4/2019. számú iránymutatás a 25. cikk szerinti beépített és alapértelmezett adatvédelemről

2.0 változat

Elfogadás időpontja: 2020. október 20.

A változatok előzményei

1.0. változat	2019. november 13.	Az iránymutatás nyilvános konzultáció céljából történő elfogadása
2.0 változat	2020. október 20.	Az iránymutatás nyilvános konzultációt követő elfogadása az Európai Adatvédelmi Testület által

Tartalomjegyzék

Az Európai Adatvédelmi Testület

tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 70. cikke (1) bekezdésének e) pontjára,

tekintettel az EGT-megállapodásra és különösen annak az EGT Vegyes Bizottság 2018. július 6-i 154/2018 határozatával módosított XI. mellékletére és 37. jegyzőkönyvére,

tekintettel eljárási szabályzatának 12. és 22. cikkére,

ELFOGADTA A KÖVETKEZŐ IRÁNYMUTATÁST:

Összefoglaló

Egy mindinkább digitalizált világban a beépített és alapértelmezett adatvédelemmel kapcsolatos követelmények betartása döntő szerepet játszik a magánélet védelmének és az adatvédelem társadalmi előmozdításában. Ezért alapvető fontosságú, hogy az adatkezelők komolyan vegyék e felelősséget, és az adatkezelési műveletek tervezésekor eleget tegyenek az általános adatvédelmi rendeletben foglalt kötelezettségeknek.

Ez az iránymutatás az általános adatvédelmi rendelet 25. cikkében megállapított beépített és alapértelmezett adatvédelem követelményével kapcsolatban nyújt általános eligazítást. A beépített és alapértelmezett adatvédelem méretüktől és az adatkezelés összetettségének mértékétől függetlenül minden adatkezelő számára kötelező. Ahhoz, hogy az adatkezelő teljesíteni tudja a beépített és alapértelmezett adatvédelem követelményeit, elengedhetetlen, hogy tisztában legyen az adatvédelmi elvekkel, továbbá az érintettek jogaival és szabadságaival.

Az alapvető kötelezettség azon *megfelelő* intézkedések és szükséges garanciák alkalmazása, amelyek biztosítják az *adatvédelmi elvek* és ebből következően az *érintettek beépített és alapértelmezett jogainak és szabadságainak hatékony érvényesülését*. A 25. cikk előírja, hogy figyelembe kell venni a beépített és alapértelmezett elemeket. Ez az iránymutatás részletesebben kitér ezekre az elemekre.

A 25. cikk (1) bekezdése úgy rendelkezik, hogy az adatkezelőnek már az új adatkezelési művelet tervezésekor szem előtt kell tartania a beépített és alapértelmezett adatvédelmet. Az adatkezelő az adatkezelés *előtt* és az adatkezelés során *folyamatosan* megvalósítja a beépített és alapértelmezett adatvédelmet azáltal, hogy rendszeresen felülvizsgálja a választott intézkedések és garanciák hatékonyságát. A beépített és alapértelmezett adatvédelmet azon már meglévő rendszerek esetében is alkalmazni kell, amelyek személyes adatokat kezelnek.

Az iránymutatás – a fő beépített és alapértelmezett elemek, valamint gyakorlati példák felsorolásával – útmutatást is tartalmaz arra vonatkozóan, hogy miként lehet hatékonyan megvalósítani az 5. cikkben foglalt adatvédelmi elveket. Az adatkezelőnek a konkrét adatkezelési folyamattal összefüggésben kell mérlegelnie a javasolt intézkedések megfelelőségét.

Az Európai Adatvédelmi Testület ajánlásokat fogalmaz meg arra vonatkozóan, hogy az adatkezelők, az adatfeldolgozók és szolgáltatók hogyan működhetnek együtt a beépített és alapértelmezett

adatvédelem megvalósítása érdekében. Arra bátorítja egy adott ágazat adatkezelőit, az adatfeldolgozókat és szolgáltatókat, hogy termékeik adatkezelők és érintettek részére történő értékesítésekor a beépített és alapértelmezett adatvédelmet mint versenyelőnyhöz juttató eszközt alkalmazzák. Ezenfelül minden adatkezelőt tanúsítványok és magatartási kódexek alkalmazására ösztönöz.

1 ALKALMAZÁSI KÖR

1. Az iránymutatás a beépített és alapértelmezett adatvédelemnek az adatkezelők által az általános adatvédelmi rendelet 25. cikkében foglalt kötelezettség alapján történő megvalósítására összpontosít.[1] Más szereplők, például a 25. cikk által közvetlenül nem érintett adatfeldolgozók, valamint a termékek, szolgáltatások és alkalmazások előállítói (a továbbiakban: szolgáltatók) szintén hasznosnak találhatják ezt az iránymutatást az általános adatvédelmi rendeletnek megfelelő olyan termékek és szolgáltatások létrehozásában, amelyek lehetővé teszik az adatkezelők számára, hogy eleget tegyenek adatvédelmi kötelezettségeiknek.[2] Az általános adatvédelmi rendelet (78) preambulumbekezdése hozzáteszi, hogy a beépített és alapértelmezett adatvédelmet figyelembe kell venni a közbeszerzések során. Annak ellenére, hogy minden adatkezelőnek kötelessége, hogy a beépített és alapértelmezett adatvédelmet beépítse adatkezelési tevékenységeibe, ez a rendelkezés előmozdítja az adatvédelmi elvek elfogadását; ezen a területen a közigazgatási szerveknek kell példát mutatniuk. Az adatkezelő felelős azért, hogy az adatfeldolgozói és megbízott adatfeldolgozói által végzett adatfeldolgozás tekintetében teljesüljenek a beépített és alapértelmezett adatvédelem követelményei, ezért erre figyelemmel kell lennie, amikor e felekkel szerződést köt.

2. A 25. cikkben ismertetett követelmény szerint az adatkezelőnek az adatvédelmet alapértelmezés szerint és a teljes adatkezelési életciklusra kiterjedően be kell építenie a személyes adatok kezelésének folyamatába. A beépített és alapértelmezett adatvédelem követelménye az általános adatvédelmi rendelet hatálybalépése előtt meglévő rendszerekre is vonatkozik. Az adatkezelőnek az adatkezelést következetesen naprakésszé kell tennie az általános adatvédelmi rendelettel összhangban. További információk arra vonatkozóan, hogy hogyan feleltethető meg egy meglévő rendszer az általános adatvédelmi rendeletnek, az iránymutatás 2.1.4. alfejezetében találhatók. A rendelkezés lényege, hogy mind *beépített*, mind *alapértelmezett* módon biztosítsa a *megfelelő* és *hatékony* adatvédelmet, ami azt jelenti, hogy az adatkezelőknek képesnek kell lenniük annak bizonyítására, hogy az adatkezelést illetően megfelelő intézkedésekkel és garanciákkal rendelkeznek az adatvédelmi elvek, valamint az érintettek jogai és szabadságai hatékonyságának biztosítására.

3. Az iránymutatás 2. fejezete a 25. cikkben meghatározott követelmények értelmezésére összpontosít, és megvizsgálja a rendelkezés által bevezetett jogi kötelezettségeket. A beépített és alapértelmezett adatvédelem konkrét adatvédelmi elvekkel összefüggésben történő alkalmazásának módjára vonatkozóan példákat a 3. fejezet tartalmaz.

---

[1] Az iránymutatásban foglalt értelmezések a (EU) 2016/680 irányelv 20. cikkére és a 2018/1725 rendelet 27. cikkére is vonatkoznak.

[2] Az általános adatvédelmi rendelet (78) preambulumbekezdése egyértelműen kimondja ennek szükségességét: *„Az olyan alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek, a termékek, szolgáltatások és alkalmazások előállítóit arra kell ösztönözni, hogy e termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védeleméhez való jogot, és a tudomány és technológia állását kellően figyelembe véve gondoskodjanak arról, hogy az adatkezelők és az adatfeldolgozók adatvédelmi kötelezettségeiknek eleget tegyenek.”*

4. Az iránymutatás a 25. cikknek való megfelelés bizonyítására szolgáló tanúsítási mechanizmus létrehozásának lehetőségével a 4. fejezet foglalkozik, az 5. fejezet pedig arra is kitér, hogy a felügyeleti hatóságok hogyan érvényesíthetik az említett cikket. Végezetül az iránymutatás további ajánlásokat fogalmaz meg az érdekelt felek számára a beépített és alapértelmezett adatvédelem sikeres megvalósításának módjára vonatkozóan. Az Európai Adatvédelmi Testület tisztában van azzal, hogy a kis- és középvállalkozások (a továbbiakban: kkv-k) számára mekkora kihívást jelent a beépített és alapértelmezett adatvédelem követelményeinek maradéktalan teljesítése, így a 6. fejezetben további ajánlásokat fogalmaz meg kifejezetten a kkv-k számára.

2 A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEMRŐL SZÓLÓ 25. CIKK (1) ÉS (2) BEKEZDÉSÉNEK ELEMZÉSE

5. E fejezet célja az általános adatvédelmi rendelet 25. cikkének (1) bekezdésében foglalt, a beépített adatvédelemre, illetve az általános adatvédelmi rendelet 25. cikkének (2) bekezdésében foglalt, az alapértelmezett adatvédelemre vonatkozó követelmények megvizsgálása és azokkal kapcsolatban útmutatás nyújtása. A beépített adatvédelem és az alapértelmezett adatvédelem egymást kiegészítő, egymást kölcsönösen megerősítő fogalmak. Az érintettek jobban érvényesíthetik az alapértelmezett adatvédelmet, ha azzal egyidejűleg beépített adatvédelem is megvalósul, és fordítva.

6. A beépített és alapértelmezett adatvédelem minden adatkezelő számára kötelező, ideértve a kisvállalkozásokat és a multinacionális vállalatokat is. Ebből adódóan a beépített és alapértelmezett adatvédelem megvalósításának összetettsége az egyes adatkezelési műveletektől függően változhat. Mérettől függetlenül azonban a beépített és alapértelmezett adatvédelem megvalósításának az adatkezelő és az érintett szempontjából is pozitív hozadékai vannak.

2.1 A 25. cikk (1) bekezdése: beépített adatvédelem

2.1.1 Az adatkezelő kötelezettsége a megfelelő technikai és szervezési intézkedések végrehajtására és a szükséges garanciák adatkezelés folyamatába történő beépítésére

7. A 25. cikk (1) bekezdésével összhangban az adatkezelőnek *megfelelő* technikai és szervezési *intézkedéseket* kell végrehajtania, amelyek célja az adatvédelmi elvek érvényesítése, továbbá a követelmények teljesítéséhez, valamint az érintettek jogainak és szabadságainak védelméhez *szükséges garanciák* beépítése az adatkezelés folyamatába. Mind a megfelelő intézkedések, mind a szükséges garanciák ugyanazt a célt hivatottak szolgálni, az érintettek jogainak védelmét és annak biztosítását, hogy személyes adataik védelme beépüljön az adatkezelés folyamatába.

8. A *technikai és szervezési intézkedések* és a szükséges *garanciák* tágabb értelmezés szerint bármely olyan módszert vagy eszközt jelenthetnek, amelyet az adatkezelő az adatkezelés során alkalmazhat. A *megfelelőség* azt jelenti, hogy az intézkedéseknek és a szükséges garanciáknak a tervezett cél teljesítéséhez kell igazodniuk, azaz *hatékonyan* kell érvényesíteniük az adatvédelmi elveket[3]. A megfelelőség követelménye tehát szorosan kapcsolódik a hatékonyság követelményéhez.

9. Technikai vagy szervezési intézkedés és garancia lehet bármi a fejlett technikai megoldások használatától kezdve a személyzet alapképzéséig. A körülményektől és a szóban forgó adatkezeléstől függően megfelelő példa lehet többek között a személyes adatok álnevesítése[4]; a rendelkezésre álló

[3] A „hatékonysággal” a lenti 2.1.2. alfejezet foglalkozik.
[4] Az általános adatvédelmi rendelet 4. cikkének 5. pontjában szereplő fogalommeghatározás szerint.

személyes adatok tagolt, széles körben használt, géppel olvasható formátumban történő tárolása; az adatfeldolgozásba való beavatkozás lehetővé tétele az érintettek számára; tájékoztatás a személyes adatok tárolásáról; rosszindulatú számítógépes programok észlelésére szolgáló rendszerek alkalmazása; az alkalmazottak alapvető „kiberhigiéniával" kapcsolatos képzése; adatvédelem-kezelési és információbiztonsági irányítási rendszerek létrehozása, szerződésben kötelezve az adatfeldolgozókat meghatározott adattakarékossági gyakorlatok végrehajtására stb.

10. Az adatkezelők különböző kategóriáit képviselő egyesületek és egyéb szervek által elismert szabványok, bevált gyakorlatok és magatartási kódexek segítséget nyújthatnak a megfelelő intézkedések meghatározásához. Az adatkezelőnek azonban az adott adatkezelési folyamattal összefüggésben kell ellenőriznie az intézkedések megfelelőségét.

2.1.2 A cél az adatvédelmi elvek hatékony megvalósítása, valamint az érintettek jogainak és szabadságainak védelme

11. Az *adatvédelmi elveket* az 5. cikk tartalmazza (a továbbiakban: az elvek), az *érintettek jogai és szabadságai* megegyeznek a természetes személyek alapvető jogaival és szabadságaival, különös tekintettel a személyes adatok védelméhez való jogukra, amelyek védelmét az 1. cikk (2) bekezdése az általános adatvédelmi rendelet céljaként jelöli meg (a továbbiakban: a jogok)[5]. Pontos meghatározásuk az Európai Unió Alapjogi Chartájában található. Az adatkezelő számára alapvető fontosságú, hogy tisztában legyen *az elvek* és *a jogok* jelentésével, amelyek az általános adatvédelmi rendelet, és különösen a beépített és alapértelmezett adatvédelemre vonatkozó kötelezettség által nyújtott védelem alapját képezik.

12. A megfelelő technikai és szervezési intézkedések végrehajtása során az intézkedéseket és garanciákat a fent említett elvek, jogok és szabadságok hatékony megvalósítására és a jogok ebből következő védelmére figyelemmel kell *kialakítani*.

