

A username and password are being returned.
The site says: "Member Site"

Username: |

Password:



Nemzeti Adatvédelmi és
Információszabadság Hatóság

A GDPR biztonságtechnikát érintőpontjai

2019. február 8.

dr. Kiss Attila

Milyen követelményekről beszélünk?

- ▶ **Adatvédelem**: a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító **alapelvek, szabályok, eljárások**, adatkezelési eszközök és módszerek összessége. („jogi” fogalom)
 - ▶ Vizsgált szempontok például:
 - ▶ Megőrzési idő, cél, adatkezelő, felelőségek
 - ▶ Adatgyűjtés / felvétel készítése (helye, látószög, adatkör)
 - ▶ Felhasználása – továbbítása – hozzáférés – adatok biztonsága
 - ▶ Érintettek jogai (pl. előzetes tájékoztatás és másolat kiadása)
- ▶ **Adatbiztonság**: az adatok *jogosulatlan megszerzése, módosítása és megsemmisítése* elleni **műszaki és szervezési megoldások** (műszaki/biztonsági fogalom)
 - ▶ Vizsgált szempontok:
 - ▶ Adatátvitel, rögzítő/megjelenítő eszközök elhelyezése
 - ▶ Tárolás módja, helye (fájl és adatbázis titkosítás)
 - ▶ Hozzáférési jogosultságok és naplózás, incidenskezelés



Kezel személyes adatot a rendszer?

Személyes adat

- az érintettre vonatkozó **bármely információ**
 - kép, hang, biometrikus adat, mozgás, tartózkodási hely
- akár hivatali ügyben, munkaviszonyban, eljárás során is!
- mindaddig megőrzi e minőségét, **amíg kapcsolata az érintettel helyreállítható:**
 - Pl. rendszám, IP-cím, telefonszám, belépőkártya száma, RFID is lehet

Érintett

- közvetlen vagy közvetett módon azonosított vagy azonosítható természetes személy
- *Munkatársak és az állomány intézkedő tagja / vagyonőr / fbö is!!!*



Ha igen: Alkalmazandó előírások 1.

*Általános Adatvédelmi Rendelet (679/2016 - **GDPR**)*

- Közvetlenül alkalmazandó
 - Az egész EU-ban egységes feladatok és szankciók
- Tagállamok nem alkothatnak ellentétes jogszabályt, nemzeti jogszabályok felett áll a teljes szöveg
 - Felül kell vizsgálni az ágazati szabályozást (pl. Szvmt. és Mt.)
 - „Saláta-törvény” <http://www.parlament.hu/irom41/04479/04479.pdf>
- NAIH nem értelmezheti a GDPR előírásait
 - Egységes jogalkalmazást segítik az Európai Adatvédelmi Testület iránymutatásai (<http://naih.hu/29-es-munkacsoport-iranymutatasai.html>)
- Automatizált és (Infotv. miatt) nem automatizált rendszerek is!
 - KKV-k nem esnek kivétel alá!



Ha igen: Alkalmazandó előírások 2.

GDPR hatályán kívüli tevékenységek

- I. Természetes személyek *kizárólag személyes vagy otthoni* tevékenységük keretében végzik (nincs gazdasági érdek)
 - Nincs adatkezelő sem! (Magánnyomozó? Magánkamera?)
- II. *Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.)*
 - Bűnügyi irányelv - Bűnmegelőzési, bűnüldözési cél, szabálysértési és büntetőeljárás
 - De csak az arra felhatalmazott szerv (pl. Rendőrség, BV, NAV) ilyen adatkezelései!
 - Uniós jog hatályán kívüli tevékenységek
 - honvédelem, nemzetbiztonság, igazságszolgáltatási jogkörben bíróságok
 - Kiegészítő előírások, ahol GDPR megengedi



Csak akkor jogszerű, ha van jogalap

- Korábban hozzájárulás és kötelező adatkezelés

2018 május 25-től:

- **Hozzájárulás** csak kivételes esetben
 - Bármikor jogosult visszavonni, alá-fölérendeltség esetén nem alkalmazható!
 - Nincs általános hozzájárulás, nem érheti semmilyen hátrány ha nem ad
 - Kamera, beléptető: 14 év alatti esetén törvényes képviselő járulhat hozzá
- **Közhatalom gyakorlása, közfeladat + törvényi felhatalmazás**
 - Pl. minősített irat, elektronikus információs rendszer védelme
 - személyszállítási szolgáltatásokról szóló 2012. évi XLI. törvény
- **Jogi kötelezettség** (törvény előírja)
 - Pl. rendőrség/közterület-felügyelet térfigyelő kamera
- **Jogos érdek**
 - érdekmérlegelés – adatkezelő kell igazolja
 - Pl. vagyonvédelem, munkahelyi ellenőrzés, csalások megelőzése
 - Közterületre nem irányulhat (osztrák döntés)



Jogos érdeken alapuló adatkezelés 1.

GDPR elsőbbsége + Saláta-tv. tervezete: a **személy- és vagyonvédelmi**, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény kamerát, beléptető rendszert, távfelügyeletet érintő módosítása:

- Nincs „felhatalmazás”, nincs hozzájárulás
- Nincs megőrzési idő
(se törvényre tekintettel lehetőség a hosszabb megőrzés alátámasztására!)
- Nincs a cél meghatározva
- Nincs felhasználás, címzett kapcsán megkötés
- Nincs adatbiztonsággal kapcsolatos rendelkezés
- ~~vagyonőrzési feladatokat ellátó személy adatkezelőnek minősül~~



Jogos érdeken alapuló adatkezelés 2.

GDPR elsőbbsége + Saláta-tv. tervezete: az Szvmt. kamerát, beléptető rendszert, távfelügyeletet érintő módosítása:

- 28. § a GDPR alapján adandó tájékoztatást pontosítja
- 30. § (2) „A vagyonőr elektronikus megfigyelőrendszert **kizárólag magánterületen** alkalmazhat.”
- 30. § (3) „Nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a **megfigyelés az emberi méltóságot sértheti**, így különösen öltözőben, próbafülkében, mosdóban, illemhelyen, kórházi szobában és szociális intézmény lakóhelyiségében.”
- 31. § „Az elektronikus megfigyelőrendszer működése útján rögzített kép-, hang-, valamint kép- és hangfelvétel megismerésének okát és idejét, valamint a megismerő személyét **jegyzőkönyvben kell rögzíteni**. Az ezen adatokat igazolható módon tartalmazó elektronikus nyilvántartás is jegyzőkönyvnek minősül.”
- 32. § „**Elektronikus beléptető rendszer** az erre vonatkozó megbízási szerződés alapján és akkor alkalmazható, ha jogszabály vagy a terület használatára jogosult rendelkezése szerint a védett területre csak az arra jogosultak léphetnek be.”



Jogos érdeken alapuló adatkezelés 3.

GDPR elsőbbsége + Saláta-tv. tervezete

- A **társasházakról** szóló 2003. évi CXXXIII. törvény és a **lakásszövetkezetekről** szóló 2004. évi CXV. törvény módosítása (tervezet)
- Nincs megőrzési idő, együttes feltételek, erre az **érdekmérlegelésben** kell kitérni
- Érintetti jogok gyakorlása – visszautal a **GDPR előírásaira**



Biometrikus adatkezelés

Csak akkor valósul meg, ha teljesül:

- ▶ a biometrikus adat rögzítése, átalakítása biometrikus sablonná
- ▶ a biometrikus adat/sablon tárolása egy központi adatbázisban vagy adathordozón
- ▶ a biometrikus adat/sablon összevetése a tárolt biometrikus adattal/sablonnal

Munkavállalók biometrikus adatainak kezelése (Saláta-tv. tervezete):

