ADAPTO

GDPR-
INFORMATIKAI MEGOLDÁSOK A JOGI MEGFELELÉS BIZTOSÍTÁSÁNAK ÉRDEKÉBEN

Pflanzner Sándor – ADAPTO Solutions

ISOFÓRUM Tavasz-2018. Konferencia

Kockázatelemzés követelménye a rendeletben

Az adatkezelő és az adatfeldolgozó ... a változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja .. :

- a személyes adatok álnevesítését és titkosítását
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- 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;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

ADAPTO

29-es mcs. állásfoglalása a hatásvizsgálatról

Az általános adatvédelmi rendelet (90) preambulumbekezdése az adatvédelmi hatásvizsgálat több olyan elemét is megjelöli, amely egybevág jól körülhatárolt kockázatkezelési elemekkel (lásd például az **ISO 31000** szabványt)

Az általános adatvédelmi rendelet szerinti adatvédelmi hatásvizsgálat **az érintettek jogait érintő kockázatok kezelésére szolgál**, így az ő szemszögükből készül, ahogy az bizonyos szakterületeken megfigyelhető (például társadalmi biztonság). Ugyanakkor más szakterületeken (például információbiztonság) a szervezet áll a középpontban.

ADAPTO

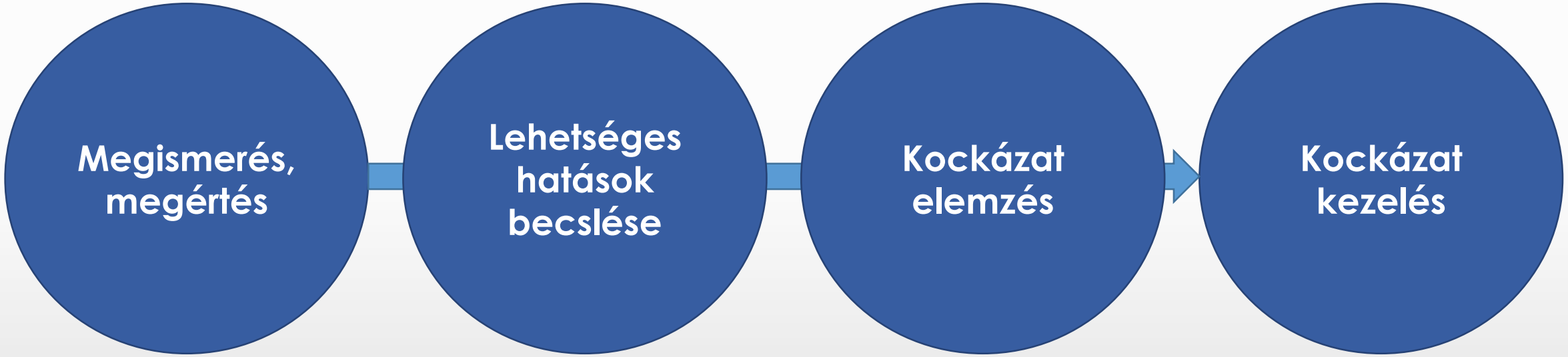
29-es mcs. állásfoglalása a hatásvizsgálatról

A kockázatkezelés szempontjából az adatvédelmi hatásvizsgálat célja, hogy **a természetes személyek jogait és szabadságait érintő "kockázatokat kezelje"** a következő eljárások felhasználásával:

- a körülmények meghatározása: „az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve";
- a kockázatok értékelése: „felmérje a magas kockázat különös valószínűségét és súlyosságát";
- a kockázatok orvoslása: „az említett kockázat mérséklését", „a személyes adatok védelmét" és „az e rendeletnek való megfelelés bizonyítását".

