



**SELECTED
SOLUTION
MANAGEMENT**

Az IT biztonság szerepe a könyvvizsgálatban

Kancsal Tamás - Komenda Roland

FORTIX

Visegrádi Termal Hotel SPA



Miről fogunk beszélni:



- Jelen
- GDPR felkészülés
- Hosszútávú megoldás

Jelen



Zsarolóvírusok

- 100% védelem nincs
- I/O kontroll – DLP
- Vírus/malware
- Rendszeres mentés
- Folyamatos frissítés



Európai Adatvédelmi Rendelet

- 2018. május 25.
- Ip cím, ID, Cookie, gps, video,
- Megfordul a bizonyítás
- Rekord büntetés (6mdr)
- Hatóság erősödik
- Adatvédelmi hatásvizsgálat
- Adatvédelmi tisztviselő
- Felejtés joga
- Átláthatóság



Alkalmazotti visszaélés

- Jogosultságok kezelése
- Naplózás
- Monitoring rendszer
- Adatszivárgás védelem
- Incidens detektálás
- Jogi kontrollok



Hackerek

- MS forráskód lopás
- NSA kiberfegyver lopás – Wanna Cry
- Beláthatatlan következmények
- Nem tervezhető kockázatok

Tiszta vizet a pohárba



az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint az EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)



enisa



NIS irányelv

3 Jogi pillére az információkezelésnek

A GDPR célja



„Az új szabályok biztosítják, hogy a személyes adatok védelmének alapjoga mindenki számára garantált legyen.

Az általános adatvédelmi rendelet segíti majd az EU-ban a digitális egységes piac élénkítését azáltal, hogy világos és egységes szabályokra alapozva erősíti a felhasználók online szolgáltatásokba vetett bizalmát és a vállalkozások jogbiztonságát.”

GDPR – SZEMÉLYES ADAT (3/1)

Definíció

„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.”

GDPR – SZEMÉLYES ADAT (3/2)

Példák – személyes adat

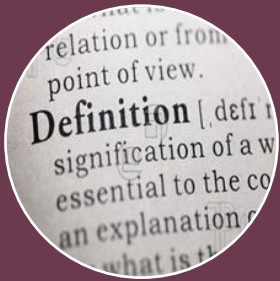
- Családi és utónév
- Adószám
- Életkor
- Email-cím
- Fotó
- Jogosítvány száma
- Születési dátum
- ...
- Útlevélszám
- SIM kártya száma
- Nem
- Facebook azonosító
- Bankszámlaszám
- IP cím
- Lakcímkártya száma
- ...

GDPR – SZEMÉLYES ADAT (3/3)

Példák – különleges személyes adat

- Faji, etnikai származás
- Politikai vélemény
- Vallási vagy világnézeti meggyőződés
- Szakszervezeti tagság
- Természetes személyek azonosítására szolgáló genetikai és biometrikus adatok
- Egészségügyi adatok
- Szexuális irányultságra vonatkozó adatok
- ...

TELJESKÖRŰ VÉDELEM



Személyes
adatok
meghatározása



Feldolgozás jogi
alapjának a
meghatározása



Adatvédelem
beágyazása



Adatbiztonság
fenntartása

A személyes adat megfelelő védelme a kezelés/feldolgozás teljes ideje alatt

Végrehajtás helyi szinten

- Itthon a NAIH fogja felügyelni
- Adatvédelmi incidens esetén 72 órán belül be kell jelenteni
- A nem megfelelő adatkezelés/adatfeldolgozás bírsága:

max. 20M EUR, vagy a szervezet árbevételének 4%-a

AMELYIK A NAGYOBB!



