



# Adatvédelmi szabályzat bevezetése 2020-2021

## Önellenőrzés módszertana

Dr. Keczely Béla Zoltán LL. M.

*Oktatás, kutatás,  
gyógyítás: 250 éve az  
egészség szolgálatában*

2020

# Önellenőrzés mikor és miért

- ↳ **Mikor?** Minden év január 31. napjáig
- ↳ **Mit ?** Adatvédelmi elveknek megfelelő –e az adatkezelési tevékenység
- ↳ **Hogyan?** Nyilvántartások vezetése, dokumentumok aktualitása, tájékoztatók, hozzájárulások rendelkezésre állása biztosított-e.

# Az adatkezelési tevékenység nyilvántartásának megfelelősége

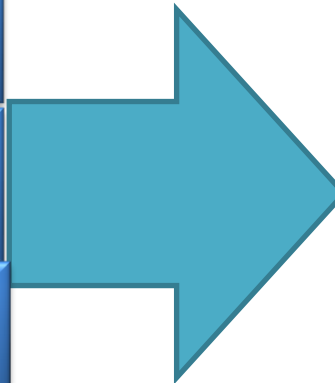
A Szervezeti Egység felülvizsgálja a nyilvántartásban szereplő adatkezeléseket, valamint az azokról nyilvántartott adatait.

A Szervezeti Egység megvizsgálja, hogy a nyilvántartása az Infotv. 25/E §-a, és a GDPR 30. cikkelye által előírtaknak megfelel-e és az feltüntetett adatok teljes körűek és valódiak.

Minden adatkezelés nyilvántartásba került –e ?

Minden adatkezelésről minden adat nyilvántartásra került –e ?

Az új adatkezelések nyilvánításra kerültek-e nyilvántartásra került –e ?



Cél, jogcím,  
kezelt adatok,  
érintettek köre,  
kezelést végzők,  
adatkezelés ideje,  
adatifeldolgozók

# Az adatkezelési tájékoztatók megfelelősége

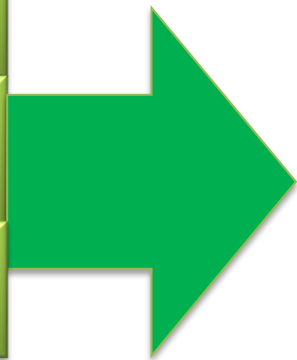
A Szervezeti Egység felülvizsgálja hogy elkészítette és közzétette –e az érintettek részére adatkezelési célonként az adatkezelési tájékoztatókat

A Szervezeti Egység megvizsgálja, hogy a tájékoztatók megfelelnek a GDPR 13. és 14. cikkelyei által előírtaknak, az azokban feltüntetett adatok teljes körűek és valódiak.

Minden adatkezelés készült-e tájékoztató?

Az adatkezelésről minden adat tájékoztatóba került –e ?

Minden tájékoztató nyilvántartására és közzétételére került –e ?



Cél, jogcím,  
kezelt adatok,  
érintettek köre,  
adatkezelés ideje,  
adatifeldolgozók

# Az adatkezelési tevékenység célhoz kötöttségének megfeleltetése

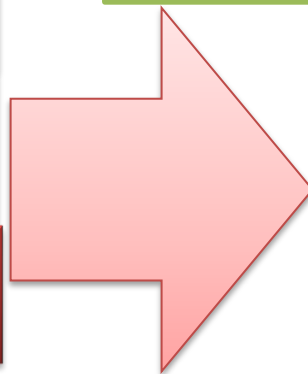
A Szervezeti Egység Annak biztosítása érdekében, hogy a személyes adatok kezelése csak az adott célhoz kötött legyen, a szervezeti egységek az általuk kezelt adatok célhoz kötöttségét felülvizsgálják.

A Szervezeti Egység megvizsgálja, hogy az adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat nem kezelik ezekkel a célokkal össze nem egyeztethető módon. Az esetlegesen nem megfelelő vagy nem igazolt céllal kezelt adatok esetén a célt megfelelő célra módosítja, vagy az adatkezelést megszünteti a megfelelő cél nélkül kezelt adatokat töröli.

