáció.

IN NUCE

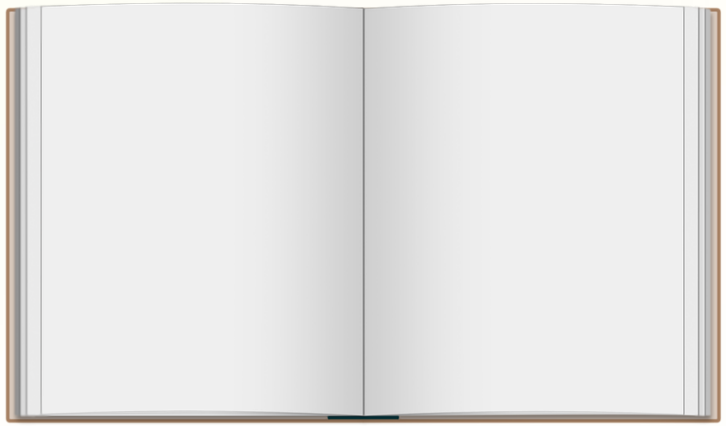
Dióhéjban a GDPR: EU általános adatvédelmi rendeletére való felkészülési folyamatát segítő anyagok összesége.

www.tmsi.hu/in-nuce · (+361) 321-0631 · innuce@tmsi.hu

in nuce = 100%-os GDPR megfelelés?

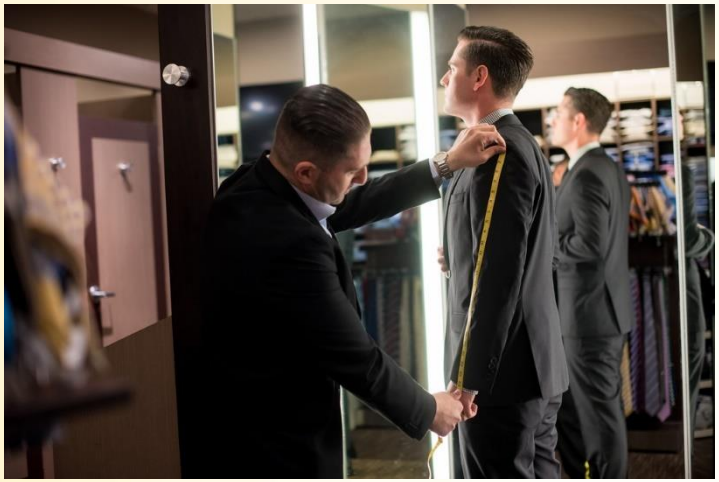
- Sajnos nem…
- Viszont:

>



in nuce = 100%-ban testreszabott?

- Sajnos nem…
- Viszont a költségei sem:



>

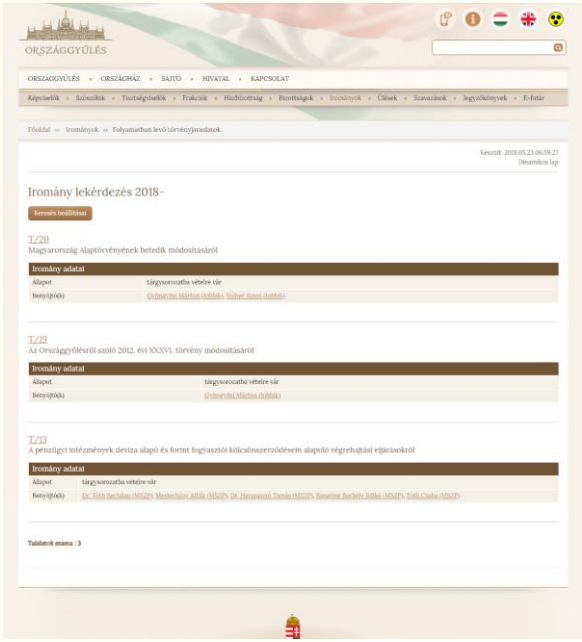
in nuce erősségei

- Egy helyen vannak a legszükségesebb anyagok
- **Nem** template, sablon, jogszabály-magyarázat: DOC+XLS!
- Magyarul, világosan, érthetően, útmutatókkal
- **TUDJUK, hogy mi nincs benne, mi lenne további segítség az ügyfeleinknek**

- Viszonylag
  - olcsón,
  - gyorsan, és
  - egyszerűen

  történhet meg a GDPR felkészülés.