A hatékonyság biztosítása

13. A beépített adatvédelem fogalmának középpontjában a hatékonyság áll. Az elvek hatékony érvényesítésének követelménye azt jelenti, hogy az adatkezelőnek ezen elvek védelme érdekében életbe kell léptetnie a szükséges intézkedéseket és garanciákat, hogy az érintettek jogai biztosítottak legyenek. Minden egyes életbe léptetett intézkedésnek a kívánt eredménnyel kell járnia az adatkezelő által tervezett adatkezelési folyamat tekintetében. E megállapításnak két következménye van.

14. Először is a 25. cikk nem követeli meg konkrét technikai és szervezési intézkedések végrehajtását, hanem azt írja elő, hogy a választott intézkedéseknek és garanciáknak az adott adatkezelés esetében kell biztosítaniuk az adatvédelmi elvek érvényesülését. Ennek során az intézkedéseket és garanciákat úgy kell kialakítani, hogy megbízhatóak legyenek, és az adatkezelőnek a kockázat növekedése esetén képesnek kell lennie további intézkedések végrehajtására[6]. Ezért az, hogy az intézkedések hatékonyak-e, az adott adatkezelés körülményeitől és azon elemek értékelésétől függ, amelyeket figyelembe kell

[5] Lásd az általános adatvédelmi rendelet (4) preambulumbekezdését.

[6] „Az adatkezelőkre alkalmazandó alapelveknek (azaz a jogszerűségnek, az adattakarékosságnak, a célhoz kötöttségnek, az átláthatóságnak, az adatok integritásának, az adatok pontosságának) az adatkezeléstől és az érintetteket érintő kockázatoktól függetlenül változatlannak kell maradniuk. Az ilyen adatkezelés jellegének és hatókörének kellő figyelembevétele azonban mindig is szerves részét képezte ezen elvek alkalmazásának, így azok eredendően méretezhetők." A 29. cikk szerinti munkacsoport. „Nyilatkozat a kockázatalapú megközelítés adatvédelmi jogi keretekben betöltött szerepéről". WP 218., 2014. május 30., 3. o. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

venni az adatkezelés módjának meghatározásakor. A fent említett elemekkel a lenti 2.1.3. alfejezet foglalkozik.

15. Másrészt, az adatkezelőknek képesnek kell lenniük arra, hogy igazolják az elvek érvényesülését.

16. A végrehajtott intézkedéseknek és garanciáknak el kell érniük az adatvédelem tekintetében kívánt hatást, és az adatkezelőnek rendelkeznie kell a végrehajtott technikai és szervezési intézkedések dokumentációjával.[7] Ennek érdekében az adatkezelő megfelelő fő teljesítménymutatókat határozhat meg a hatékonyság bizonyítására. A fő teljesítménymutató az adatkezelő által választott, mérhető érték, amely azt mutatja, hogy milyen hatékonysággal teljesíti az adatkezelő adatvédelmi célkitűzését. A fő teljesítménymutatók lehetnek *kvantitatívak*, mint például a hamis pozitív vagy hamis negatív százalékaránya, a panaszok számának csökkenése, a válaszadási idő csökkenése, amikor az érintettek jogaikat gyakorolják, vagy *kvalitatívak*, mint például teljesítményértékelések, minősítési rendszer használata vagy szakértői értékelések. Fő teljesítménymutatók alkalmazása helyett az elvek hatékony érvényesülését az adatkezelő úgy is bizonyíthatja, ha bemutatja, milyen szempontok szerint végzi a választott intézkedések és garanciák hatékonyságának értékelését.

2.1.3 Figyelembe veendő elemek

17. A 25. cikk (1) bekezdése felsorolja azokat az elemeket, amelyeket az adatkezelőnek figyelembe kell vennie egy konkrét adatkezelési művelet intézkedéseinek meghatározásakor. A következőkben útmutatást adunk arra vonatkozóan, hogy miként kell alkalmazni ezen elemeket a tervezési folyamat során, amelynek az alapértelmezett beállítás tervezése is részét képezi. Ezen elemek mindegyike fontos annak eldöntésekor, hogy egy intézkedés megfelelő-e az elvek hatékony érvényesülése szempontjából. Így ezek az elemek nem külön-külön, önmagukban megvalósítandó célok, hanem a célkitűzés elérése érdekében együttesen vizsgálandó tényezők.

2.1.3.1 „a tudomány és technológia állása”

18. „A tudomány és technológia állásának” fogalma számos uniós vívmányban szerepel, például a környezetvédelem és a termékbiztonság területén. Az általános adatvédelmi rendelet nemcsak a 32. cikkben, a biztonsági intézkedések[89] tekintetében, hanem a 25. cikkben is hivatkozik „a tudomány és technológia állására”[10], kiterjesztve ezzel e referenciamutatót az adatkezelésbe beágyazott összes technikai és szervezési intézkedésre.

19. A 25. cikkel összefüggésben „a tudomány és technológia állására” való hivatkozás arra kötelezi az adatkezelőket, hogy a megfelelő technikai és szervezési intézkedések meghatározásakor **vegyék figyelembe** a piacon rendelkezésre álló **technológia jelenlegi fejlettségét**. A követelmény szerint adatkezelőknek ismeretekkel kell rendelkezniük és naprakésznek kell lenniük a technológiai fejlődést, valamint azt illetően, hogy a technológia milyen módon jelenthet adatvédelmi kockázatot vagy

[7] Lásd a (74) és (78) preambulumbekezdést.
[8] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security
[9] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/
[10] Lásd a német szövetségi alkotmánybíróság Kalkar ügyben hozott 1978. évi határozatát (https://germanlawarchive.iuscomp.org/?p=67); e határozat adott esetben megalapozhatja a fogalom objektív meghatározásának módszertanát. Ez alapján „a tudomány és technológia állásának” megfelelő technológiai szintet a „meglévő tudományos ismereteknek és kutatásnak” megfelelő technológiai szint és a bevettebb „általánosan elfogadott technológiai szabályok” között kell meghatározni. „A tudomány és technológia állása” tehát a piacon létező olyan szolgáltatás, technológia vagy termék technológiai szintjeként határozható meg, amely a leghatékonyabb az azonosított célkitűzések elérése szempontjából.

lehetőséget az adatkezelési műveletre nézve, és hogy miként kell megvalósítani és naprakésszé tenni azokat az intézkedéseket és garanciákat, amelyek *biztosítják* az elvek és az érintettek jogainak *hatékony érvényesítését* a technológiai környezetre tekintettel.

20. „A tudomány és technológia állása" egy dinamikus fogalom, amely nem határozható meg statikus módon egy adott időpontban, hanem azt a technológiai fejlődés összefüggésében *folyamatosan* értékelni kell. A technológiai fejlődés fényében az adatkezelő megállapíthatja, hogy egy olyan intézkedés, amely korábban megfelelő szintű védelmet biztosított, már nem nyújt ilyen védelmet. A technológiai változások figyelemmel kísérésének elmulasztása ezért a 25. cikknek való megfelelés hiányához vezethet.

21. „A tudomány és technológia állására" vonatkozó kritérium nemcsak a technológiai intézkedések, hanem a szervezési intézkedések esetében is alkalmazandó. A megfelelő szervezési intézkedések hiánya csökkentheti vagy akár teljes mértékben alá is áshatja a választott technológia hatékonyságát. A szervezési intézkedések közé tartozik például a belső szabályzatok elfogadása, a naprakész technológiai, biztonsági és adatvédelmi képzés, valamint az informatikabiztonság-irányítási és -kezelési szabályzatok.

22. A különböző területeken meglévő és elfogadott keretek, szabványok, tanúsítványok, magatartási kódexek stb. szerepet játszhatnak abban, hogy megmutassák „a tudomány és technológia aktuális állását" az adott felhasználási területen. Amennyiben léteznek ilyen szabványok és azok a jogi követelményeknek megfelelően vagy azokat meghaladva magas szintű védelmet nyújtanak az érintettek számára, az adatkezelőnek azokat figyelembe kell vennie az adatvédelmi intézkedések megtervezésekor és megvalósításakor.

2.1.3.2 „a megvalósítás költségei"

23. Az adatkezelő a megvalósítás költségeire is figyelemmel lehet azon megfelelő technikai és szervezési intézkedések, illetve szükséges garanciák kiválasztásakor és alkalmazásakor, amelyekkel az érintettek jogainak védelme érdekében hatékonyan érvényesíthetők az elvek. A költségek általánosságban az erőforrásokra vonatkoznak, ideértve az időt és az emberi erőforrásokat is.

24. A költségelem nem kívánja meg az adatkezelőtől aránytalan mértékű erőforrás ráfordítását, ha már léteznek más, kevésbé erőforrásigényes, de hatékony intézkedések. A megvalósítás költsége mindazonáltal olyan tényező, amelyet a beépített adatvédelem megvalósításakor figyelembe kell venni, okot viszont nem adhat a megvalósítás elmaradására.

25. A választott intézkedéseknek tehát a költségektől függetlenül biztosítaniuk kell, hogy az adatkezelő által tervezett adatkezelési tevékenység keretében ne kezeljenek az elvekkel össze nem egyeztethető módon személyes adatokat. Az adatkezelőnek a teljes költséggel tudnia kell gazdálkodni ahhoz, hogy hatékonyan szerezhessen érvényt minden elvnek és így a jogok védelmének.

2.1.3.3 „az adatkezelés jellege, hatóköre, körülményei és céljai"

26. Az adatkezelőnek a szükséges intézkedések meghatározásakor figyelemmel kell lennie az adatkezelés jellegére, hatókörére, körülményeire és céljaira.

27. Az adatvédelmi elveknek az adatkezelés folyamatába történő beépítése érdekében ezeket a tényezőket az általános adatvédelmi rendelet egyéb rendelkezéseiben, például a 24., 32. és 35. cikkében betöltött szerepükkel összhangban kell értelmezni.

28. Röviden, a **jelleg** fogalma az adatkezelés sajátos[11] jellemzőjeként értelmezhető. A **hatókör** az adatkezelés méretére és terjedelmére vonatkozik. A **körülmények** az adatkezelés körülményeire vonatkoznak, amelyek befolyásolhatják az érintett elvárásait, a **cél** pedig az adatkezelés céljaihoz kapcsolódik.

2.1.3.4 „a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat"

29. Az általános adatvédelmi rendelet koherens kockázatalapú megközelítést alkalmaz több rendelkezésében – a 24., 25., 32. és 35. cikkben – a megfelelő technikai és szervezési intézkedéseknek az egyének és személyes adataik védelme, valamint az általános adatvédelmi rendelet követelményeinek való megfelelés érdekében történő meghatározása céljából. A védendő értékek mindig azonosak (az egyének személyes adataik védelme révén) ugyanazokkal az (egyének jogaira jelentett) kockázatokkal szemben, ugyanazokat a feltételeket (az adatkezelés jellegét, hatókörét, körülményeit és céljait) figyelembe véve.

30. A 25. cikknek való megfelelés céljából végzett kockázatelemzéskor az adatkezelőnek azonosítania kell az elvek sérülése esetén az érintettek jogaira jelentett kockázatokat, valamint meg kell határoznia azok előfordulásának valószínűségét és súlyosságukat, hogy a feltárt kockázatok hatékony mérséklése végett intézkedéseket léptethessen életbe. Kockázatértékeléskor létfontosságú az adatkezelés folyamatának szisztematikus és alapos értékelése. Az adatkezelő például a gyermekek és 18 év alatti fiatalok mint kiszolgáltatott csoport személyes adatainak kezelésével összefüggésben értékeli az önként adott hozzájárulás elmaradásával – ami sérti a jogszerűség elvét – járó konkrét kockázatokat, amely esetben az adatkezelésnek nincs más jogalapja, és megfelelő intézkedéseket léptet életbe az érintettek e csoportjával kapcsolatban feltárt kockázatok kezelése és hatékony mérséklése érdekében.

31. Az Európai Adatvédelmi Testület adatvédelmi hatásvizsgálat elvégzéséről szóló iránymutatása,[12] amely annak megállapítására összpontosít, hogy egy adatkezelési művelet az érintettre nézve valószínűsíthetően magas kockázattal jár-e vagy sem, útmutatást nyújt az adatvédelmi kockázatok értékelésének és az adatvédelmi kockázatértékelés elvégzésének módjáról is. Ezen iránymutatás valamennyi fent említett cikk – többek között a 25. cikk – esetében is hasznos lehet a kockázatértékelés során.

32. A kockázatalapú megközelítés nem zárja ki alapértékek, legjobb gyakorlatok és szabványok alkalmazását. Ezek hasznos eszköztárral szolgálhatnak az adatkezelők számára hasonló helyzetekben (az adatkezelés jellege, hatóköre, körülményei és célja) hasonló kockázatok kezeléséhez. Mindazonáltal továbbra is fennáll a 25. cikkben (valamint a 24. és a 32. cikkben, továbbá a 35. cikk (7) bekezdésének c) pontjában) foglalt azon kötelezettség, hogy figyelembe kell venni „*a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat[ot]*". Ezért annak ellenére, hogy ilyen eszközök rendelkezésükre állnak, az adatkezelőknek minden egyes esetben el kell végezniük az adott adatkezelési tevékenységgel kapcsolatos adatvédelmi kockázatok értékelését, és ellenőrizniük kell a javasolt megfelelő intézkedések és garanciák hatékonyságát. Ezt

[11] A példák közé tartoznak a személyes adatok különleges kategóriái, az automatikus döntéshozatal, az egyenlőtlen erőviszonyok, a kiszámíthatatlan adatkezelés, az érintettek nehézségei a jogok gyakorlása terén stb.

[12] A 29. cikk szerinti munkacsoport, „Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában »valószínűsíthetően magas kockázattal jár«-e". WP 248 rev.01, 2017. október 4. ec.europa.eu/newsroom/document.cfm?doc_id=47711 – az Európai Adatvédelmi Testület által jóváhagyva.

követően adatvédelmi hatásvizsgálatra vagy a meglévő adatvédelmi hatásvizsgálat frissítésére is szükség lehet.

2.1.4 Időtényező

2.1.4.1 Az adatkezelés módjának meghatározásakor

33. A beépített adatvédelmet „*az adatkezelés módjának meghatározásakor*” kell megvalósítani.

34. „*Az adatkezelés módja*” az általánostól a részletes tervezési elemekig terjed, beleértve a felépítést, az eljárásokat, a protokollokat, az elrendezést és a megjelenést.

