

A GDPR alkalmazásának hatósági tapasztalatai

Budapest, 2018. szeptember 19.

- Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR)
- Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről

Adatvédelmi hatóságok hatásköre és eljárásai

Hatáskörök

- Vizsgálati
- Korrekciós
- Engedélyezési és tanácsadási
- Bírósági jogorvoslat
- Bírósági eljárásban való részvétel
- További hatáskörök tagállami szabályozástól függően

Egyablakos ügyintézés

60. cikk

- Panasz
- Határon átnyúló adatkezelés?
- Hatóságok közötti egyeztetés – fő és érintett felügyeleti hatóság
- Konszenzusos döntéshozatal
- Vitarendezés a Testület előtt

Egyablakos ügyintézés 60. cikk

- A határozat az EU egész területén érvényesítendő
- Jogorvoslat: a döntéshozatal helye szerinti bíróság előtt

Az Európai Adatvédelmi Testület

- Egységességet szolgáló
vélemények
- Vitarendezési eljárás
- Közös informatikai platform

Az Európai Adatvédelmi Testület véleménye, 64. cikk

- Egységes alkalmazást szolgálja
- Tartalma kötelező a tagállamra nézve
- Véleménytől eltérő tagállami döntés esetén vitarendezési eljárás indul

Kölcsönös segítségnyújtás

A Hatóságok közötti együttműködéssel
összefüggő tapasztalatok

A fő- és érintett felügyeleti hatóságok
azonosítása

Adatvédelmi incidens bejelentése 1. 33-34. cikk

Az adatvédelmi incidens jelentés három szintje

- 1 Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.
[GDPR 33. cikk (5) bekezdés]
- 2 Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
[GDPR 33. cikk (1) bekezdés]
- 3 Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
[GDPR 34. cikk (1) bekezdés]

Adatvédelmi incidens bejelentése 4. 33-34. cikk

| Formanyomtatvány | |
|--|--|
| Bejelentő adatai | pl.: az adatvédelmi tisztviselő elérhetősége |
| Időpontok | pl.: az incidens időpontja, az incidensről való tudomásszerzés időpontja, az esetleges késedelmes jelentés indokai |
| Az adatvédelmi incidens jellege | pl.: eszköz elvesztése vagy ellopása, informatikai rendszer feltörése, rosszindulatú számítógépes programok (zsarolóvírus) |
| Az adatvédelmi incidenssel érintett személyes adatok bemutatása és mennyisége | |
| Érintettek kategóriái | pl.: alkalmazottak, ügyfelek, kiskorúak stb. |
| Az incidens előtt alkalmazott intézkedések | |
| Következmények megjelölése | pl.: bizalmas jelleg sérülése, integritás sérülése, rendelkezésre állás sérülése |
| Az incidens valószínűsíthető hatásai az érintettekre, valamint ezek súlyossága | pl.: az érintetteket ért fizikai, anyagi vagy nem vagyoni károk bemutatása |
| Megtett intézkedések, ideértve az érintettek tájékoztatását | pl.: a tájékoztatás időpontja, formája, tartalma, módja; az adatvédelmi incidens orvoslására tett intézkedések (password reset, patch, update) |
| Egyéb bejelentések | pl.: a vezető hatóságnak bejelentett határokon átnyúló adatvédelmi incidens; az EU felügyeleti hatóságok megnevezése, amelyeket az adatvédelmi incidens érinthet; NIS irányelv szerinti jelentés történt-e |

Nyilvántartás vezetése az adatvédelmi incidensről

Az **adatkezelő** nyilvántartja az **adatvédelmi incidenseket**, feltüntetve az adatvédelmi incidenshez kapcsolódó **tényeket**, annak **hatásait** és az **orvoslására tett intézkedéseket**. E nyilvántartás lehetővé teszi, hogy a **felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést**.

GDPR 33. cikk (5)

Tipikus ügyek

Köszönöm a figyelmet!