ADAPTO

A kockázatelemzés lépései

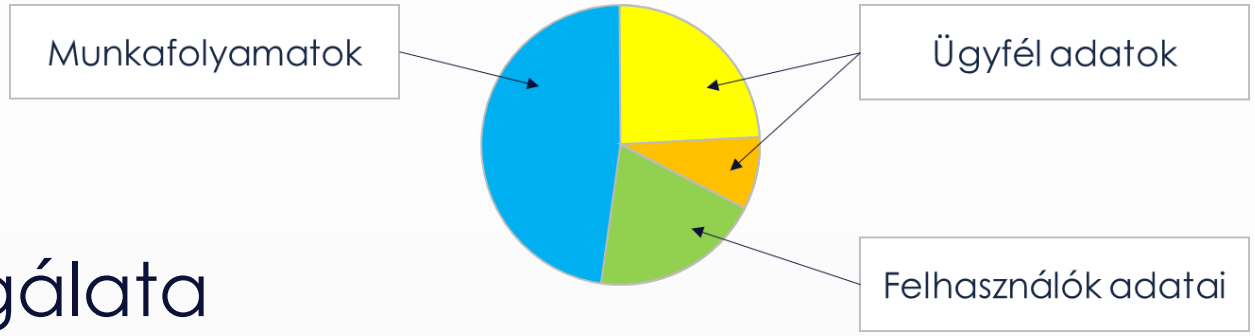


ADAPTO

GDPR módszertan
Érintett adatok körének meghatározása

Érintett adatok köre (az összes adatok közül)

- nem érintett
- személyes
- különleges személyes



A személyes adatok vizsgálata

- adatkezelés jogszerűsége
- célhoz kötöttségi elemzés
- érdekmérlegelési teszt

Adatkezelésbe bevontak köre

- adat kezelése (adatkezelő és feldolgozó)
- adatmegosztás

ADAPTO

GDPR módszertan
Adatvédelmi hatásvizsgálat

Jelentéktelen	Az elektronikus információs rendszer nem kezel jogszabályok által védett (pl.: személyes) adatot.
Csekély	Személyes adat sérülhet …
Közepes	Különleges személyes adat, vagy nagy tömegű személyes adatok sérülhetnek …
Nagy	Nagy tömegű különleges személyes adat sérülhet vagy a személyi sérülések esélye megnőhet (ideértve például a káresemény miatti ellátás elmaradását, a rendszer irányítatlansága miatti veszélyeket) ….
Kiemelkedően nagy	Kiemelten nagy tömegű különleges személyes adat sérül ….

ADAPTO

Kockázat = Hatás * Valószínűség

Hatás csökkentése

- Jogszerűség, célhoz kötöttség (érdekmérlegelés), adattakarékosság, korlátozott tárolhatóság, adatkezelők és feldolgozók azonosítása, adatmegosztás