35. „*Az adatkezelési mód[ja] meghatározás[ának ideje]*” arra az időszakra vonatkozik, amikor az adatkezelő dönt az adatkezelés elvégzésének módjáról és arról, hogy miként kerül sor az adatkezelésre, valamint az adatkezelés elvégzéséhez alkalmazandó mechanizmusokról. Az adatkezelőnek az ilyen döntések meghozatala során kell értékelnie azokat a megfelelő intézkedéseket és garanciákat, amelyek lehetővé teszik az elvek és az érintettek jogainak az adatkezelés során történő hatékony megvalósítását, és figyelembe kell vennie olyan elemeket, mint a tudomány és technológia állása, a megvalósítás költségei, a jelleg, a hatókör, a körülmények és a cél, valamint a kockázatok. Idetartozik az adatkezelő szoftver, hardver és szolgáltatások beszerzéséhez és bevezetéséhez szükséges idő is.

36. A beépített és alapértelmezett adatvédelem korai figyelembevétele kulcsfontosságú az elvek érvényesítéséhez és az érintettek jogainak védelméhez. Költség-haszon szempontból továbbá az adatkezelők érdeke is, hogy a beépített és alapértelmezett adatvédelmet minél hamarabb figyelembe vegyék, mivel a már elkészített terveken és a már megtervezett adatkezelési műveleteken a későbbiekben nehéz és költséges lehet változtatásokat eszközölni.

2.1.4.2 Az adatkezelés során (karbantartás és az adatvédelmi követelmények felülvizsgálata)

37. Az adatkezelés megkezdését követően az adatkezelőnek a jogok védelme érdekében kötelessége folyamatosan gondoskodnia a beépített és alapértelmezett adatvédelemről, azaz az elvek folyamatos, hatékony érvényesüléséről, naprakésznek kell lennie a tudomány és technológia állásával kapcsolatban, újból értékelnie kell a kockázat szintjét stb. Az adatkezelési műveletek jellege, hatóköre és körülményei, valamint a kockázatok is változhatnak az adatkezelés során, így az adatkezelőnek a választott intézkedések és garanciák rendszeres felülvizsgálatával és újbóli értékelésével ismételten értékelnie kell adatkezelési műveleteit.

38. Az adatkezelési művelet karbantartásának, felülvizsgálatának és szükség esetén naprakésszé tételének kötelezettsége a korábban meglévő rendszerekre is vonatkozik. Ez azt jelenti, hogy a már az általános adatvédelmi rendelet hatálybalépése előtt kialakított rendszereket felülvizsgálatnak és karbantartásnak kell alávetni az elvek és az érintettek jogainak hatékony érvényesülését szolgáló intézkedések és garanciák megvalósításának biztosítása érdekében, az ebben az iránymutatásban foglaltak szerint.

39. Ez a kötelezettség kiterjed az adatfeldolgozók közreműködésével végzett bármely adatkezelésre is. Az adatfeldolgozók műveleteit az adatkezelőnek rendszeresen felül kell vizsgálnia és értékelnie kell annak biztosítása érdekében, hogy lehetővé tegyék az elveknek való folyamatos megfelelést és az adatkezelő e tekintetben fennálló kötelezettségeinek teljesítését.

2.2 A 25. cikk (2) bekezdése: alapértelmezett adatvédelem

2.2.1 Alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerül sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek

40. A számítástechnikában használt általános meghatározás szerint az „alapértelmezés” egy szoftveralkalmazáshoz, számítógépes programhoz vagy eszközhöz rendelt konfigurálható beállítás előzetesen meglévő vagy előzetesen kiválasztott értékét jelenti. Az ilyen beállításokat „alap” vagy „gyári” beállításnak is nevezik, különösen az elektronikus eszközök esetében.

41. A személyes adatok kezelése során tehát az „alapértelmezés szerint” kifejezés egy adott adatkezelő rendszerben meghatározott vagy előírt konfigurációs értékekkel vagy adatkezelési lehetőségekkel, például szoftveralkalmazással, szolgáltatással vagy eszközzel, vagy manuális adatkezelési eljárással kapcsolatos választásokra vonatkozik, amelyek kihatással vannak a gyűjtött személyes adatok mennyiségére, kezelésének mértékére, tárolásának időtartamára és hozzáférhetőségére.

42. Az adatkezelőnek oly módon kell megválasztania az adatkezelés alapértelmezett beállításait és lehetőségeit, illetve felelősséget vállalnia azok végrehajtásáért, hogy alapértelmezés szerint kizárólag a meghatározott, jogszerű cél eléréséhez feltétlenül szükséges adatkezelésre kerüljön sor. E vonatkozásban az adatkezelőknek az adatkezelés szükségességét illetően a 6. cikk (1) bekezdésében foglalt jogalapokra tekintettel elvégzett értékelésükre kell támaszkodniuk. Ez azt jelenti, hogy alapértelmezés szerint az adatkezelő nem gyűjthet a szükségesnél több adatot, a gyűjtött adatokat csak az adatgyűjtés céljához szükséges mértékben kezelheti, és az adatokat nem tárolhatja a szükségesnél hosszabb ideig. Alapvető követelmény, hogy az adatvédelem alapértelmezés szerint beépüljön az adatkezelés folyamatába.

43. Az adatkezelőnek előre meg kell határoznia a személyes adatok gyűjtésének és kezelésének meghatározott, egyértelmű és jogszerű célját.[13] Az intézkedéseknek alapértelmezés szerint megfelelőnek kell lenniük annak biztosítására, hogy kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Az európai adatvédelmi biztosnak a személyes adatok védelméhez való jogot korlátozó intézkedések szükségességének és arányosságának értékelésére vonatkozó iránymutatása hasznos lehet annak eldöntéséhez is, hogy mely adatokat szükséges kezelni egy adott cél eléréséhez.[14] [15] [16]

44. Ha az adatkezelő harmadik féltől származó vagy kész szoftvert alkalmaz, a termékre vonatkozóan kockázatértékelést kell végeznie, és gondoskodnia kell arról, hogy a jogalap nélküli vagy az adatkezelés céljával nem összeegyeztethető funkciókat kikapcsolják.

45. Ugyanezek a megfontolások vonatkoznak az adatkezelési műveleteket támogató szervezési intézkedésekre is. Azokat – kezdetben – csak az adott műveletekhez szükséges minimális mennyiségű személyes adat kezelésére kell kialakítani. Ezt különösen figyelembe kell venni, amikor a különböző

[13] Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének b), c), d) és e) pontja.
[14] Európai adatvédelmi biztos. „Iránymutatás az adatvédelemhez való jogot korlátozó intézkedések szükségességének és arányosságának értékeléséről”. 2019. február 25. edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf
[15] Lásd még: Európai adatvédelmi biztos. „A személyes adatok védelméhez való alapvető jogot korlátozó intézkedések szükségességének értékelése: eszköztár” https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] A szükségességgel kapcsolatos további információkért lásd: A 29. cikk szerinti munkacsoport. „06/2014. számú vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról”. WP 217, 2014. április 9. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf

feladatokat ellátó és különböző hozzáférést igénylő személyzet részére biztosítják az adatokhoz való hozzáférést.

46. Az alapértelmezett adatvédelemmel összefüggésben a megfelelő „technikai és szervezési intézkedések” kifejezést tehát a fenti 2.1.1. alfejezetben kifejtetteknek megfelelően kell értelmezni, de az említett alfejezet szerinti értelmezést kifejezetten az adattakarékosság elvére kell alkalmazni.

47. A kizárólag az adott konkrét cél szempontjából szükséges személyes adatok kezelésére vonatkozó fent említett kötelezettség a következő elemekre vonatkozik:

2.2.2 Az adattakarékossági kötelezettség dimenziói

48. A 25. cikk (2) bekezdése felsorolja az alapértelmezett adatkezelésre vonatkozó adattakarékossági kötelezettség dimenzióit, ennek megfelelően a kötelezettség kiterjed a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre.

2.2.2.1 „a gyűjtött személyes adatok mennyisége”

49. Az adatkezelőknek figyelembe kell venniük mind a személyes adatok mennyiségét, mind az adatkezeléshez szükséges személyes adatok típusait, kategóriáit és részletességét. Az adatkezelők kialakításkal kapcsolatos döntéseinek figyelembe kell venniük az integritás és a bizalmas jelleg, az adattakarékosság és a korlátozott tárolhatóság elvére jelentett fokozott kockázatot nagy mennyiségű részletes személyes adat gyűjtése során, és e kockázatot össze kell vetniük az érintettekkel kapcsolatos kevesebb és/vagy kevésbé részletes információk gyűjtése által jelentett kisebb kockázattal. Az alapértelmezett beállítás semmiképpen nem foglalhatja magában olyan személyes adatok gyűjtését, amelyek nem szükségesek a konkrét adatkezelési cél eléréséhez. Más szóval, ha a személyes adatok bizonyos kategóriái szükségtelenek, vagy ha részletes adatokra azért nincs szükség, mert kevésbé részletes adatok is elegendőek, a felesleges személyes adatok nem gyűjthetők.

50. Ugyanezen alapértelmezett követelmények vonatkoznak a szolgáltatásokra is az alkalmazott platformtól vagy eszköztől függetlenül, kizárólag az adott cél eléréséhez szükséges személyes adatok gyűjthetők.

2.2.2.2 „kezelésük mértéke”

51. A személyes adatokon végzett adatkezelési[17] műveleteknek a szükségesre kell korlátozódniuk. Egy adatkezelési célhoz számos adatkezelési művelet hozzájárulhat. Mindazonáltal önmagában az, hogy egy cél eléréséhez személyes adatokra van szükség, nem jelenti azt, hogy bármilyen típusú és számú adatkezelési művelet elvégezhető az adatokon. Az adatkezelőknek ügyelniük kell arra is, hogy ne terjesszék ki a 6. cikk (4) bekezdése szerinti „összeegyeztethető célok” határait, és szem előtt kell tartaniuk, hogy milyen adatkezelés felel meg az érintettek észszerű elvárásainak.

2.2.2.3 „tárolásuk időtartama”

52. A gyűjtött személyes adatok nem tárolhatók, ha arra az adatkezelés céljának eléréséhez nincs szükség, és annak nincs más, a 6. cikk (4) bekezdése szerinti összeegyeztethető célja és jogalapja. Az

[17] Az általános adatvédelmi rendelet 4. cikkének 2. pontja szerint ez a gyűjtést, rögzítést, rendszerezést, tagolást, tárolást, átalakítást vagy megváltoztatást, lekérdezést, betekintést, felhasználást, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján történő közlést, összehangolást vagy összekapcsolást, korlátozást, törlést, illetve megsemmisítést foglalja magában.

adatmegőrzésnek szükség szerint az adatkezelő által objektíven indokolhatónak kell lennie az elszámoltathatóság elvével összhangban.

53. Az adatkezelőnek az adatmegőrzés időtartamát az adott cél eléréséhez szükségesre kell korlátoznia. Ha a személyes adatokra az adatkezelés céljának eléréséhez már nincs szükség, azokat alapértelmezés szerint törölni vagy anonimizálni kell. Az adatmegőrzés időtartama ezért az adott adatkezelés céljától függ. Ez a kötelezettség közvetlenül kapcsolódik a korlátozott tárolhatóság 5. cikk (1) bekezdésének e) pontjában foglalt elvéhez, és alapértelmezés szerint meg kell valósulnia, vagyis az adatkezelőnek az adatkezelés folyamatába beépített szisztematikus adattörlési vagy anonimizálási eljárásokkal kell rendelkeznie.

54. A személyes adatok anonimizálása[18] a törlés alternatívája, feltéve, hogy az összes releváns kontextuális elemet figyelembe veszik, és rendszeresen értékelik a kockázat – az újraazonosítási kockázatot is ideértve – valószínűségét és súlyosságát.[19]

2.2.2.4 „hozzáférhetőségük”

55. Az adatkezelőnek a szükségesség értékelése alapján korlátoznia kell, hogy ki és milyen típusú személyes adatokhoz férhet hozzá, és azt is biztosítania kell, hogy a személyes adatok szükség esetén – például kritikus helyzetekben – ténylegesen hozzáférhetők legyenek azok számára, akiknek szükségük van azokra. Az adatkezelés során a teljes adatáramlás tekintetében be kell tartani a hozzáférés ellenőrzését.

56. A 25. cikk (2) bekezdése kimondja továbbá, hogy a személyes adatok a természetes személy beavatkozása nélkül nem válhatnak hozzáférhetővé meghatározatlan számú személy számára. Az adatkezelőnek alapértelmezés szerint korlátoznia kell a hozzáférhetőséget, és lehetőséget kell adnia az érintettnek a beavatkozásra, mielőtt meghatározatlan számú természetes személy számára közzéteszi vagy egyéb módon hozzáférhetővé teszi az érintettre vonatkozó személyes adatokat.

57. A személyes adatok meghatározatlan számú személy számára történő hozzáférhető tétele az adatok eredetileg tervezettnél szélesebb körben történő terjesztését eredményezheti. Ez különösen az internet és a keresőmotorok összefüggésében bír jelentőséggel. Ez azt jelenti, hogy az adatkezelőnek alapértelmezés szerint lehetőséget kell adnia az érintetteknek a beavatkozásra, mielőtt a személyes adatok a nyílt interneten hozzáférhetővé válnak. Ez különösen fontos a gyermekek és a kiszolgáltatott csoportok esetében.

58. Az adatkezelés jogalapjától függően a beavatkozás lehetősége az adatkezelés körülményei alapján eltérő lehet. Például hozzájárulás kérése a személyes adatok nyilvánosan hozzáférhetővé tételéhez vagy adatvédelmi beállítások alkalmazása, hogy az érintettek maguk szabályozhassák a nyilvános hozzáférést.

[18] A 29. cikk szerinti munkacsoport. „05/2014. számú vélemény az anonimizálási technikákról” WP 216, 2014. április 10. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf

[19] Lásd: az általános adatvédelmi rendelet 4. cikkének 1. pontja és (26) preambulumbekezdése, valamint a 29. cikk szerinti munkacsoport 05/2014. számú véleménye az anonimizálási technikákról. Lásd még a jelen dokumentum 3. szakaszának a „Korlátozott tárolhatóság” című alszakaszát, amely arra hivatkozik, hogy az adatkezelőnek biztosítania kell az alkalmazott anonimizálási technika (technikák) hatékonyságát.

