KPMG

Vállalati adatvédelem és a GDPR

Hargitai László, kiberbiztonsági tanácsadó

2017. március 2.

Tartalom

Hogyan azonosítjuk a (kiber)személyeket?

A személyek elsődleges azonosítása 100 év alatt teljesen átalakult: a helyi, személyes és rokoni ismeretségtől az állami dokumentáción át eljutott a kibertér korszakába.

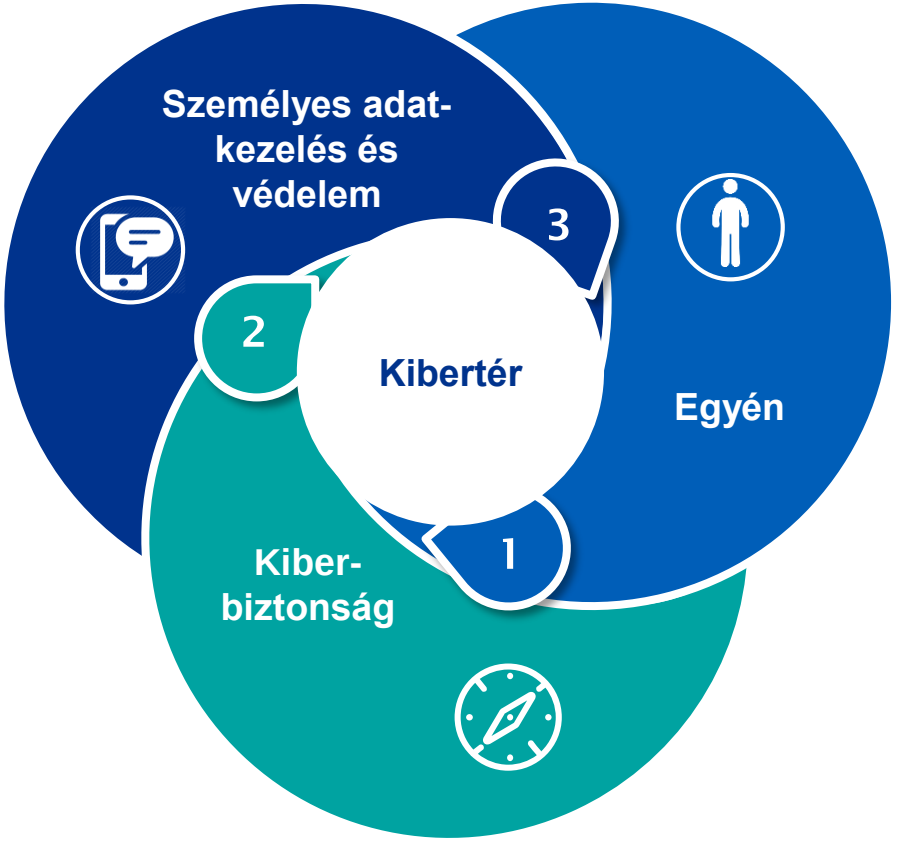
Milyen személyi azonosítókat használunk a kibertérben?

- Felhasználónév, jelszó
- Közösségi alkalmazás profil
- E-mai cím, telefonszám
- Biometrikus azonosítók

Ám nem csak ezek számítanak személyes adatnak, hanem bármi, ami potenciálisan alkalmas az azonosítására: bankszámlaszám, vásárlási szokások, vélemények, képek, hobbik, hajszín, egészségügyi adatok …

A személyes adatok hatékony védelme két pilléren nyugszik:

- A külső és belső támadók (hackerek, szervezett bűnözők, titkosszolgálatok) elleni védelem a **kiberbiztonság** feladata.
- A személyes adatokhoz üzleti céllal hozzáférők elleni védelem **megfelelő adatkezeléssel** érhető el.



Személyes adatok: üzleti érték és kockázat

Adatvagyon:

A személyes adatok értékét a piac már régen felfedezte, lásd pl. vásárlási preferenciák, születésnapi ajánlatok. Az okos eszközök által gyűjtött adatok mennyisége és a big data azonban új távlatokat nyit. **Mind több személyes adat értékesíthető közvetlen áruként.** Nem csak legálisan, a fekete piacon is.