Keretrendszer: GDPR

} Jogi szakterület

Valószínűség csökkentése

- Az adatot kiszolgáló infrastruktúra védelme

Keretrendszer: ISO 27001

} Informatikai szakterület

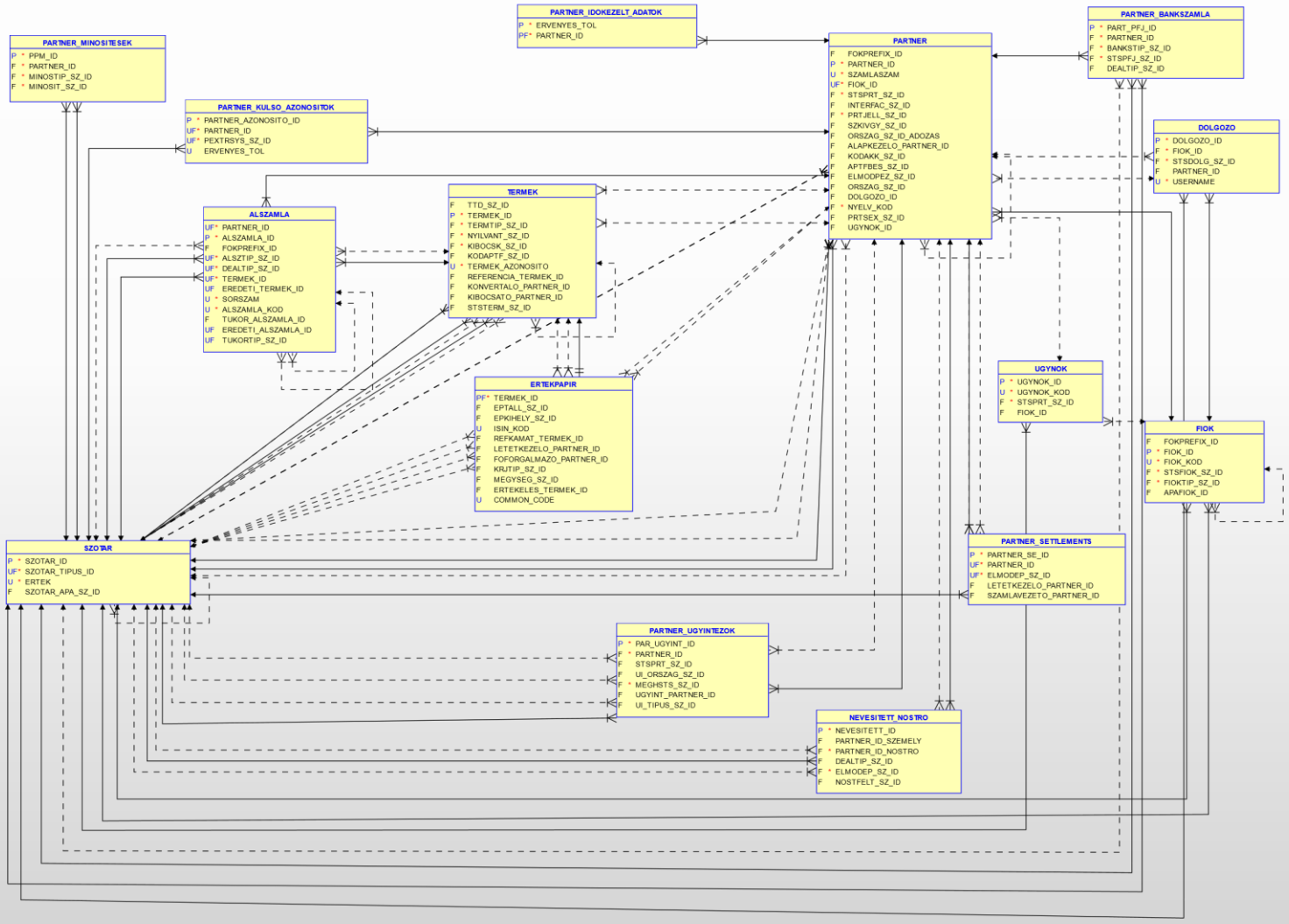
ADAPTO

Érintettek jogai – integrált vállalati rendszerben

1. Tájékoztatás: mit tart nyilván a cég az érintettről – ADAPTO + jogszabály ismertetése
2. Hozzáférés: adatkezelés tárgyát képező személyes adatok másolatát az érintettnek át kell adni –
   MIS rendszer
3. Helyesbítés: adatszinkronizálás, redundáns információk egységes munkafolyamatba szervezett módosítása –
   alkalmazói rendszerek
4. Törlés: tényleges törlés vagy felülírás, ha nem törölhető, meg kell védeni! (2.bekezdés) –
   alkalmazói rendszerek
5. Adatkezelés korlátozása: az érintett adatainak korlátozott felhasználása – alkalmazói rendszerek, valamint az adatot felhasználó munkafolyamat korlátozása
6. Adathordozás joga: adatexport készítése ismert formátumban) –
   alkalmazói rendszerek
7. Tiltakozás profilalkotás ellen, és az automatizált döntéshozatal eredménye ellen –
   munkafolyamatok átszervezése
8. Adatkezelés korlátozása – Kellemes Ünnepeket!

ADAPTO

Adattárolási rendszer feltérképezése



Az érintettek jogainak érvényesítéséhez minden adattárolási forma összegyűjtése

- strukturált
- nem strukturált (e-mail, pdf, sms, ….)

