Az új általános európai adatvédelmi szabályozás és az adatkezelői kötelezettségek

Árvay Viktor – Balogh Gyöngyi – Buzás Péter –
Eszteri Dániel – Hackspacher Andrea –
Kiss Ernő – Majsa Ágnes – Révész Balázs

A kiadvány a KÖFOP-2.1.1-VEKOP-15-2016-00001 „A közszolgáltatás komplex kompetencia, életpálya-program és oktatás technológiai fejlesztése” című projekt keretében készült el és jelent meg.

Szerzők:

Dr. Árvay Viktor
Dr. Balogh Gyöngyi
Dr. Buzás Péter
Dr. Eszteri Dániel
Dr. Hackspacher Andrea
Dr. Kiss Ernő
Dr. Majsa Ágnes
Dr. Révész Balázs

Szakmai lektor:

Dr. Péterfalvi Attila

Olvasószerkesztő:

Császár-Biró Anna

A kézirat lezárásának dátuma:

2018. szeptember 17.

Kiadja:

© NKE, 2018

Felelős kiadó:

Prof. Dr. Kis Norbert
Dékán

TARTALOM

1. BEVEZETÉS

Az Európai Parlament és a Tanács 2016. április 27. napján négyéves előkészületet követően fogadta el az új adatvédelmi csomagot:

Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR).

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

A GDPR teljes egészében kötelező és közvetlenül alkalmazandó, nem igényel tagállami átültetést, 2016. május 24. napjától hatályos, azonban 2018. május 25. napjától alkalmazandó.

Nem tartoznak a GDPR hatálya alá:

- az olyan iratok, illetve iratok csoportjai, amelyek nem rendszerezettek;
- az uniós jog hatályán kívül eső tevékenységek (például nemzetbiztonság);
- a természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett adatkezelések; személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás, valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek;
- az elhunyt személyekkel kapcsolatos személyes adatok sem; ugyanakkor a tagállamok számára lehetővé kell tenni, hogy az elhunyt személyek személyes adatainak kezelését szabályozzák.

2. ALAPFOGALMAK

A GDPR az adatvédelemmel kapcsolatos alapfogalmak terén kevés újdonságot tartalmaz. Amit érdemes e tekintetben kiemelni az az, hogy a rendelet szerinti meghatározások megszövegezése egyszerűsödött korábbi, adatvédelmi irányelvben található fogalmakhoz képest. Példaként a személyes adat és az adatfeldolgozó említhető. Emellett pedig az adatvédelmi szabályozásban is egységes meghatározást kaptak például a biometrikus és a genetikai adatok, amelyek bevezetése nagy előrelépést jelent az ezen információkkal végzett adatkezelések vonatkozásában.

2.1. A személyes adat

A személyes adat az adatvédelem központi eleme. E fogalom ismerete elengedhetetlen az adatkezelés jogszerűségének vizsgálatához. Egyrészt a vonatkozó adatvédelmi követelmények meghatározása, érvényesülésének ellenőrzése kizárólag a kezelt személyes adatok, ezen adatok körének felmérése, behatárolása révén lehetséges. Másrészt a személyes adatok kezelésének ténye az adatkezeléssel kapcsolatos – adatkezelői és adatfeldolgozói – felelősség szempontjából is alapvető fontosságú.

A GDPR értelmében személyes adatnak minősül az azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.[1] Ebből következően a következő fogalmai elemeket kell megvizsgálni: azonosított vagy azonosítható természetes személy („érintett”), az adat és az érintett közötti kapcsolat („vonatkozó”), illetve az adat formai és tartalmi kritériumai („bármely információ”). Emellett – a GDPR-ral és az Infotv.-vel összhangban – ki kell emelni néhány speciális adatkategóriát is.

2.1.1. Az érintett

A személyes adatok védelméhez fűződő jog alanyát érintettnek vagy adatalanynak nevezzük. Érintett bármely olyan meghatározott természetes személy lehet, aki személyes adata alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható. Az adatalany vonatkozásában mindenekelőtt a természetes személy mivolt, illetve az azonosíthatóság kérdésköre érdemel figyelmet.