59. Még ha a személyes adatokat az érintett hozzájárulásával és beleegyezésével teszik is nyilvánosan hozzáférhetővé, ez nem jelenti azt, hogy a személyes adatokhoz hozzáféréssel rendelkező bármely más adatkezelő saját céljaira szabadon kezelheti azokat, hanem saját jogalappal kell rendelkeznie.[20]

3 AZ ADATVÉDELMI ELVEK MEGVALÓSÍTÁSA A SZEMÉLYES ADATOK KEZELÉSE SORÁN BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM RÉVÉN

60. Az adatkezelőnek az adatkezelési tevékenységek tervezésének minden szakaszában – a közbeszerzést, az ajánlattételi felhívást, a kiszervezést, a fejlesztést, a támogatást, a karbantartást, a tesztelést, a tárolást, a törlést stb. is ideértve – figyelembe kell vennie és mérlegelnie kell a beépített és alapértelmezett adatvédelem különböző elemeit, amelyeket az e fejezetben szereplő, az elvek megvalósításának összefüggésébe helyezett példák szemléltetnek.[21] [22] [23]

61. Az adatkezelőnek a beépített és alapértelmezett adatvédelem biztosításához meg kell valósítania az elveket. Ezek az elvek többek között a következők: átláthatóság, jogszerűség, tisztességes eljárás, célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság, integritás és bizalmas jelleg, valamint elszámoltathatóság. Ezeket az elveket az általános adatvédelmi rendelet 5. cikke és (39) preambulumbekezdése ismerteti. Annak teljes körű megértéséhez, hogy hogyan valósítható meg a beépített és alapértelmezett adatvédelem, fontos tudni, hogy ezek az elvek egyenként mit jelentenek.

62. A beépített és alapértelmezett adatvédelem megvalósítására vonatkozó példák bemutatása keretében minden egyes elv esetében felsoroljuk **a beépített és alapértelmezett adatvédelem fő elemeit**. A példák, miközben kiemelik a szóban forgó konkrét adatvédelmi elvet, átfedésben lehetnek más, szorosan kapcsolódó elvekkel is. Az Európai Adatvédelmi Testület hangsúlyozza, hogy az alábbiakban bemutatott fő elemek és példák se nem teljes körűek, se nem kötelező jellegűek, csupán útmutatásul szolgálnak az egyes elvek tekintetében. Az adatkezelőnek értékelnie kell, hogy hogyan biztosítható az elveknek való megfelelés az adott adatkezelési művelettel összefüggésben.

63. Jóllehet ez a szakasz az elvek érvényesítésére összpontosít, az adatkezelőnek *megfelelő* és *hatékony* módszereket is alkalmaznia kell az érintettek jogainak védelme érdekében az általános adatvédelmi rendelet III. fejezete szerint is, amennyiben maguk az elvek nem szereznek érvényt ennek.

64. Az elszámoltathatóság elve átfogó elv: megköveteli az adatkezelőtől, hogy felelősséggel válassza meg a szükséges technikai és szervezési intézkedéseket.

3.1 Átláthatóság[24]

[20] Lásd: Satakunnan Markkinapörssi Oy és Satamedia Oy kontra Finnország, 931/13. sz. ügy.
[21] További példák találhatók a norvég adatvédelmi hatóságnál. „Software Development with Data Protection by Design and by Default" („Beépített és alapértelmezett adatvédelmet biztosító szoftverfejlesztés"). 2017. november 28. www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf
[24] Az átláthatóság fogalmának értelmezésével kapcsolatos részletek tekintetében lásd: a 29. cikk szerinti munkacsoport. „Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról". WP 260 rev.01, 2018. április 11. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=54194 – az Európai Adatvédelmi Testület által jóváhagyva

65. Az adatkezelőnek egyértelműen és nyíltan közölnie kell az érintettel a személyes adatok gyűjtésének, felhasználásának és megosztásának módját. Az átláthatóság azt jelenti, hogy lehetővé kell tenni az érintettek számára, hogy megértsék a 15–22. cikkben foglalt jogaikat, és szükség esetén éljenek azokkal. Az elvet a 12., 13., 14. és 34. cikk tartalmazza. Az átláthatóság elvének támogatására bevezetett intézkedéseknek és garanciáknak e cikkek végrehajtását is támogatniuk kell.

66. Az átláthatóság elvének fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:

- Egyértelműség – az információknak világosan és közérthetően megfogalmazottnak, tömörnek és érthetőnek kell lenniük.
- Szemantika – a tájékoztatásnak egyértelmű jelentéssel kell bírnia a szóban forgó közönség számára.
- Hozzáférhetőség – az információknak könnyen hozzáférhetőnek kell lenniük az érintett számára.
- Kontextualitás – az információkat a megfelelő időpontban és formában kell megadni.
- Relevancia – az információknak relevánsnak kell lenniük, és a konkrét érintettre kell vonatkozniuk.
- Egyetemes tervezés – az információknak minden érintett számára hozzáférhetőnek kell lenniük, ideértve a géppel olvasható nyelvek használatát is az olvashatóság és az érthetőség elősegítése és automatizálása érdekében.
- Érthetőség – az érintetteknek megfelelő ismeretekkel kell rendelkezniük arról, hogy mit várhatnak el személyes adataik kezelése tekintetében, különösen akkor, ha az érintettek gyermekek vagy más kiszolgáltatott csoportok.
- Többcsatornás jelleg – az információkat különböző csatornákon és médiumokon keresztül, nem csupán szöveges változatban kell megadni annak érdekében, hogy az információk minél nagyobb valószínűséggel ténylegesen eljussanak az érintetthez.
- Többrétegűség – a teljesség és érthetőség egyidejű biztosítása érdekében többrétegű tájékoztatást kell nyújtani az érintettek észszerű elvárásainak figyelembevételével.

Példa[25]

Az adatkezelő adatvédelmi szabályzatot dolgoz ki és azt közzéteszi webhelyén az átláthatósági követelményeknek való megfelelés érdekében. Az adatvédelmi szabályzat ne legyen túl terjedelmes, az átlagos érintett számára nehezen felfogható és érthető. Azt világosan és tömören kell megfogalmazni úgy, hogy a webhely felhasználója könnyen megértse, hogy személyes adatait hogyan kezelik. Az adatkezelő ezért többrétegű tájékoztatást nyújt, amelyben kiemeli a legfontosabb pontokat. A részletesebb információkat könnyen hozzáférhetővé kell tenni. Az adatkezelő legördülő menüket és más oldalakra mutató linkeket biztosít annak érdekében, hogy érthetőbbé tegye a nyilatkozatban szereplő elemeket és fogalmakat. Az adatkezelő arról is gondoskodik, hogy a tájékoztatás többcsatornás módon történjen, és videoklipeket biztosít az írásbeli tájékoztatás legfontosabb pontjainak ismertetésére. A különböző oldalak közötti szinergia alapvető annak biztosításához, hogy a többrétegű tájékoztatás ne fokozza, hanem csökkentse a zavart.

Az adatvédelmi szabályzathoz való hozzáférés nem lehet nehéz az érintettek számára. Az adatvédelmi szabályzat így elérhető és látható a szóban forgó honlap valamennyi weblapján, így az érintett mindig csak egy kattintásra van attól, hogy hozzáférjen az információkhoz. A rendelkezésre bocsátott

[25] A francia adatvédelmi hatóság számos példát tett közzé a felhasználók tájékoztatásának legjobb gyakorlatairól, valamint más átláthatósági elvekről: https://design.cnil.fr/en/.

információkat emellett az egyetemes tervezés legjobb gyakorlataival és szabványaival összhangban úgy alakították ki, hogy azok mindenki számára hozzáférhetők legyenek.

Ezenkívül a szükséges információkat megfelelő időben és körülmények között kell megadni. Mivel az adatkezelő a webhelyen gyűjtött adatokkal számos adatkezelési művelet végez, a webhelyen közzétett általános adatvédelmi szabályzat önmagában nem elegendő ahhoz, hogy az adatkezelő teljesítse az átláthatóság követelményeit. Az adatkezelő ezért olyan információáramlást alakít ki, amely az érintettet a megfelelő körülmények között releváns információkkal látja el, például információmorzsákat vagy felugró ablakokat használva. Például amikor az adatkezelő arra kéri az érintettet, hogy adja meg személyes adatait, tájékoztatja az érintettet a személyes adatok kezelésének módjáról és arról, hogy az adott személyes adatokra miért van szükség az adatkezeléshez.

3.2 Jogszerűség

67. Az adatkezelőnek meg kell határoznia a személyes adatok kezelésének érvényes jogalapját. Az intézkedéseknek és garanciáknak támogatniuk kell az annak biztosítására vonatkozó követelményt, hogy az adatkezelés teljes életciklusa összhangban legyen az adatkezelésmegfelelő jogalapjaival.

68. A jogszerűség fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
- Relevancia – az adatkezelésre a megfelelő jogalapot kell alkalmazni.
- Differenciálás[26] – meg kell különböztetni az egyes adatkezelési tevékenységek esetében alkalmazott jogalapokat.
- Meghatározott cél – a megfelelő jogalapnak egyértelműen az adatkezelés meghatározott céljához kell kapcsolódnia.[27]
- Szükségesség – az adatkezelésnek szükségesnek és feltétel nélkülinek kell lennie ahhoz, hogy jogszerű legyen.
- Autonómia – az érintett számára a lehető legnagyobb mértékű autonómiát kell biztosítani a személyes adatok feletti ellenőrzés tekintetében a jogalap keretein belül.
- Az érintett hozzájárulásának megszerzése – az érintett hozzájárulásának önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie.[28] Külön figyelmet kell fordítani arra, hogy a gyermekek és fiatalok képesek-e előzetes tájékoztatáson alapuló hozzájárulást adni.
- Hozzájárulás visszavonása – amennyiben hozzájárulás az adatkezelés jogalapja, a hozzájárulás visszavonását is lehetővé kell tenni. A visszavonásnak ugyanolyan egyszerűnek kell lennie, mint a hozzájárulás megadásának. Ellenkező esetben az adatkezelő hozzájárulási mechanizmusa nem felel meg az általános adatvédelmi rendeletnek.[29]
- Érdekek mérlegelése – amennyiben az adatkezelés jogalapja jogos érdek, az adatkezelőnek mérlegelnie kell a különböző érdekeket, külön figyelmet fordítva a kiegyensúlyozatlan erőviszonyokra, különösen a 18 év alatti gyermekek és más kiszolgáltatott csoportok esetében.

[26] Európai Adatvédelmi Testület. „2/2019 iránymutatás a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében". 2.0. változat, 2019. október 8. edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf

[27] Lásd alább a célhoz kötöttségről szóló szakaszt.

[28] Lásd: 05/2020. sz. iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[29] Lásd: 05/2020. sz. iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról, 24. o. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Az érintettekre gyakorolt kedvezőtlen hatás mérséklésére intézkedéseket és garanciákat kell életbe léptetni.

- Előzetes meghatározás – a jogalapot az adatkezelés előtt kell megállapítani.
- Megszűnés – ha a jogalap alkalmazandósága megszűnik, az adatkezelés ennek megfelelően megszűnik.
- Kiigazítás – ha az adatkezelés jogalapja érvényesen megváltozik, a folyamatban lévő adatkezelést az új jogalapnak megfelelően ki kell igazítani.[30]
- A felelősség megosztása – közös adatkezelés tervezése esetén a feleknek egyértelmű és átlátható módon meg kell osztaniuk az érintettel szembeni felelősségüket, és az adatkezelési intézkedéseket e felelősségmegosztásnak megfelelően kell megtervezni.

Példa

Egy bank szolgáltatás nyújtását tervezi a hitelkérelmek kezelésének hatékonyabbá tétele érdekében. A szolgáltatás mögött az az elképzelés húzódik meg, hogy a bank az ügyfél engedélyének kikérésével tud az ügyfélről adatokat közvetlenül lekérni az állami adóhatóságtól. Ez a példa más forrásból származó személyes adatok kezelését nem szemlélteti.

Az érintett pénzügyi helyzetével kapcsolatos személyes adatok megszerzésére a hitelszerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez van szükség.[31] Nincs szükség azonban arra, hogy a személyes adatokat közvetlenül az adóhatóságtól szerezzék meg, mert az ügyfél szerződést köthet és saját maga adhatja meg az adóhatóságtól származó információkat. Bár a banknak jogos érdeke fűződik ahhoz, hogy a dokumentumokat közvetlenül az adóhatóságtól szerezze meg, például a hitelkérelem hatékony feldolgozása érdekében, ha a bank közvetlen hozzáférést kap a hiteligénylő személyes adataihoz, az kockázatot jelent a hozzáférési jogok gyakorlása vagy az azokkal való esetleges visszaélés tekintetében.

A jogszerűség elvének megvalósítása során az adatkezelő felismeri, hogy ebben az esetben nem használhatja fel a „szerződéshez szükséges” alapot az adatkezelés azon részéhez, amely személyes adatoknak közvetlenül az adóhatóságoktól való gyűjtését foglalja magában. Az a tény, hogy ez a konkrét adatkezelés azzal a kockázattal jár, hogy az érintett kevésbé vesz részt adatainak kezelésében, szintén releváns tényező az adatkezelés jogszerűségének értékelése szempontjából. A bank arra a következtetésre jut, hogy az adatkezelés ezen részét más jogalapra kell helyezni. Az adatkezelő helye szerinti tagállamban hatályos nemzeti törvények értelmében a bank közvetlenül az adóhatóságtól gyűjthet információt, ha ehhez az érintett előzetesen hozzájárulását adja.

A bank ezért az online kérelmezési platformon oly módon ad tájékoztatást az adatkezelésről, hogy az érintettek könnyen megértsék, hogy az adatkezelés mely része kötelező és mely része választható. Az adatkezelési lehetőségek alapértelmezés szerint nem teszik lehetővé az adatok közvetlenül az érintettől eltérő forrásból történő lekérdezését, és a közvetlen információlekérdezés lehetőségét oly módon mutatják be, hogy az ne tartsa vissza az érintettet a tartózkodástól. A közvetlenül más adatkezelőktől történő adatgyűjtéshez adott hozzájárulás egy konkrét információkészlethez való ideiglenes hozzáférési jog.