- ▶ Mt. 11. § (1) A **munkavállaló biometrikus adata** az érintett azonosítása céljából **abban az esetben kezelhető, ha** ez valamely dologhoz vagy adathoz történő olyan jogosulatlan hozzáférés megakadályozásához szükséges, amely
 - a) a munkavállaló vagy mások élete, testi épsége vagy egészsége, vagy
 - b) törvényben védett jelentős érdek**súlyos vagy tömeges, visszafordíthatatlan sérelmének a veszélyével járna.**
- ▶ (2) Az (1) bekezdés b) pontja alkalmazásában jelentős védett érdek különösen
 - a) a legalább „Bizalmas!” minősítési szintű minősített adatok védelméhez,
 - b) a lőfegyver, lőszer, robbanóanyag őrzéséhez,
 - c) a mérgező vagy veszélyes vegyi vagy biológiai anyagok őrzéséhez,
 - d) a nukleáris anyagok őrzéséhez,
 - e) a Büntető Törvénykönyv szerint legalább különösen nagy vagyoni érték védelméhez fűződő érdek.



Az új szabályozás koncepciója

Elszámoltathatóság

- Az adatkezelőnek nem csak **megfelelnie** kell az adatvédelmi alapelveknek és követelményeknek, hanem képesnek kell lennie e **megfelelés igazolására**. („köteles bizonyítani”)
- Tudatosság (dokumentált)
- Kockázatok értékelése (biztonsági és jogi is!)
- Megfelelő és hatékony intézkedések (dokumentáltan)
- Érintetti jogok biztosítása
- Ellenőrzés és szankciórendszer



Miért felel az adatkezelő?

- Gyűjt-e, kezel-e adatot?
- Milyen jogszerű célból?
 - Vagyonvédelem, munkaidő, esetleg munkahelyi ellenőrzés?
- Milyen eszközzel? Milyen adatokat? Milyen területen?
 - Feltétlenül szükséges, arányos, nincs enyhébb eszköz?
- Kinek ad hozzáférést?
 - Üzemeltető vagyonvédelmi céget vesz igénybe? Felhőben tárol?
 - Csak telepít, távoli frissítést küld – ha nem fér adathoz nem adatfeldolgozó
 - Felel az adatfeldolgozó kiválasztásáért, az átadott adatok jogszerűségéért, adatfeldolgozói szerződés írásbeli megkötéséért (kivéve ha jogszabály jelöli ki, pl. NISZ Zrt.)
- GDPR alapelveinek és előírásainak történő megfelelésért
 - Érintetti jogok – részletes tájékoztató és figyelemfelhívó matrica
 - Érdekmérlegelési teszt – igazolni a dolgozónak és NAIH-nak
 - Adatbiztonsági követelményekért (adatvédelmi incidens)
 - Az adatvédelmi hatásvizsgálat lefolytatásáért



Miért felel az adatfeldolgozó?

- Az adatfeldolgozási szerződésben foglaltak betartásáért
- Saját munkatársai, vagy alvállalkozói tevékenységéért
- Adatbiztonságért (gyűjtés, továbbítás, tárolás, naplófájl, biztonsági mentés, hálózat, végpontvédelem)
- Adatok szolgáltatásáért (**hatásvizsgálat, incidens**)
- Adatvédelmi tisztviselő kijelöléséért – ha igazak rá a feltételek
- Saját célra nem használhat fel személyes adatot, **mert adatkezelővé válik**
- Adatfeldolgozói nyilvántartás vezetéséért



Hozzáférés joga

- ▶ Érintett joga, hogy az adatkezelőtől „**visszajelzést kapjon**”, hogy az adatainak kezelése folyamatban van-e (volt-e).
- ▶ Ha igen:
 - ▶ Adatkezelés céljáról, az adatkezelés jogalapjáról,
 - ▶ Adatok tárolásának időtartamáról vagy azt ezt meghatározó szempontokról,
 - ▶ A **konkrét (kezelt) személyes adatokról**, az adatok forrásáról, ha az nem az érintett
 - ▶ Címzettek köréről, adattovábbításokról
 - ▶ **Egyéb jogairól** (pl. helyesbítés, törlés, korlátozás)
 - ▶ **Jogorvoslati jogról** (NAIH, bíróság)
 - ▶ **Másolatot kérhet**, első alkalommal díjmentesen, ha lehetővé teszi a beazonosítását



Hozzáféérés joga 2.