ADAPTO

Részletes információk bekérése a tárolt adatokról

Adatkör neve:	Felhasználók adatai
Adatkör rövid leírása:	A rendszer felhasználóinak adatai. A felhasználó adja meg a saját nevét, email címét az első bejelentkezéskor.
Személyes adat:	Igen
Személyes adat kategóriája:	Természetes személyazonosító (név, cím) Munkahelyre, vállalkozásra vonatkozó adatok (cím, telefonszám, email cím, pozíció)
Különleges személyes adat:	Nem
Különleges személyes adat kategóriája:	
Hol éri el a felhasználó ezt a személyes/különleges személyes adatkört	• My profile/Email, Full name • Tools/ADAPTO users/Full name • BCM/Emergency/Alerts/Sender
Van-e procedúra arra, hogy ezt az adatkört töröljék a megtartási idő lejárta után?	A törlésre vállalati folyamatot kell kialakítani
Azoknak az interfészeknek a leírása (ideértve bármilyen API-t, vagy eljárást) ami lehetővé teszi ennek az adatkörnek az olvasását/módosítását	Nincs interfésze.
Tartalmazza-e az alkalmazás az inaktivált/lezárt bejegyzéseket?	Igen (naplózás folytonossága miatt)
Melyik az a legrégebbi időpont a nyilvántartásban, amikor az érintett adatrekordját (az érintettre vonatkozó bejegyzést) inaktiváltak?	Nem értelmezhető.

A struktúrált formában tárolt adatot milyen adatbázis milyen mezőiben tárolja a rendszer?					
Adat leírása	**Különleges?**	**Adatbázis**	**Tábla**	**Mező**	**A tárolás egyéb leírása**
Kapcsolattartó neve	Nem	ADAPTO	CONTACT	NAME	
Kapcsolattartó telefonszáma	Nem	ADAPTO	CONTACT	PHONE	
Kapcsolattartó e-mail címe	Nem	ADAPTO	CONTACT	EMAIL	
Riasztás címzettjének neve	Nem	ADAPTO	ALERT_LOG_RECEPIENT	NAME	
Riasztás címzettjének e-mail címe	Nem	ADAPTO	ALERT_LOG_RECEPIENT	EMAIL	
Task felelőse	Nem	ADAPTO	MANUAL_TASK	RESPONSIBLE	
Project owner	Nem	ADAPTO	PROJECTMANAGEMENT	OWNER	
Project manager	Nem	ADAPTO	PROJECTMANAGEMENT	MANAGER	
Külső partner képviselőjének címe	Nem	ADAPTO	EXTERNALS	R_ADDRESS	
Külső partner képviselőjének telefonja	Nem	ADAPTO	EXTERNALS	R_PHONE	
Külső partner képviselőjének emailje	Nem	ADAPTO	EXTERNALS	R_EMAIL	
Külső partner DPO címe	Nem	ADAPTO	EXTERNALS	C_ADDRESS	
Külső partner DPO telefonja	Nem	ADAPTO	EXTERNALS	C_PHONE	
Külső partner DPO emailje	Nem	ADAPTO	EXTERNALS	C_EMAIL	
Külső partner képviselőjének neve	Nem	ADAPTO	EXTERNALS	R_NAME	
Külső partner DPO neve	Nem	ADAPTO	EXTERNALS	C_NAME	
Kontakt neve	Nem	ADAPTO	CONTACT	NAME	
Kontakt telefonja	Nem	ADAPTO	CONTACT	PHONE	