[30] Ha az eredeti jogalap a hozzájárulás, lásd: 05/2020. sz. iránymutatás az (EU) 2016/679 rendelet szerinti hozzájárulásról. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[31] Lásd az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontját.

A megadott hozzájárulásokat elektronikusan, dokumentálható módon kezelik, és az érintettek könnyen ellenőrizhetik, hogy mihez járultak hozzá, és könnyen visszavonhatják hozzájárulásukat.

Az adatkezelő előzetesen értékelte ezeket a beépített és alapértelmezett adatvédelemmel kapcsolatos követelményeket, és e kritériumok mindegyikét belefoglalja a platformra vonatkozó ajánlattétel követelményeibe. Az adatkezelő tisztában van azzal, hogy amennyiben nem foglalja bele a beépített és alapértelmezett adatvédelemmel kapcsolatos követelményeket az ajánlattételi felhívásba, előfordulhat, hogy túl késő vagy nagyon költséges folyamat lesz az adatvédelmet később beépíteni.

3.3 Tisztességes eljárás

69. A tisztességes eljárás olyan átfogó elv, amely megköveteli, hogy a személyes adatokat ne kezeljék az érintettre nézve indokolatlanul hátrányos, jogellenesen hátrányosan megkülönböztető, váratlan vagy félrevezető módon. A tisztességes eljárás elvét megvalósító intézkedések és garanciák az érintettek jogait és szabadságait is támogatják, különösen a tájékoztatáshoz való jogot (átláthatóság), a beavatkozáshoz való jogot (hozzáférés, törlés, adathordozhatóság, helyesbítés) és az adatkezelés korlátozásához való jogot (ahhoz való jog, hogy az érintettre ne terjedjen ki az egyedi ügyekben történő automatizált döntéshozatal és az érintettek hátrányos megkülönböztetésének tilalma ezekben az eljárásokban).

70. A tisztességes eljárás fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
- Autonómia – az érintett számára a lehető legnagyobb mértékű autonómiát kell biztosítani ahhoz, hogy meghatározzák, hogyan használják fel személyes adataikat, továbbá a felhasználás és kezelés hatóköre és feltételei feletti ellenőrzés tekintetében.
- Interakció – az érintettek számára lehetővé kell tenni, hogy az adatkezelő által kezelt személyes adatokkal kapcsolatban kommunikálhassanak az adatkezelővel, és gyakorolhassák jogaikat vele szemben.
- Elvárások – az adatkezelésnek meg kell felelnie az érintettek észszerű elvárásainak.
- A hátrányos megkülönböztetés tilalma – az adatkezelő tisztességtelen módon nem alkalmazhat hátrányos megkülönböztetést az érintettekkel szemben.
- A kihasználás tilalma – az adatkezelő nem használhatja ki az érintettek nehézségeit vagy sebezhetőségeit.
- A fogyasztó választása – az adatkezelő nem „tarthatja fogva” tisztességtelen módon a felhasználóit. Amennyiben egy személyes adatok kezelésével járó szolgáltatás védett, a felhasználó a szolgáltatás foglyául eshet, ez adott esetben nem tisztességes, ha gátolja az érintetteket a 20. cikk szerinti adathordozhatósághoz való joguk gyakorlásában.
- Kiegyenlített erőviszonyok – a kiegyenlített erőviszonyok fontos célja kell hogy legyen az adatkezelő és az érintett közötti kapcsolatnak. Kerülni kell a kiegyensúlyozatlan erőviszonyokat. Ha ez nem lehetséges, azt megfelelő ellenintézkedésekkel kell elismerni és figyelembe venni.
- Kockázatáthárítás tilalma – az adatkezelők nem háríthatják át a vállalkozás kockázatait az érintettekre.
- Megtévesztés tilalma – az adatkezeléssel kapcsolatos információkat és lehetőségeket tárgyilagos és semleges módon kell bemutatni, kerülve a megtévesztő vagy manipulatív nyelvezetet vagy megfogalmazást.
- Jogok tiszteletben tartása – az adatkezelőnek tiszteletben kell tartania az érintettek alapvető jogait, és megfelelő intézkedéseket és garanciákat kell életbe léptetnie, továbbá e jogokat nem korlátozhatja, hacsak azt valamilyen törvényi rendelkezés kifejezetten nem indokolja.

- Etikusság – az adatkezelőnek látnia kell az adatkezelés által az egyének jogaira és méltóságára gyakorolt szélesebb körű hatásokat.
- Őszinteség – az adatkezelőnek tájékoztatást kell adnia a személyes adatok kezelésének módjáról, és az elmondottaknak megfelelően kell eljárnia, nem vezetheti félre az érintetteket.
- Emberi beavatkozás – az adatkezelőnek olyan *képzett* személyzettel kell rendelkeznie, amely beavatkozás útján képes felfedni azokat az torzulásokat, amelyeket a gépek okozhatnak az ahhoz való joggal kapcsolatban, hogy az érintettre ne terjedjen ki a 22. cikk szerinti, egyedi ügyekben történő automatizált döntéshozatal.[32]
- Tisztességes algoritmusok – rendszeresen értékelni kell, hogy az algoritmusok a célnak megfelelően működnek-e, a feltárt torzulások mérséklése érdekében az algoritmusokat módosítani kell, és biztosítani kell, hogy az adatkezelés tisztességes legyen. Az érintetteket tájékoztatni kell a személyes adatok olyan algoritmusok alapján történő kezelésének végrehajtásáról, amelyek rájuk vonatkozó elemzéseket vagy előrejelzéseket végeznek például a munkahelyi teljesítményükkel, gazdasági helyzetükkel, egészségi állapotukkal, személyes preferenciáikkal, megbízhatóságukkal vagy viselkedésükkel, tartózkodási helyükkel vagy mozgásukkal kapcsolatban.[33]

1. példa

Az adatkezelő olyan keresőmotort működtet, amely főként a felhasználók által generált személyes adatokat kezel. Az adatkezelőnek előnye származik abból, hogy nagy mennyiségű személyes adattal rendelkezik, és hogy e személyes adatokat célzott hirdetésekhez használhatja fel. Az adatkezelő ezért arra kívánja ösztönözni az érintetteket, hogy tegyék lehetővé személyes adataik szélesebb körű gyűjtését és felhasználását. Az érintettek hozzájárulásának kikérésekor be kell mutatni az adatkezelési lehetőségeket.

A tisztességes eljárás elvének megvalósítása során, figyelembe véve az adatkezelés jellegét, hatókörét, körülményeit és célját, az adatkezelő felismeri, hogy nem tudja oly módon bemutatni a lehetőségeket, amely arra ösztönzi az érintettet, hogy lehetővé tegye az adatkezelő számára, hogy több személyes adatot gyűjtsön annál, mint amennyit a lehetőségek egyenlő és semleges módon történő bemutatása esetén gyűjthetne. Ez azt jelenti, hogy az adatkezelő nem mutathatja be az adatkezelési lehetőségeket olyan módon, amely megnehezíti az érintettek számára az adataik megosztásától való tartózkodást, vagy megnehezíti az érintettek számára adatvédelmi beállításaik módosítását és az adatkezelés korlátozását. Ezek a 25. cikk szellemiségével ellentétes, tisztességtelen gyakorlatokra példák. Az adatkezelés alapértelmezett lehetőségei nem lehetnek invazívak, és a további adatkezelés választásának lehetőségét oly módon kell bemutatni, hogy az ne kényszerítse az érintettet a hozzájárulásra. Az adatkezelőnek ezért a hozzájárulás és a tartózkodás lehetőségét két egyformán látható opcióként kell ismertetnie, pontosan bemutatva az érintett számára mindkét lehetőség következményeit.

[32] Lásd: Iránymutatás az (EU) 2016/679 rendelet alkalmazásában egyedi ügyekben történő automatizált döntéshozatalról és profilalkotásról.
https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49826
[33] Lásd az általános adatvédelmi rendelet (71) preambulumbekezdését.

2. példa

Egy másik adatkezelő személyes adatokat kezel streamingszolgáltatás nyújtása céljából, mely szolgáltatás esetében a felhasználók választhatnak egy szokványos minőségű rendes előfizetés és egy magasabb minőségű prémium előfizetés között. A prémium előfizetés részeként az előfizetők elsőbbségi ügyfélszolgálatot kapnak.

A tisztességes eljárás elvére tekintettel a prémium előfizetőknek nyújtott elsőbbségi ügyfélszolgálat nem különböztetheti meg hátrányosan a rendes előfizetők lehetőségét arra, hogy gyakorolják az általános adatvédelmi rendelet 12. cikke szerinti jogaikat. Ez azt jelenti, hogy bár a prémium előfizetők elsőbbségi szolgáltatást kapnak, ez nem eredményezheti az arra irányuló megfelelő intézkedések hiányát, hogy a rendes előfizetők kéréseit indokolatlan késedelem nélküli, de legkésőbb a kérések kézhezvételétől számított egy hónapon belül megválaszolják.

A kiemelt ügyfelek fizethetnek a jobb szolgáltatásért, de minden érintett számára egyenlő és hátrányos megkülönböztetéstől mentes lehetőséget kell biztosítani arra, hogy az általános adatvédelmi rendelet 12. cikke szerint érvényesítsék jogaikat és szabadságaikat.

3.4 Célhoz kötöttség[34]

71. Az adatkezelő meghatározott, egyértelmű és jogszerű célból gyűjthet adatokat, és azokat nem kezelheti a gyűjtésük céljával össze nem egyeztethető módon.[35] Az adatkezelés formáját ezért annak megfelelően kell kialakítani, hogy mi szükséges a célok elérése szempontjából. Amennyiben további adatkezelésre kerül sor, az adatkezelőnek először meg kell győződnie arról, hogy ezen adatkezelés céljai összeegyeztethetők az eredeti célokkal, és ennek megfelelően kell megterveznie az ilyen adatkezelést. Azt, hogy egy új cél összeegyeztethető-e vagy sem, a 6. cikk (4) bekezdésében foglalt kritériumok alapján kell értékelni.

72. A célhoz kötöttség fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
- Előzetes meghatározás – a jogszerű célokat az adatkezelés megtervezése előtt kell meghatározni.
- Meghatározottság – a célokat meg kell határozni, azoknak egyértelművé kell tenniük, hogy miért történik a személyes adatok kezelése.
- Célorientáltság – az adatkezelés céljának kell vezérelnie az adatkezelés megtervezését és meghatároznia az adatkezelés határait.
- Szükségesség – a cél meghatározza, hogy mely személyes adatok szükségesek az adatkezeléshez.
- Összeegyeztethetőség – minden új célnak összeegyeztethetőnek kell lennie azzal az eredeti céllal, amelyből az adatokat gyűjtötték, és az adatkezelés kialakítását adott esetben ezen új célnak megfelelően kell módosítani.
- A további adatkezelés korlátozása – az adatkezelő nem kapcsolhatja össze az adatkészleteket, és nem végezhet további adatkezelést új, összeegyeztethetetlen célok érdekében.
- A további felhasználás korlátozása – az adatkezelőnek – a hash-t és titkosítást is ideértve – technikai intézkedéseket kell alkalmaznia, hogy korlátozza a személyes adatok más célra

[34] A 29. cikk szerinti munkacsoport útmutatást nyújtott a célhoz kötöttség 95/46/EK irányelv szerinti elvének értelmezéséhez. Bár a véleményt nem az Európai Adatvédelmi Testület fogadta el, az releváns lehet, mivel az általános adatvédelmi rendeletben az elv ugyanúgy van megfogalmazva. A 29. cikk szerinti munkacsoport. „03/2013. számú vélemény a célhoz kötöttségről”. WP 203, 2013. április 2. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[35] Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének b) pontja.

történő felhasználásának lehetőségét. Az adatkezelőnek szervezési intézkedéseket – például szabályzatokat és szerződéses kötelezettségeket – is életbe kell léptetnie a személyes adatok további felhasználásának korlátozására.

- Felülvizsgálat – az adatkezelőnek rendszeresen felül kell vizsgálnia, hogy az adatkezelés szükséges-e azon célokhoz, amelyekből az adatokat gyűjtötték, és meg kell vizsgálnia a kialakítást a célhoz kötöttség szempontjából.

Példa

Az adatkezelő az ügyfeleire vonatkozó személyes adatokat kezel. Az adatkezelés célja a szerződés teljesítése, vagyis hogy az árukat a megfelelő címre lehessen szállítani, és be lehessen szedni az ellenértéket. A tárolt személyes adatok a vásárlási előzmények, a név, a cím, az e-mail cím és a telefonszám.

Az adatkezelő olyan ügyfélkapcsolat-kezelés (CRM) termék megvásárlását veszi fontolóra, amely egy helyre gyűjti össze az értékesítésekkel, marketinggel és ügyfélszolgálattal kapcsolatos összes ügyféladatot. A termék lehetőséget nyújt az összes telefonhívás, tevékenység, dokumentum, e-mail és marketingkampány tárolására, hogy teljes képet lehessen alkotni az ügyfélről. A CRM alkalmas továbbá az ügyfelek vásárlóerejének nyilvános információk felhasználásával történő automatikus elemzésére. Az elemzés célja a reklámtevékenységek célba juttatásának javítása. Ezek a tevékenységek nem képezik az adatkezelés eredeti, jogszerű célját.

A célhoz kötöttség elvével való összhang megteremtése érdekében az adatkezelő megköveteli a termék szolgáltatójától, hogy térképezze fel a személyes adatokat az adatkezelő szempontjából releváns célokból felhasználó különböző adatkezelési tevékenységeket.

A feltérképezés eredményeinek beérkezését követően az adatkezelő felméri, hogy az új marketingcél és a tervezett reklámcél összeegyeztethető-e azokkal az eredeti célokkal, amelyeket az adatgyűjtés idején határoztak meg, valamint azt, hogy elegendő jogalapja van-e az adott adatkezelésnek. Ha az értékelés eredménye ezt nem erősíti meg, az adatkezelő az adott funkciókat nem használhatja. Az adatkezelő dönthet úgy is, hogy eltekint az értékeléstől, és egyszerűen nem használja a termék fent ismertetett funkcióit.