Bizalom:

Egy adatszivárgás miatt az ügyfelek bizalmát véglegesen el lehet veszíteni. De mi befolyásolja még az ügyfelek bizalmát?

- Csökkenti a bizalmat: **otthoni tevékenység naplózása**, **személyes adatok továbbértékesítése, kontrollvesztés** érzete.
- A KPMG globális felmérése alapján az emberek 46 %-a hajlandó árengedményért cserébe átadni személyes adatait.

Kockázat:

Az EU Általános Adatvédelmi Rendelete (GDPR) új alapokra helyezi a személyes adatok kezelését és védelmét. A bírság emelkedésénél is **nagyobb kockázatot okoznak a kártérítési keresetek.**

GDPR – új követelmények és kockázatok

A GDPR legfontosabb változásai a vállalatok számára:

Bírságok
A maximális kiszabható bírság 20 m EUR, vagy az árbevétel 4 %-a (amelyik magasabb).

Adatvédelmi tisztviselő
Bizonyos esetekben (pl. különleges adatok kezelése nagy számban) kötelező válik adatvédelmi tisztviselő kinevezése.

Adatkezelési nyilvántartás
Bizonyos esetekben (akár 250-es létszám alatt is) kötelező lesz belső adatkezelési nyilvántartást létrehozni.

Incidens bejelentése
Hatóság és érintettek késedelem nélküli kiértesítése (~72 óra).

Adatbiztonság
Konkrét követelmények, pl. titkosítás, álnevesítés.

Adatvédelmi hatáselemzés
Magas kockázatú adatkezelésnél kötelező lesz elvégezni.

Érintettek jogai
Bővülnek az érintettek jogai, többek között az adatok továbbítása és„elfeledtetése” terén

Különleges adatok
Új kategóriák jelennek meg (pl. biometrikus, genetikai azonosítók)

Hozzájárulás
A „privacy by design” elv alapján változik a hozzájárulás tartalma.

Adatfeldolgozók
Új követelmények jelennek meg az adatkezelő és adatfeldolgozók közötti szerződésekre nézve.

Megoldás: adatkezelés a szervezet szintjén

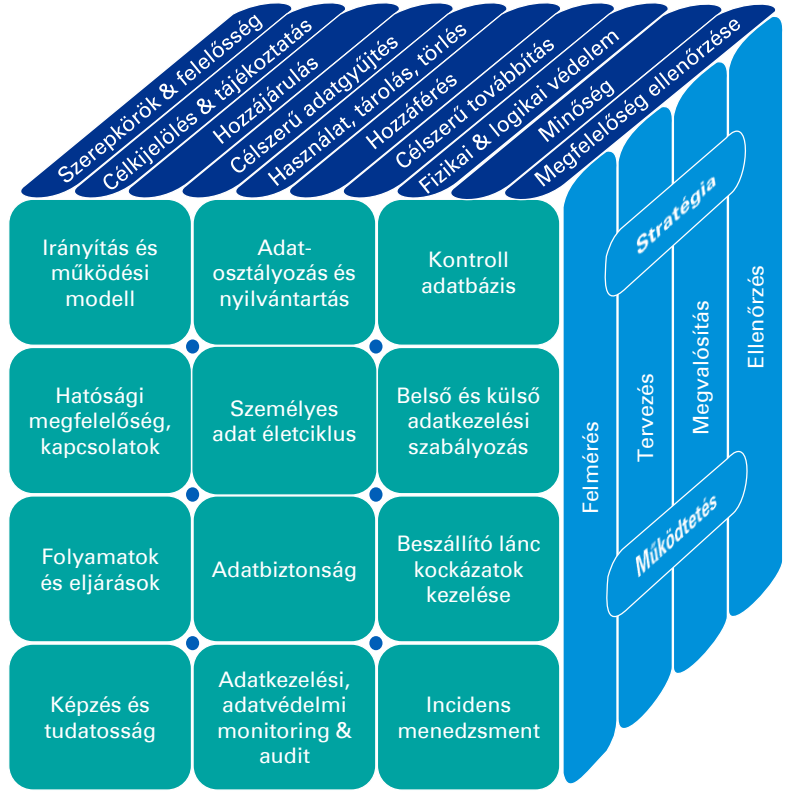
A GDPR megmondja, hogy „minek” kell megfelelni az adatkezelésben, de nem ad támpontot a „hogyan”-hoz.