- ▶ Jogos érdek miatt a zárolást (adatkezelés korlátozását) bárki kérheti
- ▶ Ez nem sértheti mások jogait



Adatvédelmi tisztviselő kötelező kijelölése?

GDPR 37. cikk (1) bek. és Preambulum (97) bek.

- 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** az érintettek nagymértékű, rendszeres és szisztematikus nyomon követését teszik szükségessé
- c) **fő tevékenységei** (alaptevékenysége) **során** 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.

➤ De ahol nem kötelező is jó gyakorlat!



Adatvédelmi tisztviselő kötelező kijelölése?

➤ **Nagymértékű**

- érintettek száma (db, vagy %)
- adatok mennyisége és/vagy köre
- tevékenység időtartama vagy állandósága
- földrajzi kiterjedése

➤ **Rendszeres**

- Folyamatosan vagy meghat. időközönként történik egy adott időszakban
- Meghatározott időpontokban ismétlődő vagy megismétlik

➤ **Szisztematikus**

- Egy adott rendszer szerint, stratégia részeként fordul elő
- Előre megszervezett vagy módszeres

- Pl. marketing, pontozás, interneten történő nyomon követés és profilalkotás valamennyi formája, térfigyelő- és biztonsági kamera, GPS alapú helymeghatározás, okoseszközök követése, hűségprogram, stb.



A korábbi előírások és a GDPR viszonya

▶ **Megszokások** – korábbi rossz minták:

- Jogalap jogszabályhelye
- Hozzájárulás helyett tudomásul veszi a tájékoztatást, tiltakozhat!
- Címzett fogalmának változása (adatfeldolgozó mindig, rendőrség csak eseti)
- NAIH nyilvántartás helyett:
 - adatkezelői nyilvántartás
 - adatfeldolgozói nyilvántartás
- Előzetes tájékoztató kötelező **minden esetben**
 - „ne okozzon meglepetést az érintettnek” (használhatjuk, átadhatjuk)
 - nem azonos a hozzáférési joggal – ott minden valóban kezelt adatról tájékoztatni
 - Kivéve Infotv. szerinti bűnüldözési, honvédelmi, nemzetbiztonsági érdek
- Másolatot kérhet az érintett – első alkalommal ingyenesen



Jelentős hatósági ügyek

▶ Tisztességesség követelménye

- ▶ Rejtett megfigyelés általános tilalma: rejtett mikrofon egy benzinkúton – 18 millió Ft bírság
- ▶ Áruházlánc „vetköztető helyiségének” bekamerázása *
- ▶ Munkavállalók egész napos tevékenységének megfigyelése

▶ Átláthatóság követelménye

- ▶ Adatvédelmi tájékoztatóban
 - ▶ „kezelhetjük, összekapcsolhatjuk”
 - ▶ „ügyfélszegmentációs szimulációk elvégzése”
 - ▶ törvény szövegének megismétlése
- ▶ Dolgozók tájékoztatásának hiánya + * - 15 millió Ft bírság

▶ Adatbiztonság követelménye

- ▶ Társasházi kamerarendszer – 500.000 Ft bírság

▶ GDPR – Ausztria:

járdát is figyelte a magáncég, nincs kamera matrica

Az idei év adatvédelmi kihívásai

- ▶ Ágazati jogszabályok – jogharmonizáció
- ▶ Európai Adatvédelmi Testület iránymutatások
- ▶ Választások, kampányok
- ▶ Fogyasztóvédelmi szemlélet erősödése
- ▶ Az első ügyek Magyarországon
- ▶ A GDPR határainak feszegetése





Köszönöm a figyelmet!

dr. Kiss Attila

osztályvezető

Elnöki Kabinet

Adatvédelmi Tanúsítási Osztály

*H-1125 Budapest, Szilágyi Erzsébet fasor 22/C.
H-1530 Budapest, Pf. 5.*

Tel.: +36 391-1400

Fax: +36 391-1410

kiss.attila@naih.hu

ugyfelszolgalat@naih.hu

www.naih.hu