Mi fog történni május 26. után?



Semmi és bármi…

Infotörvény és NAIH

Mi van ha:

- rossz helyre megy a mail
- elveszítenek egy USB-t
- ellopnak egy notebookot, telefont, tabletet
- zsarolóvírus
- trójai/… kiszivárgás
- adathalászat

… személyes adatokkal?

BKK esettanulmány

2017 július 13:

- megjelenik a BKK online jegyértékesítő rendszere
- a rendszer egy hétig elérhető
- 5000-en regisztrálnak
- 800-an vásárolnak 6 millió forintért
- több hullámban internetes támadás éri a r[illegible]szert

2017 július 14:

- Napközben megjelennek az első [illegible]molyabb hibákat


S

P, 14 júl. 2017 14:49:23 +0200 • ELKÜLDÖTT

"shop" <shop@bkk.hu>

Tags

Tisztelt Cím!

Biztonsági rést találtam a weboldalukon, a kosá
én akarok.. (50 forintért vettem havi bérletet)
Nem használtam fel a bérletet, célom világos és


index

VÁLASZTÁS 2018 | ELIOS-ÜGY | ÍGÉRETSZÁMLÁLÓ | OSCAR-DÍJ

BELFÖLD KÜLFÖLD GAZDASÁG TECH TUDOMÁNY KULT SPORT VÉLEMÉNY VIDEÓ FO

TECH | BKK | INFORMATIKA | KIBERBIZTONSÁG | FAIL | VÁSÁRLÁS | PROGRAMOZÁS | JEGY | JEGYVÁSÁRLÁS | BKK E-JEGY

Meghekkelhető a BKK rendszere, bármennyiért lehet jegyet venni

TÓTH BALÁZS

KÖVETÉS

2017.07.14. 16:31

Reggel teszteltük, hogy a BKK miként képzeli el a modern jegyértékesítést, és azóta is forranak a szervereink az olvasóktól érkező visszajelzésektől. Az egészben az a legkellemetlenebb, hogy a BKK értékesítési rendszerében nagyon durva biztonsági hibákat is találtak.

BKK esettanulmány

naih.hu/hatosagi-hatarozatok---vegzesek.html

2017. július 24: A 24.hu hírportál megküldte a NAIH részére a kiszivárgott adatokat.

2018. január 22: NAIH határozat

Nemzeti Adatvédelmi és Információszabadság Hatóság

Ügyszám: NAIH/2018/356/3/H.
Előzmény: NAIH/2017/3979/H

Tárgy: a BKK Budapesti Közlekedési Központ Zrt. adatkezelése

HATÁROZAT

A BKK Budapesti Közlekedési Központ Zrt. (1075 Budapest, Rumbach Sebestyén utca 19-21.) (a továbbiakban: Kötelezett) fenti számú ügyében a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) az alábbi döntéseket hozza:

1. A Hatóság megállapítja a Kötelezett jogellenes adatkezelését és felszólítja az alábbiakra:

- Az adatkezelés megkezdését megelőző tájékoztatási kötelezettségének megsértése miatt az adatkezelési tájékoztatási gyakorlatát az Infotv. rendelkezéseire figyelemmel módosítsa, és a jövőben adjon megfelelő tájékoztatást az adatalanyok részére.
- Az adatbiztonság követelményének megsértése miatt tegye meg a szükséges intézkedéseket annak érdekében, hogy az adatvédelmi incidens körülményeit, valószínűsíthető kockázatait feltárja, és ezekről a 2017. július 24. előtti időszakban regisztrált felhasználókat tájékoztassa.
- Megfelelően gondoskodjon az adatbiztonsági követelmények teljesítéséről, és ennek keretében alkosson meg az incidensek kezelésével kapcsolatos belső eljárásrendet, valamint a megbízott adatfeldolgozót is lássa el az ehhez szükséges utasításokkal, és ezeket írásban rögzítse az adatfeldolgozásra vonatkozó szerződésben.