3.5 Adattakarékosság

73. Csak olyan személyes adatok kezelhetők, amelyek a cél szempontjából megfelelőek és relevánsak, valamint a **szükségesre** korlátozódnak.[36] Az adatkezelőnek ezért előre meg kell határoznia, hogy a személyes adatok kezelésére használt rendszerek és támogató funkcióik mely jellemzői és paraméterei megengedettek. Az adattakarékosság a szükségesség elvét támasztja alá és valósítja meg. A további adatkezelés során az adatkezelőnek időszakonként meg kell vizsgálnia, hogy a kezelt személyes adatok továbbra is megfelelőek, relevánsak és szükségesek-e, illetve hogy az adatokat törölni vagy anonimizálni kell-e.

74. Az adatkezelőknek mindenekelőtt meg kell határozniuk, hogy kezelniük kell-e egyáltalán személyes adatokat saját céljaikra. Az adatkezelőnek ellenőriznie kell, hogy az adott célok elérhetők-e kevesebb személyes adat kezelésével vagy kevésbé részletes, vagy összesített személyes adatok birtokában, vagy

[36] Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja.

anélkül, hogy személyes adatokat kellene kezelni[37] Az ellenőrzésre még az adatkezelés előtt sort kell keríteni, de az adatkezelés életciklusa során bármikor elvégezhető. Ez a 11. cikkel is összhangban van.

75. A takarékosság az azonosítás fokára is utalhat. Ha az adatkezelés célja nem kívánja meg, hogy a végső adathalmaz egy azonosított vagy azonosítható egyénre vonatkozzon (például a statisztikák esetében), de az eredeti adatkezelés (például az adatok összesítése előtt) megkívánja ezt, az adatkezelőnek törölnie vagy anonimizálnia kell a személyes adatokat, amint az azonosításra már nincs szükség. Vagy ha az egyéb adatkezelési tevékenységekhez folyamatos azonosításra van szükség, a személyes adatokat álnevesíteni kell az érintettek jogaira jelentett kockázatok mérséklése érdekében.

76. Az adattakarékosság fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
- Az adatok elkerülése – teljes mértékben kerülni kell a személyes adatok kezelését, ha ez az adott cél szempontjából lehetséges.
- Korlátozás – az összegyűjtött személyes adatok mennyiségének a cél szempontjából a szükségesre való korlátozása.
- Hozzáférés korlátozása – az adatkezelést oly módon kell kialakítani, hogy feladatai ellátásához csak minimális számú személynek kelljen hozzáférnie a személyes adatokhoz, a hozzáférést pedig ennek megfelelően kell korlátozni.
- Relevancia – a személyes adatoknak relevánsnak kell lenniük a szóban forgó adatkezelés szempontjából, és az adatkezelőnek képesnek kell lennie e relevancia bizonyítására.
- Szükségesség – minden személyesadat-kategóriának szükségesnek kell lennie a meghatározott célok szempontjából, és azok csak akkor kezelhetők, ha a cél más módon nem érhető el.
- Összesítés – lehetőség szerint összesített adatokat kell használni.
- Álnevesítés – a személyes adatokat álnevesíteni kell, amint már nincs szükség közvetlenül azonosítható személyes adatokra, és külön kell tárolni az azonosítási kulcsokat.
- Anonimizálás és törlés – ha a személyes adatok a cél szempontjából nem vagy már nem szükségesek, azokat anonimizálni vagy törölni kell.
- Adatáramlás – az adatáramlásnak elég hatékonynak kell lennie ahhoz, hogy ne hozzon létre a szükségesnél több másolatot.
- „A tudomány és technológia állása” – az adatkezelőnek az adatok elkerülése és az adattakarékosság érdekében korszerű és megfelelő technológiákat kell alkalmaznia.

1. példa

Egy könyvesbolt könyvek online értékesítésével kívánja növelni bevételeit. A könyvesbolt tulajdonosa egységes űrlapot kíván létrehozni a rendelési folyamathoz. Annak biztosítása érdekében, hogy a vásárlók az összes kért információt megadják, a könyvesbolt tulajdonosa az űrlap valamennyi mezőjét kötelezően kitöltendő mezőként jelöli meg (ha a vásárló nem tölti ki az összes mezőt, nem tudja leadni a megrendelést). A webáruház tulajdonosa először egy szabványos kapcsolatfelvételi űrlapot használ, amely információkat kér, többek között a vásárló születési idejéről, telefonszámáról és lakcíméről. Az űrlapnak azonban nem minden mezője feltétlenül szükséges a könyvek megvásárlásának és kézbesítésének célja szempontjából. Ebben a konkrét esetben ha az érintett azonnal kifizeti a terméket, nincs szükség az érintett születési idejére és telefonszámára a termék megvásárlásához. Ez azt jelenti, hogy ezek nem lehetnek kötelezően kitöltendő mezők a terméket megrendelő webes

[37] Az általános adatvédelmi rendelet (39) preambulumbekezdése így rendelkezik: „...Személyes adatok csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.”

űrlapon, hacsak az adatkezelő nem tudja egyértelműen bizonyítani, hogy azokra egyébként is szükség van, illetve miért szükséges kitölteni ezeket a mezőket. Emellett olyan helyzetek is előfordulnak, amelyekben a cím megadására sincs szükség. E-könyv vásárlása esetén például a vásárló közvetlenül az eszközére töltheti le a terméket.

A webáruház tulajdonosa ezért úgy dönt, hogy két internetes űrlapot készít: egyet könyvek megrendeléséhez, a vásárló címére vonatkozó mezővel, egyet pedig e-könyvek megrendeléséhez, a vásárló címére vonatkozó mező nélkül.

2. példa

Egy tömegközlekedési vállalat statisztikai adatokat kíván gyűjteni az utasok útvonalai alapján. Ez hasznos a tömegközlekedési menetrendek módosítására és a vonatok megfelelő útvonalaira vonatkozó megfelelő döntések meghozatalához. Az utasoknak minden alkalommal le kell húzniuk jegyüket egy leolvasón, amikor egy közlekedési eszközre fel- vagy arról leszállnak. Az utasok jogaival és szabadságaival kapcsolatos kockázatértékelésnek az utasok utazási útvonalainak összegyűjtése tekintetében történő elvégzését követően az adatkezelő megállapítja, hogy olyan esetekben, amikor az utas ritkán lakott területen él vagy dolgozik, az utas a jegyazonosító segítségével azonosítható az egyes útvonalak alapján. Ezért, mivel ez nem szükséges a vonatok tömegközlekedési menetrendjének és útvonalának optimalizálásához, az adatkezelő nem tárolja a jegyazonosítót. Az utazás befejeztével az adatkezelő csak az egyes utazási útvonalakat tárolja, hogy ne tudja azonosítani azokat az utazásokat, amelyek egyetlen jegyhez kapcsolódnak, hanem csak az egyes utazási útvonalakra vonatkozó információkat őrzi meg.

Azokban az esetekben, amikor még mindig fennállhat annak kockázata, hogy egy személyt kizárólag a tömegközlekedési útvonala alapján azonosítanak, az adatkezelő statisztikai intézkedéseket hajt végre a kockázat mérséklése érdekében, például levágja az útvonal kezdetét és végét.

3. példa

Egy futárszolgálat célja, hogy felmérje kézbesítéseinek hatékonyságát a szállítási idő, a munkateher ütemezése és az üzemanyag-fogyasztás szempontjából. E cél elérése érdekében a futárszolgálatnak számos, mind az alkalmazottakra (gépkocsivezetőkre), mind az ügyfelekre (címek, szállítandó tárgyak stb.) vonatkozó személyes adatot kell kezelnie. Ez az adatkezelési művelet azzal a kockázattal jár, hogy figyelemmel kísérik az alkalmazottakat, amihez különleges jogi garanciákra van szükség, és nyomon követik az ügyfelek szokásait az időről időre kézbesített tárgyakról szerzett ismeretek révén. E kockázatok jelentősen csökkenthetők az alkalmazottak és az ügyfelek megfelelő álnevesítésével. Különösen ha az álnevesítési kulcsokat gyakran váltogatják, és a részletes címek helyett makroterületeket vesznek figyelembe, hatékony adattakarékosság valósítható meg, és az adatkezelő kizárólag a kézbesítési folyamatra és az erőforrások optimalizálásának céljára összpontosíthat anélkül, hogy túllépné az egyének (ügyfelek vagy alkalmazottak) magatartásának nyomon követésére vonatkozó küszöböt.

4. példa

Egy kórház adatokat gyűjt betegeiről a kórházi információs rendszerben (elektronikus egészségügyi dokumentáció). A kórházi személyzetnek hozzá kell férnie a betegaktákhoz ahhoz, hogy megalapozott döntést hozhassanak a betegek ellátásáról és kezeléséről, és hogy dokumentálják az elvégzett diagnosztikai, ápolási és kezelési tevékenységeket. Alapértelmezés szerint csak azok az egészségügyi alkalmazottak rendelkeznek hozzáféréssel, akiket az adott beteg kezelésére megbíztak azon az osztályon, ahova a beteget beutalták. A betegaktához hozzáférő személyek köre bővül, ha a kezelésben más osztályok vagy diagnosztikai egységek is részt vesznek. A beteg kórházból történő elbocsátása és a számlázás után a hozzáférés osztályonként azon alkalmazottak kisebb körére szűkül, akik az adott beteg felhatalmazása alapján teljesítik a más egészségügyi szolgáltatótól érkező, egészségügyi információk vagy konzultáció iránti kéréseket.

3.6 Pontosság

77. A személyes adatoknak pontosnak és naprakésznek kell lenniük, és minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.[38]

78. A követelményeket az adatok konkrét felhasználásának kockázataival és következményeivel összefüggésben kell vizsgálni. A pontatlan személyes adatok kockázatot jelenthetnek az érintettek jogaira és szabadságaira nézve, például ha hibás diagnózishoz vagy egy egészségügyi protokoll helytelen kezeléséhez vezetnek, vagy ha egy személyről téves képet alkotnak, az akár manuálisan – automatizált döntéshozatal használatával –, akár mesterséges intelligencia révén hibás alapon meghozott döntésekhez vezethet.

79. A pontosság fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
    - Adatforrás – a személyes adatok forrásainak megbízhatónak kell lenniük az adatok pontossága szempontjából.
    - Pontossági fok – minden személyes adatelemnek a meghatározott célokhoz szükséges pontosságúnak kell lennie.
    - Mérhető pontosság – a hamis pozitívok és negatívok számának csökkentése, például a torzítások mérséklése az automatizált döntéshozatalban és mesterséges intelligencia esetén.
    - Ellenőrzés – az adatok azzal összefüggő jellegétől függően, hogy milyen gyakran változhatnak, az adatkezelőnek az adatkezelés előtt és annak különböző szakaszaiban ellenőriznie kell az érintettel a személyes adatok helyességét (pl. életkorral kapcsolatos követelmények).
    - Törlés/helyesbítés – az adatkezelő haladéktalanul törli vagy helyesbíti a pontatlan adatokat. Az adatkezelő különösen akkor segíti ezt elő, ha az érintettek még gyermekek vagy gyermekek voltak, később pedig el akarják távolítani a szóban forgó személyes adatokat.[39]
    - Hibaterjedés elkerülése – az adatkezelőnek mérsékelnie kell az adatkezelési láncban felhalmozódott hibák hatását.
    - Hozzáférés – a pontosság ellenőrzése és szükség esetén a helyesbítés érdekében az érintettek számára az általános adatvédelmi rendelet 12–15. cikkének megfelelően tájékoztatást kell nyújtani a személyes adatokról, és tényleges hozzáférést kell azokhoz biztosítani.
    - Folyamatos pontosság – a személyes adatoknak az adatkezelés minden szakaszában pontosnak kell lenniük, a kritikus lépéseknél el kell végezni a pontosság ellenőrzését.
    - Naprakészség – a személyes adatokat naprakésszé kell tenni, ha ez a cél szempontjából szükséges.

[38] Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének d) pontja.
[39] Vö.: (65) preambulumbekezdés.

- Adattervezés – technológiai és szervezési kialakítási funkciók alkalmazása a pontatlanság csökkentése érdekében, például tömör, előre meghatározott választási lehetőségek használata üres szövegmezők helyett.

1. példa

Egy biztosító társaság mesterséges intelligencia (MI) segítségével kívánja a biztosítási terméket vásárló ügyfelek profilját megalkotni, amelynek alapján döntést hoz a biztosítási kockázat kiszámítása során. Annak megállapítása során, hogy az MI-megoldásokat hogyan kell kifejleszteni, meghatározzák az adatkezelés módját, és figyelembe veszik a beépített adatvédelmet, amikor az eladónál kiválasztják az MI-t, és amikor döntenek arról, hogy miként képezzék ki az MI-t.

Az MI kiképzési módjának meghatározásakor az adatkezelőnek pontos adatokkal kell rendelkeznie pontos eredmények eléréséhez. Ezért az adatkezelőnek biztosítania kell, hogy az MI kiképzéséhez használt adatok pontosak legyenek.

Ha az adatkezelőnek van érvényes jogalapja arra, hogy az MI kiképzéséhez meglévő ügyfeleinek kiterjedt alcsoportjától származó személyes adatokat használjon fel, az adatkezelő a torzulások elkerülése érdekében a sokaság tekintetében reprezentatív ügyfélkört választ.

Az ügyféladatokat ezt követően összegyűjtik az adott adatkezelő rendszerből, többek között a biztosítás típusára – például egészségbiztosítás, lakásbiztosítás, utasbiztosítás stb. – vonatkozó adatokat, valamint azon nyilvánosan hozzáférhető nyilvántartásokból származó adatokat, amelyekhez jogszerűen hozzáférnek. Mielőtt az adatokat továbbítanák az MI-modell kiképzésére szolgáló rendszerbe, minden adatot álnevesítenek.

Annak biztosítása érdekében, hogy az MI kiképzéséhez felhasznált adatok a lehető legpontosabbak legyenek, az adatkezelő csak pontos és naprakész információkat tartalmazó adatforrásokból gyűjt adatokat.

A biztosítótársaság teszteli az MI megbízhatóságát, és azt, hogy megkülönböztetéstől mentes eredményeket nyújt-e mind a fejlesztés mind a termék kibocsátása előtt. Miután az MI teljes körű kiképzésére sor került és az működőképes, a biztosítótársaság az eredmények segítségével támasztja alá a biztosítási kockázatok értékelését anélkül, hogy kizárólag az MI-re támaszkodna annak eldöntésekor, hogy köt-e biztosítást, kivéve, ha a döntést az általános adatvédelmi rendelet 22. cikkének (2) bekezdésében foglalt kivételes eseteknek megfelelően hozzák.