A személyes adatok védelméhez fűződő jog a személyhez fűződő jogok csoportjába tartozik, személyes adatról ezért kizárólag már megszületett, élő emberek vonatkozásában beszélhetünk. Sem a jogi személyeket vagy más szervezeteket, sem a méhmagzatokat, sem pedig – főszabály szerint – az elhunytakat nem illeti meg a személyes adatok védelméhez fűződő jog. Ez nemcsak magából a szabályozásból, hanem e jog személyhez fűződő jellegéből is fakad.[2] Az egyes tagállamok ugyanakkor jogosultak arra, hogy kiterjesszék az adatvédelmi előírások hatályát az elhunyt személyekre vonatkozó

---

1 GDPR 4. cikk 1. pont.

2 L. a Polgári Törvénykönyvről szóló 2013. évi V. törvény 2:43. § e) pontját.

adatok kezelésének némely vonatkozásaira is, amennyiben ezt jogszerű érdek igazolja.[3] Hazánkban például az elhunyt halálának okára és elhalálozásának körülményeivel, az elhunyt személyes adatait tartalmazó levéltári adatok megismerhetőségével, valamint az elhunyt adatait tartalmazó biztosítási titkokkal kapcsolatban találhatók jogszabályi rendelkezések.[4] Az említett eseteken túlmenően azonban – például az elhunytak név- és lakcímadatainak aláírásgyűjtés céljából történő kezelésére vonatkozóan – nem található jogszabályi rendelkezés, az ilyen információk tehát nem tartoznak az adatvédelem körébe.

Egy információ személyes adat mivoltának vizsgálata során figyelmet kell szentelni továbbá az „azonosított" és „azonosítható" kifejezéseknek is. Az egyént akkor tekintjük általánosságban azonosítottnak, ha a természetes személyek adott csoportján belül elkülönül a csoport többi tagjától. Az azonosíthatóság pedig az azonosítás megtételének lehetőségét jelenti. Az azonosíthatóság ezért egy küszöbfeltétel, amely meghatározza, hogy az információ személyes adatnak minősül-e.

Az azonosítást jellemzően – közvetlen vagy közvetett módon – valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező teszi lehetővé.[5] E tekintetben ugyanakkor *„minden olyan módszert figyelembe kell venni, amit az adatkezelő, vagy más személy valószínűleg felhasználna az említett személy azonosítására"*.[6] Tekintettel kell továbbá lenni az azonosítás költségeire, időigényességére, az adatkezeléskor rendelkezésre álló technológiákra, valamint technológia fejlődésére is.

Közvetlenül azonosítható a természetes személy például, ha az adatkezelő ügyfélkód alapján azonosítani tudja az ügyfelet. Közvetetten pedig akkor lesz azonosítható az egyén, ha bizonyos információk összegsége alapján meghatározható a kiléte. Az érintett azonosíthatóságát ugyanis nemcsak egyedi, csak az adott személyhez köthető információk tehetik lehetővé. Bizonyos adatok egyedi kombinációja révén az adatkezelő képes közvetve azonosítani az érintett személyt: egy adott információ *„más információkkal összekapcsolva (ez utóbbi akár megvan az adatkezelőnél, akár nincs) az egyént másoktól megkülönböztethetővé teszi"*.[7] Ebben a vonatkozásban az információ személyes adat jellege nem függ az azt megismerő szubjektív adattartalmától, így irreleváns az, hogy az adatkezelő megfelelő egyéb ismeretek birtokában saját maga képes-e az érintett azonosítására.