A szervezet felkészítéséhez **a folyamatokat, a résztvevő embereket és a technológiát kezelni képes keretrendszerre van szükség**.

A kulcselemek:

- **Kiindulási keretek felmérése:** stratégiai célok, követelmények, működési modell, szereplők, meglévő adatkezelési rendszer
- **Tervezés és megvalósítás:**
  - Adatkezelő rendszer: adatosztályozás, leltár, adat életciklus kezelése
  - Szabályozás: adatvédelmi szabályzatok, adatvédelmi folyamatok és eljárások
  - Kockázatok kezelése: kontroll adatbázis, törvényi megfelelőség, informatikai biztonsági interfész, beszállítói lánc ellenőrzése, monitoring és audit
  - Képzés: munkatársak tudatosítása, ügyfelek és partnerek tájékoztatása
- **Ellenőrzés:** az adatvédelmi rendszer működtetésének folyamatos monitorozása

KPMG Privacy Management Framework



Az adatvédelem érettségének mérése

Az adatkezelési keretrendszer **minden komponenst illetően átláthatóvá teszi a szervezet érettségének fejlődését**, lehetőséget nyújt a rendszeres mérésre: a vállalat, az ügyfelek és a hatóság felé egyaránt.

Az adatvédelmi érettség skálája:

1 Ad hoc

A szervezet már foglalkozik a személyes adatok védelmével, de a folyamatok még nem szabályozottak és dokumentáltak, **esetenként változó eljárásokat** követnek.

2 Kezdeti

Az adatkezelés dokumentációja minimális, de az alkalmazott eljárások ismétlődnek és eredményük sokszor konzisztens. **A hatékonyság nagyban függ attól, melyik munkatárs végzi az adat kezelését.** A munkatársak nem részesülnek adatvédelmi képzésben.

3 Kontrollált

Az adatkezelés **eljárások szabályozottak, dokumentáltak, a résztvevők adatvédelmi tréninget kapnak.** Az adatvédelmi kontrollok működése megfelelő. Egyes részlegek együttműködnek az adatvédelem terén.