2. A Hatóság a Kötelezettet továbbá

10.000.000 forint, azaz tízmillió forint
adatvédelmi bírság

megfizetésére kötelezi.

file	határozathozatal dátuma
.pdf	2018.01.22
.pdf	2017.10.24
.pdf	2017.07.07
.pdf	2017.10.13
.pdf	2017.10.13

BKK esettanulmány

NAIH Indoklásból:

- Kötelezett az adatbiztonsági követelményekkel összefüggésben úgy nyilatkozott, hogy „az adatbázis szervereket a rendszert szállító és üzemeltető TSM a saját maga által üzemeltetett infrastruktúrán tette lehetővé, **ezekhez a szerverekhez** a BKK Zrt. Informatikai Fejlesztés és Üzleti Támogatásnak **nincs hozzáférése**, …”
- A Kötelezett **nem azonosította adatvédelmi incidensként** a sajtóban megjelent azon eseményt, mely szerint az online jegyértékesítési rendszerből több ezer felhasználó személyes adatai kerülhettek illetéktelenek birtokába, ezzel kapcsolatban nem tett nyilatkozatot.
- A Hatóság több alkalommal nyilatkozatra hívta fel a Kötelezetett arra vonatkozóan, hogy **az adatkezeléssel kapcsolatban**, így például az adatbiztonsági intézkedésekről **milyen módon, és milyen tartalmú utasításokat adott** az általa megbízott adatfeldolgozónak, a TSM-nek.
- TSM tájékoztatta a Hatóságot … , hogy „az online jegyértékesítési rendszer adatbiztonsági vizsgálatára **2017. július 26**-án felkérte az Ernst & Young Tanácsadó Kft.-t, amely cég a megkötött szerződés keretében a BKK webes értékesítési rendszerének sérülékenység és adatszivárgás vizsgálatát, továbbá komplex IT biztonsági vizsgálatát végzi el.”
    - Az elkészült vizsgálati jelentést a TSM a 2017. szeptember 21-én kelt válaszához mellékelve megküldte a Hatóság részére, és tájékoztatta a Hatóságot arról, hogy abban rögzítésre kerültek a rendszerrel kapcsolatban feltárt sérülékenységek, ugyanakkor hangsúlyozta, hogy **a független tanácsadó társaság sem tárt fel az Infotv. szerinti adatvédelmi incidensre utaló jelet, bizonyítékot**.
- A Kötelezett a vizsgálati eljárás során tett, valamint a **2017. augusztus 17-én kelt válaszaiban nem azonosította adatvédelmi incidensként a sajtóban megjelent azon eseményt**, mely szerint az online jegyértékesítési rendszerből több ezer felhasználó személyes adatai kerülhettek illetéktelenek birtokába.
- … a Kötelezett **2017. szeptember 12-én** tekintett bele az adatvédelmi hatósági eljárás irataiba, … . Az iratbetekintést követően, **2017. szeptember 15-én** kelt válaszában a Kötelezett úgy nyilatkozott, hogy az iratbetekintés során megállapította, hogy a Hatóság részére a 24.hu hírportál által elküldött adatbázis azonos a Kötelezett online jegyértékesítési rendszerének adatbázisával, vagyis **történt adatvédelmi incidens**.
- A Hatóság **2017. október 25**-én kelt … a Kötelezett ismételten arról tájékoztatta a Hatóságot, hogy … az adatvédelmi incidenssel összefüggésben folytatott vizsgálat folyamatban van, mivel **továbbra sem tudta megállapítani pontosan az adatvédelmi incidens időpontját, körülményeit**, valamint az incidenssel érintett személyes adatok körét, az érintettek számát.

- A Hatóság az eljárás során megállapította, hogy a Kötelezett **nem differenciálta az adatkezelését** aszerint, hogy definiálja, **milyen tevékenységéhez kapcsolódóan milyen adatkezelési célt szükséges meghatároznia**, illetve ehhez kapcsolódóan **mi az adatkezelés jogalapja**.

Kérdés?

zoltan.tozser@tmsi.hu

https://www.tmsi.hu