Hangsúlyozni kell, hogy éles különbség van az érintett azonosítása vagy azonosíthatósága, valamint személyazonosság megállapítása között. Előbbi esetben a kezelt adatok pusztán az érintett szeparálását teszik lehetővé a környezetétől vagy az ott lévő harmadik személyek csoportjától. Az azonosítás vagy azonosíthatóság tehát arra a kérdésre ad választ, hogy a kezelt információk mely személyhez tartoznak a csoporton belül. Ezzel szemben a személyazonosság annak megállapítását teszi lehetővé, hogy pontosan ki is az adott egyén. Az adatkezelő jellemzően jogszabályokban meghatározott különféle azonosítók – például a természetes személyazonosító adatok – segítségével felismeri az érintettet, identifikálja.[8]

Az érintett azonosítása vagy azonosíthatósága, illetve a személyazonosság megállapítása közötti különbség abból a szempontból releváns, hogy a magyar jogi gondolkodásban és a hétköznapi gyakorlatban is az a helytelen szemléletmód gyökeresedett meg, hogy csak abban az esetben beszélhetünk személyes adatokról, amennyiben azáltal az érintett abszolút módon – minimálisan névvel, esetleg még egy vagy több további információ révén – azonosított. Ez azonban rendkívüli módon

---

3 GDPR (27) preambulumbekezdés.

4 L. az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 3. § a) pontját, a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvényt, valamint a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 143. § (3) bekezdését.

5 GDPR 4. cikk 1. pont.

6 GDPR (26) preambulumbekezdés.

7 Article 29 Data Protection Working Party, 2007, 13.

8 L. a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 4. § (4) bekezdését.

leszűkítené a személyes adat fogalmát, ezáltal pedig az egyén magánéletének háborítatlanságát biztosító adatvédelmi garanciák alkalmazásának körét.

2.1.2. Vonatkozó

A személyes adat fogalmának konstitutív eleme továbbá az információ és az érintett közötti reláció. Az információknak ugyanis megszemélyesítettnek kell lennie, azaz az adatalanyhoz kell kapcsolódnia. A fogalommeghatározásban szereplő „vonatkozó" kitétel e kapcsolódási pont meglétét feltételezi.

Általánosan fogalmazva az információt az érintettre „vonatkozónak" tekinthetjük, ha az adott egyénről szól.[9] E tekintetben három – vagylagos – elem meglétét lehet vizsgálat alá vetni. A „tartalom" elemről ott lehet beszélni, ahol az adott információt egy adott személyről adják meg, azaz a személyes adat ez esetben tehát az adott személyről szól. A „cél" elem dominál, amennyiben – az eset összes körülménye alapján – megállapítható, hogy a személyes adatot abból a célból használják fel, hogy *„az egyén státuszát vagy viselkedését értékeljék, bizonyos bánásmódban részesítsék vagy befolyásolják"*.[10] A „eredmény" elemet pedig akkor kell vizsgálni, ha az információ kezelése valószínűleg hatással van egy adott személy jogaira és érdekeire.

Az információ mindaddig megőrzi személyes adat minőségét, amíg kapcsolata az érintettel helyreállítható. A helyreállíthatóság kritériuma akkor teljesül, amennyiben az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyekkel az információ és az adatalany közötti kapcsolat helyreállítható.[11] *„Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható"12*

Álnevesítés esetén azonban helyreállítható a kapcsolat az érintett és az adat között. A pszeudonimizálás azt az esetet jelenti, amikor *„további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik"*.[13] Az azonosításhoz szükséges további információk az adatkezelő birtokában vannak, azokat külön tárolja, és technikai és szervezési intézkedések megtételével biztosítja, hogy a személyes adatot nem lehessen természetes személyekhez kapcsolni.

2.1.3. Bármely információ

A személyes adat fogalommeghatározásában szereplő „bármely információ" kifejezés az adatok széles körét fedi le. Általánosságban minden olyan információt személyes adatnak tekintünk, amely kötődik az egyénhez, és helyzetét valamilyen módon befolyásolja, vagy befolyásolhatja. Az információ tehát, mivel kihat az egyén helyzetére, befolyásolja azt, személyes adatnak minősül. A személyes adatok vonatkozásában ugyanakkor megkülönböztethető két általános csoport: az érintettre vonatkozó adatok, valamint az adatokból az érintett vonatkozásában levont következtetések köre.[14]

Az adatalanyra vonatkozó adat körébe tartozik különösen az érintett neve, azonosító jele, egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző