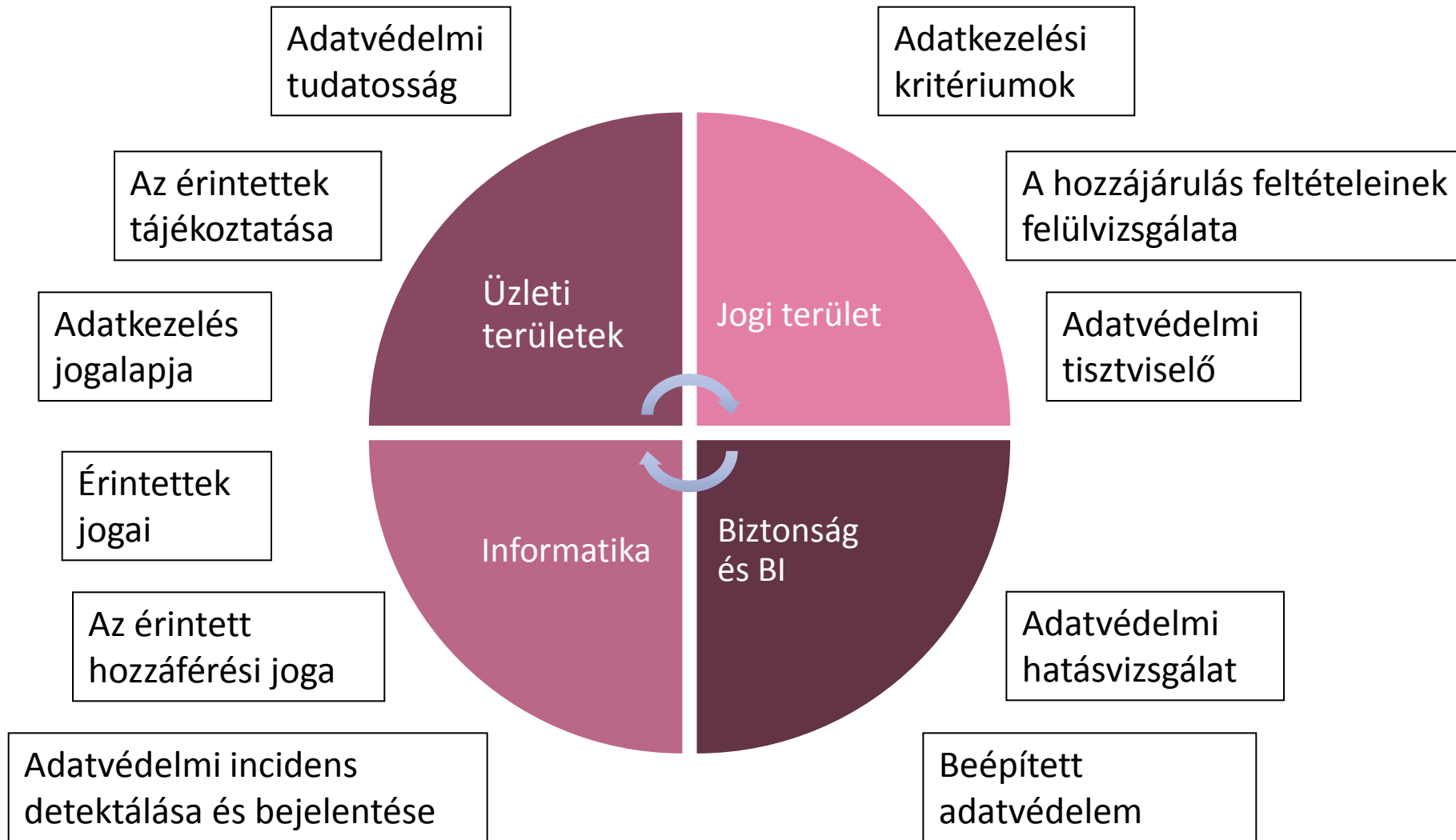
Készüljünk fel a rendelet elvárásaira

1. Adatkezelés kritériumainak felülvizsgálata
2. Adatvédelmi tisztviselő kinevezése
3. Kategorizált adatvagyon leltár
4. Adat térkép-folyamatok azonosítása
5. Jogalaphoz igazítás
6. Hozzájárulás feltételeinek megteremtése
7. Előzetes adathatás elemzés

Készüljünk fel a rendelet elvárásaira

- 8. Azonosított kockázatok csökkentése
- 9. Beépített adatvédelem megteremtése
- 10. Adat alanyok jogainak érvényesítése:
Transzparencia, felejtés joga, ...
- 11. Incidens detektálási képesség kialakítása
- 12. Érintettek tájékoztatása és képzése
- 13. Hatóság tájékoztatása

KIHÍVÁSOK, VESZÉLYEK



Miért kell hosszútávú megoldás?



Payment Services Directive
(PSD2)



...Amik kötelezettségeket róhatnak ránk. (A teljesség igénye nélkül.)

Hosszútávú megoldás

➤ Informatikai és adatvédelmi kompetencia központ

- Informatika
- Jog, adatvédelem
- It biztonság
- Incidens kezelés
- Ajánlás készítés
- Folyamatos képzés



Hosszútávú megoldás

Mit nyerhetünk mindezzel?

- Szakmákon átívelő kompetenciák lefedését.
- Az informatikai eszközök hatékonyabb alkalmazását.
- Tanácsadást – erőforrás kölcsönzést.

Köszönjük a figyelmet!

FORTIX



**SELECTED
SOLUTION
MANAGEMENT**

info@ssm.hu

info@fortix.hu