A biztosítótársaság emellett a megbízhatóság fenntartása érdekében rendszeresen felülvizsgálja az MI-től származó eredményeket, és szükség esetén módosítja az algoritmust.

2. példa

Az adatkezelő olyan egészségügyi intézmény, amely módszereket keres az ügyfélnyilvántartásaiban szereplő személyes adatok integritásának és pontosságának biztosítására.

Azokban az esetekben, amikor két személy egyszerre érkezik az intézménybe, és e személyek azonos kezelésben részesülnek, fennáll a kockázata annak, hogy összekeverik őket, ha megkülönböztetésükre egyedül a nevük szolgál paraméterként. A pontosság biztosítása érdekében az adatkezelőnek minden egyes személyre vonatkozóan egyedi azonosítóra és ezért az ügyfél nevénél több információra van szüksége.

Az intézmény több, az ügyfelek személyes adatait tartalmazó rendszert használ, és biztosítania kell, hogy az ügyféllel kapcsolatos információk mindenkor helyesek, pontosak és következetesek legyenek az összes rendszerben. Az intézmény számos olyan kockázatot azonosított, amely akkor merülhet fel, ha az információt csak az egyik rendszerben változtatják meg.

Az adatkezelő úgy dönt, hogy a kockázatot hash technikával mérsékli, amely biztosítja a kezelési napló adatainak integritását. Megváltoztathatatlan kriptográfiai időbélyegeket hoz létre a kezelési naplók bejegyzései és az azokhoz társított ügyfél számára, hogy szükség esetén felismerhetők, összefüggésbe hozhatók és nyomon követhetők legyenek a változások.

3.7 Korlátozott tárolhatóság

80. Az adatkezelőnek biztosítania kell, hogy a személyes adatok tárolása olyan formában történjen, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.[40]
Alapvető fontosságú, hogy az adatkezelő pontosan tudja, hogy a vállalkozás milyen személyes adatokat kezel és miért. A személyes adatok tárolásának időtartamát meghatározó fő kritériumnak az adatkezelés céljának kell lennie.

81. A korlátozott tárolhatóság elvét érvényesítő intézkedések és garanciák kiegészítik az érintettek jogait és szabadságait, különösen a törléshez és a tiltakozáshoz való jogot.

82. A korlátozott tárolhatóság fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
- Törlés és anonimizálás – az adatkezelőnek a törlésre és/vagy anonimizálásra vonatkozóan egyértelmű belső eljárásokkal és funkciókkal kell rendelkeznie.
- Az anonimizálás/törlés hatékonysága – az adatkezelőnek meg kell győződnie arról, hogy nem lehet újraazonosítani az anonimizált adatokat, illetve helyreállítani a törölt adatokat, és meg kell vizsgálnia, hogy ez lehetséges-e.
- Automatizálás – egyes személyes adatok törlését automatizálni kell.
- Tárolási kritériumok – az adatkezelőnek meg kell határoznia, hogy milyen adatokat meddig szükséges tárolni a cél szempontjából.
- Indokolás – az adatkezelőnek meg kell tudnia indokolni, hogy a cél szempontjából és az adott személyes adatok esetében miért az adott ideig szükséges tárolni az adatokat, és számot kell tudnia adni az adatmegőrzés időtartamának okairól és jogalapjáról.
- A megőrzési szabályzatok érvényesítése – az adatkezelőnek érvényesítenie kell a belső megőrzési szabályzatokat, és vizsgálatokat kell végeznie annak megállapítására, hogy a szervezet alkalmazza-e a szabályzatait.
- Biztonsági másolatok/naplók – az adatkezelőnek meg kell határoznia, hogy milyen személyes adatokat meddig szükséges tárolni a biztonsági másolatokhoz és a naplókhoz.
- Adatáramlás – az adatkezelőnek tisztában kell lennie a személyes adatok áramlásával és azzal, ha azokról bármilyen másolatot tartanak, továbbá törekednie kell arra, hogy korlátozzák ezek „ideiglenes” tárolását.

Példa

[40] Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének c) pontja.

Az adatkezelő személyes adatokat gyűjt, az adatkezelés célja az érintett tagságának adminisztrációja. A személyes adatokat a tagság megszűnésekor törlik, és az adatok további tárolásának nincs jogalapja.

Az adatkezelő először belső eljárást dolgoz ki az adatok megőrzésére és törlésére vonatkozóan. Ezen eljárás szerint a munkavállalók a megőrzési időszak lejárta után manuálisan törlik a személyes adatokat. A munkavállaló követi az adatok összes eszköz, biztonsági másolat, napló, e-mail és más releváns adathordozó tekintetében történő rendszeres törlésére és helyesbítésére vonatkozó eljárást.

A törlés hatékonyabbá tétele és a hibák mérséklése érdekében az adatkezelő a későbbiekben inkább automatikus rendszert vezet be az adatok automatikus, megbízhatóbb és rendszeresebb törlésére. A rendszer úgy van kialakítva, hogy kövesse az adatok törlésére vonatkozó adott eljárást, a törlésre pedig előre meghatározott rendszeres időközönként kerül sor a személyes adatoknak a vállalat valamennyi adathordozójáról történő eltávolítása érdekében. Az adatkezelő rendszeresen felülvizsgálja és teszteli a megőrzési eljárást, és gondoskodik arról, hogy az megfeleljen a naprakésszé tett megőrzési szabályzatnak.

3.8 Integritás és bizalmas jelleg

83. Az integritás és bizalmas jelleg elve magában foglalja a jogosulatlan vagy jogszerűtlen kezeléssel, valamint a véletlen adatvesztéssel, megsemmisítéssel vagy károsodással szembeni védelmet a megfelelő technikai és szervezési intézkedések alkalmazásával. A személyes adatok biztonságának biztosításához megfelelő intézkedések szükségesek, amelyekkel megelőzhetők és kezelhetők az adatvédelmi incidensek, garantálható az adatkezelési feladatok megfelelő végrehajtása és az egyéb elveknek való megfelelés, és amelyek elősegítik az egyének jogainak hatékony gyakorlását.

84. A (78) preambulumbekezdés szerint a beépített és alapértelmezett adatvédelemmel kapcsolatos intézkedések magukban foglalhatják azt, hogy az adatkezelő *„biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat”*. A beépített és alapértelmezett adatvédelemmel kapcsolatos egyéb intézkedések mellett a (78) preambulumbekezdés azt javasolja, hogy az adatkezelők folyamatosan értékeljék, hogy mindig a megfelelő adatkezelési eszközöket használják-e, és értékeljék, hogy a választott intézkedések ténylegesen kezelik-e a meglévő sebezhetőségeket. Az adatkezelőnek ezenfelül rendszeresen felül kell vizsgálnia a személyes adatokat körülvevő és védő információbiztonsági intézkedéseket, valamint az adatvédelmi incidensek kezelésére szolgáló eljárást.

85. Az integritás és bizalmas jelleg fő beépített és alapértelmezett elemei a következőket foglalhatják magukban:
    - Információbiztonsági irányítási rendszer (ISMS) – az információbiztonsági szabályzatok és eljárások irányításának operatív eszközével kell rendelkezni.
    - Kockázatelemzés – a személyes adatok biztonságára jelentett kockázatok értékelése az egyének jogaira gyakorolt hatás figyelembevételével, és az azonosított kockázatok kezelése. A kockázatértékelés céljára átfogó, szisztematikus és realisztikus kockázati modell kidolgozása és alkalmazása, és a tervezett szoftverre vonatkozó támadásifelület-elemzés a támadási vektorok, valamint a gyenge pontok és sebezhetőségek kiaknázására adódó lehetőségek csökkentése érdekében.
    - Beépített biztonság – a biztonsági követelményeknek a rendszer tervezésekor a lehető legkorábban történő figyelembevétele, valamint releváns tesztek kidolgozása és ezek folyamatos integrációja és elvégzése.
    - Karbantartás – szoftverek, hardverek, rendszerek és szolgáltatások stb. rendszeres felülvizsgálata és tesztelése az adatkezelést támogató rendszerek sebezhetőségének feltárása érdekében.

- Hozzáférési jogosultságok kezelése – a személyes adatokhoz csak azok a feljogosított alkalmazottak férhetnek hozzá, akiknek erre adatkezelési feladataik ellátásához szükségük van, az adatkezelőnek továbbá meg kell különböztetnie a feljogosított alkalmazottak hozzáférési jogosultságait.
    - Hozzáférés korlátozása (ágens) – az adatkezelést oly módon kell kialakítani, hogy feladataik ellátásához csak minimális számú személynek kelljen hozzáférnie a személyes adatokhoz, a hozzáférést pedig ennek megfelelően kell korlátozni.
    - Hozzáférés korlátozása (tartalom) – az egyes adatkezelési műveletekkel összefüggésben a hozzáférést adatállományként azokra az attribútumokra kell korlátozni, amelyek a művelet elvégzéséhez szükségesek. Ezenfelül a hozzáférést azokra az adatokra kell korlátozni, amelyek az adott alkalmazott feladatkörébe tartozó érintettekre vonatkoznak.
    - Hozzáférések elkülönítése – az adatkezelést oly módon kell kialakítani, hogy egyetlen személynek se kelljen hozzáférnie egy érintettről gyűjtött valamennyi adathoz, legkevésbé pedig az érintettek egy konkrét kategóriájának valamennyi személyes adatához.
- Biztonságos adattovábbítás – az adattovábbítást biztosítani kell a jogosulatlan és véletlen hozzáféréssel és változtatásokkal szemben.
- Biztonságos tárolás – az adattárolásnak biztonságosnak kell lennie a jogosulatlan hozzáféréssel és változtatásokkal szemben. Eljárásokat kell érvénybe léptetni a központosított vagy decentralizált adattárolás kockázatának értékelésére és annak felmérésére, hogy ez a személyes adatok mely kategóriáira vonatkozik. Bizonyos adatok esetében további biztonsági intézkedésekre lehet szükség, illetve szükséges lehet azok más adatoktól való elkülönítése.
- Álnevesítés – a személyes adatokat és a biztonsági másolatokat/naplókat biztonsági intézkedésként álnevesíteni kell az esetleges adatvédelmi incidensek kockázatának minimalizálása érdekében, például hash vagy titkosítás alkalmazásával.
- Biztonsági másolatok/naplók – a biztonsági másolatokat és a naplókat az információbiztonsághoz szükséges mértékben kell megőrizni, rutinszerű biztonsági ellenőrzésként ellenőrzési nyomvonalakat kell használni, és nyomon kell követni az eseményeket. Ezeket védeni kell a jogosulatlan vagy véletlen hozzáféréssel és változtatásokkal szemben, rendszeres felülvizsgálatnak kell alávetni, és az incidenseket haladéktalanul kezelni kell.
- Katasztrófa utáni helyreállítás/üzletmenet-folytonosság – az információs rendszerek katasztrófa utáni helyreállításával és az üzletmenet-folytonossággal kapcsolatos követelmények kezelése annak érdekében, hogy a személyes adatok súlyosabb incidensek után ismét elérhetők legyenek.
- Kockázat szerinti védelem – a személyes adatok valamennyi kategóriáját a biztonsági incidensek kockázata szempontjából megfelelő intézkedésekkel kell védeni. Amennyiben lehetséges, a különleges kockázatot jelentő adatokat a többi személyes adattól elkülönítve kell tartani.
- A biztonsági incidensekre való reagálás irányítása – az adatvédelmi incidensek felderítésére, megfékezésére, kezelésére, bejelentésére és az azokból való tanulásra vonatkozó gyakorlatokat, eljárásokat és erőforrásokat kell alkalmazni.
- Incidenskezelés – az adatkezelőnek a szabálysértések és incidensek kezelésére folyamatokat kell alkalmaznia, hogy az adatkezelési rendszer megbízhatóbb legyen. Idetartoznak az értesítési eljárások, például (a felügyeleti hatóságnak küldött) értesítések és (az érintetteknek adott) tájékoztatás kezelése.

Példa

Az adatkezelő nagy mennyiségű személyes adatot szeretne kinyerni egy (a betegekre vonatkozó) elektronikus egészségügyi dokumentációkat tartalmazó egészségügyi adatbázisból a vállalat egy erre kijelölt adatbázisszerverére, hogy az így kinyert adatokat minőségbiztosítási célokból kezelje. A vállalat úgy értékelte, hogy valószínűleg nagy kockázatot jelent az érintettek jogaira és szabadságaira nézve, ha a kivonatokat a vállalat valamennyi alkalmazottja számára hozzáférhető szerverre irányítják. Mivel a vállalatnál egyetlen osztálynak kell a betegadatok kivonatát kezelnie, az adatkezelő úgy dönt, hogy a kijelölt szerverhez való hozzáférést az adott osztályon dolgozó alkalmazottakra korlátozza. A kockázat további csökkentése érdekében emellett a továbbítás előtt az adatokat álnevesítik.

A hozzáférés szabályozása és a rosszindulatú szoftverek által okozott esetleges károk enyhítése érdekében a vállalat úgy dönt, hogy elszigeteli a hálózatot, és hozzáférés-ellenőrzést vezet be a szerverre vonatkozóan. Emellett a vállalat biztonsági megfigyelést, valamint a behatolás észlelésére és megelőzésére szolgáló rendszert vezet be, és azt elkülöníti a szokványos felhasználástól. A hozzáférés és a változások nyomon követésére automatizált ellenőrzési rendszert hoznak létre. E rendszer bejelentéseket és automatikus riasztásokat generál a használattal kapcsolatos bizonyos események beállítása esetén. Az adatkezelő biztosítja, hogy a felhasználók kizárólag a szükséges ismeret elve alapján és megfelelő szintű hozzáféréssel rendelkezzenek. A nem megfelelő használat gyorsan és könnyen felderíthető.

Egyes kivonatokat új kivonatokkal kell összehasonlítani, ezért azokat három hónapig kell tárolni. Az adatkezelő úgy dönt, hogy ezeket ugyanazon a szerveren külön adatbázisokba helyezi, és tárolásukhoz egyidejűleg átlátható és oszlopszintű titkosítást alkalmaz. Az oszlopszintű visszafejtéshez a kulcsokat erre a célra kijelölt biztonsági modulokban tárolják, amelyeket csak az arra jogosult alkalmazottak használhatnak, kibontásukra azonban nincs módjuk.