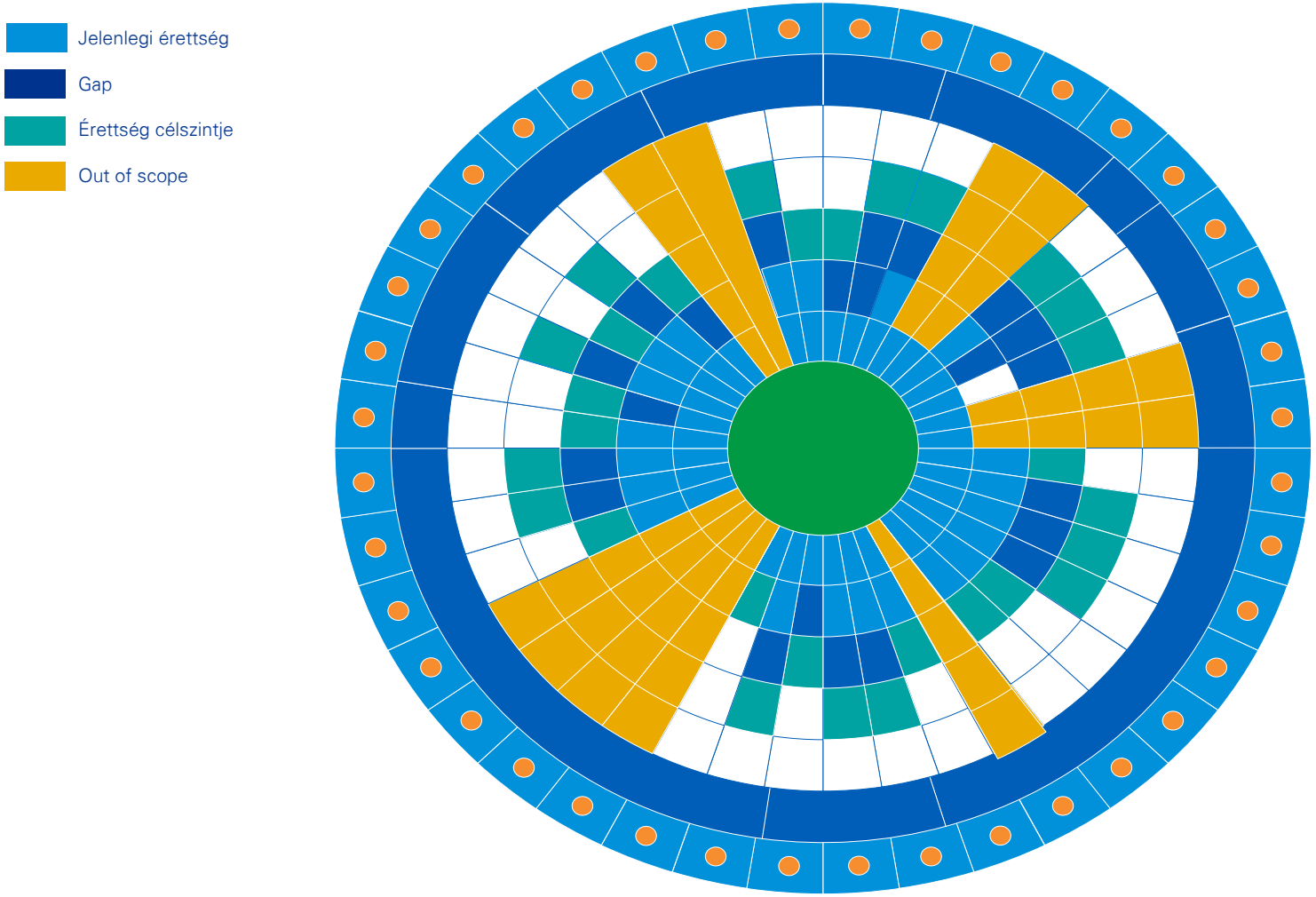
4 Ellenőrzött

Az adatvédelem és adatkezelés működését **szervezeti szinten monitorozzák**, az azonosított hiányosságok javítását, fejlesztési igények teljesítését összehangoltan végzik.

5 Optimalizált

Az **adatvédelem és adatkezelés hatékonyságának mérésére szervezet szintű** folyamatok vannak érvényben, a szervezet stratégiai célként kezeli a hatékonyság javítását.

Adatvédelmi érettség - eredmény



További információk

Amennyiben további tájékoztatásra van szüksége akár a kiberbiztonság, akár az adatkezelés és adatvédelem fejlesztése terén, várjuk megtisztelő látogatását honlapunkon.

KPMG informatikai kockázatkezelési tanácsadás:

https://home.kpmg.com/hu/hu/home/szolgaltatasok/tanacsadas/kockazatkezeles/it.html

Kiberbiztonsági érettség vizsgálata:

https://home.kpmg.com/hu/hu/home/szolgaltatasok/tanacsadas/kockazatkezeles/it/it-audit/kiberbiztonsagi-erettseg-vizsgalata.html

Adatkezelési és adatvédelmi tanácsadás:

https://home.kpmg.com/hu/hu/home/szolgaltatasok/tanacsadas/kockazatkezeles/it/informacio-biztonsagi-tanacsadas/adatkezelesi-es-szemelyesadat-vedelmi-tanacsadas.html

Köszönöm a figyelmet!

KPMG

kpmg.com/socialmedia

kpmg.com/app