Minden adatkezelés van e törvényes célja ?

A cél nem szűnt-e meg?

Az adatot nem kezelték –e más célra?



Cél,  
kezelt adatok,  
érintettek köre

egyértelmű és  
jogszerű cél

# Az adatkezelési tisztességességének és jogszerűségének (jogalapok)megfelelősége

A Szervezeti Egység valamennyi adatkezelését, a jogszerűségét és tisztességességét, valamint átláthatóságát az adatkezelések megfelelő jogalapja tekintetében felülvizsgálja.

A Szervezeti Egység megvizsgálja, hogy valamennyi adatkezelés esetén az adatkezelés jogalapját azonosították és azok az adatkezelés céljának megfelelők, e célokról, és jogalapokról az érintetteket megfelelően tájékoztatták.

Minden adatkezelésnek van e törvényes alapja ?

A jogalap nem szűnt-e meg?

Az adatot nem kezelték –e jogalappal ellentétes módon?

## JOGALAPOK

1. **Hozzájárulás:** rendelkezésre áll
2. **Szerződés:** rendelkezésre áll
3. **Jogszabály :** hatályos
4. **Létfontosságú érdek:** igazolt
5. **Közfeladat:** fennáll
6. **Jogos érdek:** érdekmérlegelési teszt

# Az adatkezelés megfelel az adattakarékosság elvének

A Szervezeti Egység valamennyi adatkezelését, az adattakarékosság tekintetében felülvizsgálja

A Szervezeti Egység megvizsgálja, hogy adatok gyűjtése, az adatkezelés meghatározott céljai szempontjából megfelelőek és relevánsak, és a szükséges mértékűre korlátozott. Az esetlegesen a céltól eltérő vagy nem releváns illetve szükségtelen adatkezeléseket megszüntette, ezen adatokat törli.

Minden adatkezelés esetében csak a szüksége adatok kezelik -e?

Nem kezelnek –e a célhoz nem feltétlenül szükséges adatot ?

A szükségtelen adatokat törölték-e ?

Tilos a  
szükségtelen  
adattárolás,  
készletezés

## **Adat minimalizálás:**

1. Csak annak az adatát
2. Csak olyan adatot
3. Csak annyit adatot
4. Csak annyi ideig  
ami feltétlenül szükséges a cél  
eléréséhez

# Az adatkezelés adatbiztonságának megfeleltetése

A Szervezeti Egység valamennyi adatkezelését, az adatok biztonságára érdekében tett szervezési és technikai intézkedések megfeleltetése tekintetében felülvizsgálja

A Szervezeti Egység megvizsgálja, hogy adatkezelés jellege, hatóköre, körülményei és céljai, változó valószínűségű és súlyosságú kockázatok a technikai fejlettség színvonala a kockázat arányos ráfordítás költsége alapján megfelelőek –e a biztonság érdekében tett szervezési és technikai intézkedések

Minden adatkezelés esetében biztosított-e folyamatos bizalmas jellegének megőrzése?

A incidens esetén adatok vissza állíthatóak-e?

A megtörténik-e a szervezési és technikai intézkedések rendszeres tesztelése, auditja?



## Adat biztonság:

1. **Szervezés:** szabályzat, hozzáférési jogosultságok
2. **Technika:** fizikai és logikai biztonság
3. **Teszt:** naplózás, audit



# Az adatkezelés beépített és alapértelmezett adatvédelem megfelelősége

A Szervezeti Egység belső normatív eszközét (szabályzatokat és munkautasításokat) a beépített és alapértelmezett adatvédelem megfelelősége tekintetében felülvizsgálja

A Szervezeti Egység megvizsgálja, hogy új adatkezelés esetén elvégzi –e az adatkezelés hatásvizsgálatát, új szabályozás esetén a szabályzatba, eljárásrendbe be kerülnek az adatvédelmet biztosító intézkedések. Az ezeknek nem megfelelő a belső normatív eszközöket módosítja.