A későbbi incidensek kezelésével a rendszer még szilárdabbá és megbízhatóbbá válik. Az adatkezelő tisztában van azzal, hogy megelőző jellegű és hatékony intézkedéseket és garanciákat kell beépíteni minden jelenlegi és jövőbeli adatkezelési tevékenységbe, és hogy ez segíthet az ilyen adatvédelmi incidensek jövőbeli megelőzésében.

Az adatkezelő meghatározza e biztonsági intézkedéseket egyrészt a pontosság, az integritás és a bizalmas jelleg biztosítása, másrészt a kibertámadások által terjesztett rosszindulatú szoftverek megelőzése és annak érdekében, hogy a megoldás megbízható legyen. A megbízható biztonsági intézkedések segítenek elnyerni az érintettek bizalmát.

3.9 Elszámoltathatóság[41]

86. Az elszámoltathatóság elve szerint az adatkezelő felelős a fent említett valamennyi elvnek való megfelelésért, és képesnek kell lennie arra, hogy igazolja a megfelelést.

87. Az adatkezelőnek képesnek kell lennie arra, hogy bizonyítsa az elveknek való megfelelést. Ennek során az adatkezelő szemléltetheti, hogy az érintettek jogainak védelme érdekében hozott intézkedések milyen hatással bírnak, és miért bizonyulnak megfelelőnek és hatékonynak az intézkedések. Szemléltetheti például azt, hogy egy intézkedés miért megfelelő a korlátozott tárolhatóság elvének hatékony érvényesítésére.

[41] Lásd a (74) preambulumbekezdést, amely megköveteli az adatkezelőktől, hogy igazolják intézkedéseik hatékonyságát.

88. A személyes adatok felelősségteljes kezeléséhez az adatkezelőnek rendelkeznie kell az adatvédelem megvalósításához szükséges ismeretekkel, és képesnek is kell lennie a megvalósításra. Ehhez szükséges, hogy az adatkezelő tisztában legyen az általános adatvédelmi rendelet szerinti adatvédelmi kötelezettségeivel és teljesíteni tudja ezeket a kötelezettségeket.

4 A 25. CIKK (3) BEKEZDÉSE (TANÚSÍTÁS)

89. A 25. cikk (3) bekezdése értelmében a 42. cikk szerinti tanúsítás felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti a beépített és alapértelmezett adatvédelmet. Ugyanakkor a beépített és alapértelmezett adatvédelem követelményének való megfelelést tanúsító dokumentumok a tanúsítási eljárás során is hasznosak lehetnek. Ez azt jelenti, hogy amennyiben az adatkezelő vagy adatfeldolgozó valamely adatkezelési művelete a 42. cikk szerint tanúsítványt kapott, a felügyeleti hatóságok figyelembe veszik azt az általános adatvédelmi rendeletnek való megfelelés értékelésekor, különös tekintettel a beépített és alapértelmezett adatvédelemre.

90. Amennyiben az adatkezelő vagy adatfeldolgozó valamely adatkezelési művelete a 42. cikk szerint tanúsítványt kapott, a 25. cikk (1) és (2) bekezdésének való megfelelés bizonyításához a tervezési folyamatokat kell figyelembe venni, azaz az adatkezelés módja meghatározásának folyamatát, az irányítás folyamatát és az adatvédelmi elvek megvalósítását szolgáló technikai és szervezési intézkedéseket. Az adatvédelmi tanúsítás szempontjait a tanúsító szervezetek vagy a tanúsítási rendszer tulajdonosa határozza meg, amelyeket ezt követően az illetékes felügyeleti hatóság vagy az Európai Adatvédelmi Testület hagy jóvá. A tanúsítási mechanizmusokra vonatkozó további információkkal kapcsolatban figyelmükbe ajánljuk az Európai Adatvédelmi Testület tanúsításról szóló iránymutatását[42] és az Európai Adatvédelmi Testület honlapján közzétett egyéb vonatkozó iránymutatásokat.

91. Az adatkezelő abban az esetben is felelős a beépített és alapértelmezett adatvédelem 25. cikkben meghatározott követelményei teljesülésének folyamatos ellenőrzéséért és javításáért, ha az adatkezelési művelet a 42. cikk szerint tanúsítványt kapott.

5 A 25. CIKK ÉRVÉNYESÍTÉSE ÉS A KÖVETKEZMÉNYEK

92. A felügyeleti hatóságok az 58. cikkben felsorolt eljárásoknak megfelelően értékelhetik a 25. cikknek való megfelelést. A korrekciós hatásköröket az 58. cikk (2) bekezdése határozza meg, és azok magukban foglalják a figyelmeztetéseket, az elmarasztalásokat, az érintettek jogainak teljesítésére vonatkozó utasításokat, az adatkezelés korlátozását vagy megtiltását, a közigazgatási bírságokat stb.

93. A beépített és alapértelmezett adatvédelem emellett az általános adatvédelmi rendelet megsértése esetén alkalmazandó pénzügyi szankciók szintje meghatározásának is egyik tényezője (lásd a 83. cikk (4) bekezdését).[43] [44]

[42] Európai Adatvédelmi Testület. „1/2018. számú iránymutatás a rendelet 42. és 43 cikkével összhangban történő tanúsításról és a tanúsítási szempontok meghatározásáról". 3.0. változat, 2019. június 4. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_hu.pdf

[43] Az általános adatvédelmi rendelet 83. cikke (2) bekezdésének d) pontja értelmében az általános adatvédelmi rendelet megsértése miatti közigazgatási bírságok kiszabásának eldöntésekor *„kellőképpen figyelembe kell venni […] az adatkezelő vagy az adatfeldolgozó felelősségének mérték[ét] , figyelembe véve az általa a 25. és 32. cikk alapján foganatosított technikai és szervezési intézkedéseket".*

[44] A bírságokkal kapcsolatos további információkért lásd: a 29. cikk szerinti munkacsoport. „Iránymutatás a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról". WP 253, 2017. október 3.

6 AJÁNLÁSOK

94. Bár a 25. cikk erre nem tér ki kifejezetten, az adatfeldolgozók és a szolgáltatók szintén a beépített és alapértelmezett adatvédelem legfontosabb előmozdítóinak tekinthetők, és tisztában kell lenniük azzal, hogy az adatkezelők csak olyan rendszerekkel és technológiákkal kezelhetnek személyes adatokat, amelyek rendelkeznek beépített adatvédelemmel.

95. Az adatkezelők nevében végzett adatkezelés vagy az adatkezelőknek, adatfeldolgozóknak és a szolgáltatóknak nyújtott megoldások körében a technológiaszolgáltatóknak ki kell használniuk szakértelmüket, hogy bizalmat építsenek ki, és iránymutatást nyújtsanak ügyfeleiknek, többek között a kkv-knak az adatvédelem adatkezelésbe való beépítésére szolgáló megoldások kidolgozása és beszerzése során. Ez azt is jelenti, hogy a termékeket és szolgáltatásokat úgy kell kialakítani, hogy azok elősegítsék az adatkezelők igényeinek teljesítését.

96. A 25. cikk végrehajtásakor szem előtt kell tartani, hogy a tervezés fő célja az elvek *hatékony érvényesítése* és az érintettek jogainak *védelme* az adatkezelés megfelelő intézkedései során. A beépített és alapértelmezett adatvédelem elősegítése és javítása érdekében az alábbi ajánlásokat fogalmazzuk meg az adatkezelők, valamint az szolgáltatók és adatfeldolgozók számára:

- Az adatkezelőknek már az adatkezelési művelet tervezésének *kezdeti szakaszaitól* kezdve, még az adatkezelés módjának meghatározása előtt gondolniuk kell az adatvédelemre.
- Ha az adatkezelő alkalmaz adatvédelmi tisztviselőt, az Európai Adatvédelmi Testület szerint az adatvédelmi tisztviselőnek érdemes aktív szerepet vállalnia a beépített és alapértelmezett adatvédelem beszerzési és fejlesztési folyamataiban, valamint az adatkezelés teljes életciklusába történő beépítésében.
- Az adatkezelési művelet *tanúsítható*. Az, ha egy adatkezelési művelet tanúsítást kap, hozzáadott értéket jelent az adatkezelő számára, amikor választani kell a szolgáltatók vagy adatfeldolgozók különböző adatkezelő szoftverei, hardverei, szolgáltatásai és/vagy rendszerei közül. A szolgáltatóknak ezért törekedniük kell annak bizonyítására, hogy egy adatkezelési megoldás fejlesztésének teljes életciklusában figyelemmel vannak a beépített és alapértelmezett adatvédelemre. A tanúsítást igazoló pecsét is segítséget nyújthat az érintettek számára a különböző termékek és szolgáltatások közötti választás során. Az, hogy egy adatkezelési művelet tanúsítást kap, versenyelőnyt jelenthet a szolgáltatók, az adatfeldolgozók és az adatkezelők számára, és akár az érintettek személyes adataik kezelésébe vetett bizalmát is növelheti. Tanúsítás hiányában az adatkezelőknek egyéb *garanciákat* kell szerezniük arra vonatkozóan, hogy a szolgáltatók vagy adatfeldolgozók megfelelnek a beépített és alapértelmezett adatvédelem követelményeinek.
- Az adatkezelőknek, adatfeldolgozóknak és a szolgáltatóknak szem előtt kell tartaniuk, hogy a 18 év alatti gyermekek és más kiszolgáltatott csoportok esetében külön védelmet kell biztosítaniuk a beépített és alapértelmezett adatvédelemnek való megfelelés érdekében.
- A szolgáltatóknak és adatfeldolgozóknak törekedniük kell arra, hogy elősegítsék a beépített és alapértelmezett adatvédelem megvalósítását annak érdekében, hogy támogassák az adatkezelőt a 25. cikk szerinti kötelezettségeinek teljesítésében. Az adatkezelők ugyanakkor nem választhatnak olyan szolgáltatókat vagy adatfeldolgozókat, amelyek nem kínálnak olyan rendszereket, amelyek lehetővé teszik vagy elősegítik az adatkezelő számára a 25. cikknek való

http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49781 – az Európai Adatvédelmi Testület által jóváhagyva

megfelelést, mivel az adatkezelők felelősségre vonhatók a cikk végrehajtásának elmulasztása miatt.

- A szolgáltatóknak és adatfeldolgozóknak aktív szerepet kell játszaniuk annak biztosításában, hogy „a tudomány és technológia állására" vonatkozó kritériumok teljesüljenek, és értesíteniük kell az adatkezelőket „a tudomány és technológia állásának" minden olyan változásáról, amely befolyásolhatja a meglévő intézkedéseik hatékonyságát. Az adatkezelőknek szerződéses kikötésként kell szerepeltetniük e követelményt annak biztosítása érdekében, hogy naprakészek legyenek.
- Az Európai Adatvédelmi Testület azt javasolja az adatkezelőknek, hogy követeljék meg a szolgáltatóktól és adatfeldolgozóktól annak szemléltetését, hogy hardvereik, szoftvereik, szolgáltatásaik és rendszereik hogyan teszik lehetővé az adatkezelő számára az elszámoltathatóság követelményeinek a beépített és alapértelmezett adatvédelemnek megfelelően való megfelelést, például fő teljesítménymutatók alkalmazásával, amelyekkel igazolható az intézkedések és garanciák hatékonysága az elvek és jogok érvényesülésében.
- Az Európai Adatvédelmi Testület hangsúlyozza, hogy az elvek és jogok hatékony érvényesüléséhez összehangolt megközelítésre van szükség, és arra ösztönzi a 40. cikkel összhangban magatartási kódexeket kidolgozó egyesületeket vagy szervezeteket, hogy a beépített és alapértelmezett adatvédelemre vonatkozóan ágazatspecifikus iránymutatásokat is foglaljanak azokba.
- Az adatkezelőknek tisztességesnek kell lenniük az érintettekkel szemben, és átláthatónak kell lenniük azzal kapcsolatban, hogy milyen módon értékelik és bizonyítják a beépített és alapértelmezett adatvédelem hatékony megvalósítását, ugyanúgy, ahogyan az adatkezelők az elszámoltathatóság elve alapján igazolják az általános adatvédelmi rendeletnek való megfelelést.
- A magánélet védelmét erősítő, már kiforrott, modern technológiák is alkalmazhatók a beépített és alapértelmezett adatvédelem követelményeinek való megfelelést szolgáló intézkedésként, ha a kockázatalapú megközelítés szerint megfelelőnek bizonyulnak. E technológiák önmagukban nem feltétlenül garantálják a 25. cikk szerinti követelmények teljesülését. Az adatkezelőnek fel kell mérnie, hogy az intézkedés megfelelő és hatékony-e az adatvédelmi elvek és az érintettek jogainak érvényesülése szempontjából.
- A már meglévő korábbi rendszerekre a beépített és alapértelmezett adatvédelem ugyanazon követelményei vonatkoznak, mint az új rendszerekre. Ha egy korábbi rendszer még nem felel meg a beépített és alapértelmezett adatvédelem követelményének, és nem hajthatók végre a kötelezettségek teljesítését lehetővé tevő változtatások, a korábbi rendszer egész egyszerűen nem felel meg az általános adatvédelmi rendelet szerinti követelményeknek, és így nem használható személyes adatok kezelésére.
- A 25. cikk nem állapít meg enyhébb követelményeket a kkv-k számára. Az alábbi pontok segíthetnek a kkv-knak a 25. cikknek való megfelelésben:
    - Végezzen korai kockázatértékelést!
    - Kisléptékű adatkezeléssel kezdjen – a későbbiekben bővítse annak hatókörét és tegye összetettebbé!
    - Keresse a szolgáltatók és adatfeldolgozók beépített és alapértelmezett adatvédelemre vonatkozó garanciáit, úgymint tanúsítás és magatartási kódex alkalmazása!
    - Igazolt referenciákkal rendelkező partnerekkel működjön együtt!
    - Konzultáljon az adatvédelmi hatósággal!

- Olvassa el az adatvédelmi hatóság és az Európai Adatvédelmi Testület iránymutatásait!
- Kövesse a magatartási kódexeket, ha rendelkezésre állnak!
- Kérje szakértő segítségét és tanácsát!

Az Európai Adatvédelmi Testület nevében

az elnök

(Andrea Jelinek)