Kockázat menedzsment

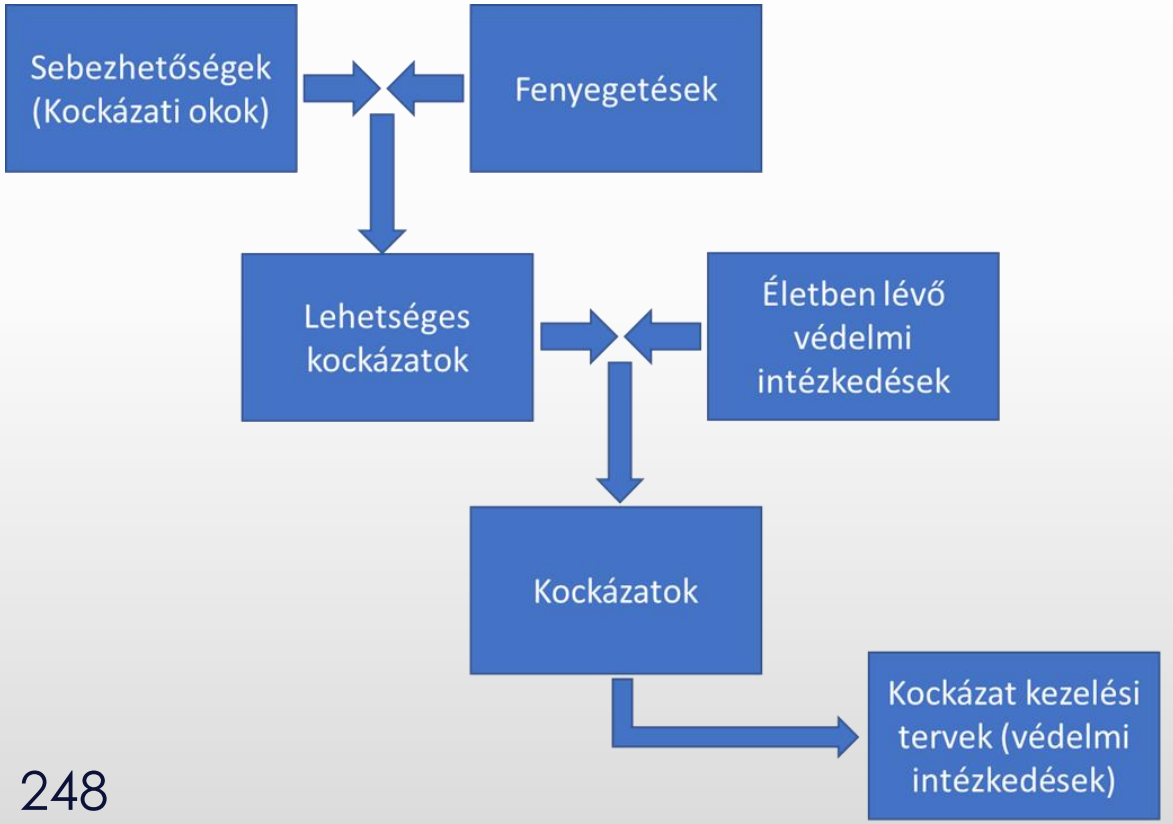
1. Informatikai rendszer vizsgálata: az adat
   - bizalmasságának,
   - sértetlenségének,
   - rendelkezésre állásának vizsgálata

   (ISO 27001 keretrendszer)

2. Az érintettek jogainak érvényesülése az alkalmazói rendszerekben:
   - betekintés
   - módosítás igénylése
   - elfeledés joga
   - tiltakozás profilalkotás ellen ….

   (GDPR keretrendszer)

3. Megfelelőségi kockázat
   - Mennyire büntet meg a hatóság? (WP 248 rev.01 – 2. melléklet)



ADAPTO

GDPR módszertan
Megfelelés igazolása

- Alkalmazhatósági nyilatkozat ISO 27001alapján a teljes informatikai rendszerre
- Alkalmazhatósági nyilatkozat GDPR alapján egyenként az alkalmazói rendszerekre (érintettek jogai)
- Alkalmazhatósági nyilatkozat GDPR alapján a jogszabálynak való megfelelésre

ADAPTO

További feladatok a GDPR kapcsán

- Érintetek jogigényének életciklusát követő munkafolyamat kialakítása
- Érintetek jogainak gyakorlását lehetővé tévő változások elvégzése az alkalmazói rendszerekben
- Álnevesítés? – integrált, de több szállítótól származó rendszerek esetén komoly tervezést igénylő, költséges feladat
- Központosított adattárolás az MIS rendszerben a betekintés jogának gyakorlásához
- Incidens kezelő rendszer bővítése egy új munkafolyamattal – incidens jelentése az adatvédelmi hatóságnak

ADAPTO

ADAPTO szoftver haszna a GDPR megfelelésben

- Be tudják építeni a GDPR-t az információbiztonság rendszerébe. (nem szigetrendszerként működik)
- Kockázatelemzés módszerével biztosítja, hogy az adatot megfelelően védik. (az érdekmérlegelési teszt önmagában nem elegendő)
- Igazolni tudja, hogy megvannak a védelmi intézkedések. (különben a GDPR felkészülés hiányos vagy hiábavaló)

ADAPTO