Minden adatkezelés új biztosított-e és vizsgálat –e az adatkezelés megfelelősége ?

Minden új vagy hatályos belső szabályozó eszköz tartalmaz-e adatvédelmi kontrollt

Az ennek nem megfelelő eszközök módosításra kerültek-e

## Beépített adatvédelem

1. Vizsgálat új adatkezelés előtt
2. Vizsgálat új szabályozás előtt
3. Rendszeres szabályozás felülvizsgálat
4. A folyamatok része az adatvédelmi intézkedés

# Az adatkezelés korlátozott tárolhatósága megfelelősége

A Szervezeti Egység felülvizsgálja adatkezeléseit, adatok kezelésének ideje illetve tárolásának ideje tekintetében.

**Minden adatkezelésnél meghatározták –e a tárolási időt?**

**A tárolási idő nem telt-e le?**

**A tárolási idő alapja dokumentált-e?**

A Szervezeti Egység megvizsgálja, hogy az adatkezelés során az adatok tárolása olyan formában történik, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor.

## **Adattárolás**

- 1. Alap: 5 év**
- 2. Bővített: ameddig azt jogszabály engedi**
- 3. Legfeljebb: közérdek, tudomány, statisztika**



# Az adatkezelés elszámoltathatóságnak megfelelése

A Szervezeti Egység felülvizsgálja adatkezeléseit, hogy azok az elszámoltathatóság elvének megfelelően dokumentáltak.

A Szervezeti Egység megvizsgálja, hogy az adatkezelés során valamennyi adatkezelési művelete megfelelően dokumentált-e. Az adatkezelések megfelelésének igazolásához a dokumentációk rendelkezésre állnak.

Minden adatkezelés dokumentált-e?

Minden a dokumentációk rendelkezésre áll-e?

A dokumentumok alkalmasak –e a megfelelés igazolására?

## Elszámolhatóság

1. Nyilvántartások vezetettsége
2. Adatkezelések megfeleléséget alátámasztó dokumentumok rendelkezésre állása (szerződések, nyilatkozatok)
3. Dokumentumok megfelelése (cél, jogalap, pontosság, aktualitás)



# Az adatfeldolgozás megfelelősége

A Szervezeti Egység felülvizsgálja adatfeldolgozások megfelelők és dokumentáltak.

A Szervezeti Egység megvizsgálja, hogy az adatkezelés során valamennyi érintetti jogot biztosította, az érintettek kérelmeire megfelelően reagált illetve arra adott választ megfelelően nyilvántartja az elszámolhatóság érdekében.

Minden van-e adatfeldolgozás nyilvántartva van-e?

Kik az adatfeldolgozók?

Az adatfeldolgozók mit csinálnak?

## Adatfeldolgozás

1. Adatfeldolgozási szerződések megfelelősége ( 28. cikk)
2. Adatfeldolgozás nyilvántartása
3. Adatfeldolgozók ellenőrzése (utasítások, biztonság)



# Az érintetti jogok biztosításának megfelelősége

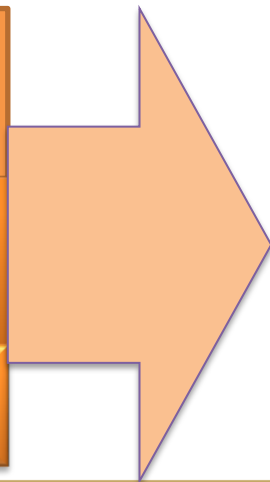
A Szervezeti Egység felülvizsgálja megfelelően biztosított-e az érintettek jogait és ezen jogok biztosítása megfelelően és dokumentált.

A Szervezeti Egység megvizsgálja, hogy az adatkezelés során valamennyi adatfeldolgozási művelete megfelelő és dokumentált-e. Az adatfeldolgozások megfelelésének igazolásához a dokumentációk rendelkezésre állnak.

Minden adatkezelésről van-e tájékoztató?

Minden kérelmet nyilvántartásba vettek-e?

Minden kérelemre érdemi választ adtak-e ?



## **Érintetti jogok**

1. Tájékoztatók
2. Kérelmek nyilvántartása
3. Dokumentáció



# Az adattovábbítás megfelelősége

A Szervezeti Egység felülvizsgálja megfelelően biztosított-e az adatigénylések elbírálása, teljesítése.

A Szervezeti Egység megvizsgálja, hogy az adatkéréseket megfelelő módon nyilvántartásba vették-e, azokra érdemben reagáltak-e, betartották-e a teljesítési határidőket.

Minden adatigénylést  
nyilvántartásba vettek-e ?

Minden kérelmet elbíráltak-e?

Betartották e határidőket?



## **adattovábbítás**

1. Nyilvántartás
2. Dokumentáció
3. Határidő



# Az adatokhoz való hozzáférés megfelelősége

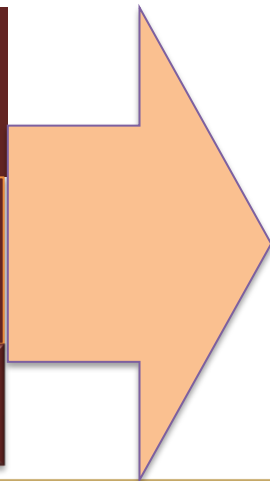
A Szervezeti Egység felülvizsgálja megfelelő-e az adatok védelme, integritása az azokhoz való hozzáférés szempontjából.

A Szervezeti Egység megvizsgálja, hogy az adatokhoz csak azok férnek hozzá a szervezeten belül akiknek arra jogosultságuk van és ezen jogosultságokat megfelelő adatkezelési cél alapozza-e meg, a jogosultságok felhasználása védett és nyilvántartott-e.

Minden jogosultságot  
nyilvántartásba vettek-e ?

Minden a jogosultságok célja  
megalapozott-e?

A jogosultságok rögzítve vannak-e a  
munkaköri leírásokban?



## jogosultság

1. Nyilvántartás
2. Dokumentáció (Munkaköri leírás)
3. Jogosultság célja
4. Jogosultság felhasználásának biztonsága
5. Jogosultság használatának ellenőrzése
6. Adatkiadások ellenőrzése

# Az adatvédelmi incidensek kezelésének megfelelősége

A Szervezeti Egység felülvizsgálja megfelelő-e az adatvédelmi incidensek kezelése

A Szervezeti Egység megvizsgálja, hogy adatvédelmi incidenseket azonosították –e, feltárták-e az incidensek által jelentett kockázatokat, intézkedtek –e azok elhárítására, jelentették –e az incidenseket az Adatvédelmi Tisztviselőnek, bejelentették-e azokat a NAIH-nak, értesítették-e az érintetteket.

Minden incidens felismertek –e és mindet nyilvántartásba vették-e

Minden a incidenst jelentettek-e

Elhárítására /ismételt előfordulása ellen intézkedtek-e

## **Incidensek**

1. Kockázat azonosítás
2. Nyilvántartás
3. Intézkedések
4. Jelentések
5. Bejelentés, értesítés
6. Elhárítás, megelőzés



# Az adatvédelmi tudatosság megfelelősége

A Szervezeti Egység felülvizsgálja megfelelő-e az adatvédelmi tudatosság szintje a szervezeti egységen belül.

A Szervezeti Egység megvizsgálja, megvalósult-e az új munkavállalók munkába lépésekor az adatvédelmi oktatásuk. Az adatvédelmi továbbképzésben részesültek-e munkatársak.

Minden részesült-e képzésben?

Minden munkatárs képzését nyilvántartják-e?

A képzésben még részt nem vettek képzését megtervezték-e?



## Tudatosság

1. képzési terv
2. Képzési Nyilvántartás
3. Utóképzés
4. ellenőrzés