9 Article 29 Data Protection Working Party, 2007.
10 Article 29 Data Protection Working Party, 2007, 10.
11 Vö. Infotv. 4. § (3) bekezdés.
12 GDPR (26) preambulumbekezdés.
13 GDPR 4. cikk 5. pont.
14 Vö. Infotv. korábban hatályos 3. § 2. pontjával.

ismeret, illetőleg a képmása, hangja és az adatalany azonosítására alkalmas fizikai jellemzők. A személyes adatok köre folyamatosan bővül, változik, függ a technológia fejlődésétől, de a társadalmi berendezkedéstől és annak fejlettségétől is. Ma már személyes adatnak minősülnek az érintettek által használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítók (például IP-címek és cookie-azonosítók), valamint az egyéb azonosítók is (például rádiófrekvenciás azonosító címkék).[15]

Másrészt az adatból levonható, az érintettre vonatkozó következtetés is személyes adat. Az ilyen, jellemzően logikai művelettel előállított ismereteket azért vonja a szabályozás a védelem körébe, mert számos adatkezelésnek éppen az a célja, hogy a felvett információkból az érintettre vonatkozó következtetéseket vonjon le, amelyek az adatalannyal kapcsolatos döntések alapját képezik. Példaként említhető a hitelkérelmek elbírálása, vagy egy munkahelyi alkalmassági vizsgálat elvégzése.

Általában véve a személyes adatok az információk széles körét felölelik, legyen szó akár az egyén magán- és családi életét érintő, akár munkahelyi, gazdasági vagy társasági tevékenységét érintő adatokról. Az információ természete szempontjából a személyes adatok az érintettre vonatkozó állítások valamennyi fajtáját felölelik, így lehetnek mind szubjektívek, mind pedig objektívek. Nem fogalmi elem ugyanakkor az igazságtartalom.[16] Az információ megjelenésének formája is irreleváns: alfabetikus, numerikus, grafikus, képi vagy akusztikus információk is lehetnek személyes adatok.

2.1.4. Speciális személyes adatok

A személyes adatok általános fogalommeghatározásán túl meg kell határozni bizonyos speciális adatköröket is. A GDPR-ban nevesített ilyen adatoknak minősülnek a személyes adatok különleges kategóriái, valamint a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok. A szabályozásban elfoglalt speciális helyüket az indokolja, hogy ezen információk hagyományosan kiemelt védelemben részesülnek. A nem a GDPR-ban nevesített adatok közül pedig a közérdekből nyilvános adatokat kell kiemelni. Esetükben egy másik alapjog, az információszabadság érvényesülése indokolja különleges előírások alkalmazását.

2.1.4.1. A személyes adatok különleges kategóriái

A személyes adatok egy jól körülhatárolható, tartalmánál fogva érzékenyebb köre az úgynevezett különleges vagy szenzitív adat. Az ilyen információk az érintett életének érzékenyebb aspektusaira vonatkoznak, ezért bizalmas jellegéhez kiemelt érdeke fűződik az adatalanyoknak, a vonatkozó szabályozás pedig kiemelt védelemben részesíti.

A személyes adatok különleges kategóriái közé tartoznak:

- faji vagy etnikai származásra vonatkozó adatok,
- politikai véleményre vonatkozó adatok,
- vallási vagy világnézeti meggyőződésre vonatkozó adatok,
- szakszervezeti tagságra vonatkozó adatok,
- a természetes személyek egyedi azonosítását célzó genetikai adatok,
- a természetes személyek egyedi azonosítását célzó biometrikus adatok,
- az egészségügyi adatok,
- a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Az érintett szempontjából hagyományosan szenzitív adatnak minősülnek az egészségügyi ada-

[15] GDPR (30) preambulumbekezdés.

[16] Article 29 Data Protection Working Party, 2007.

tok. Ezen információk az egyén múltbeli, jelenlegi vagy jövőbeli testi és pszichikai egészségi állapotára vonatkozó személyes adatok. Ide tartoznak például a természetes személyre vonatkozó olyan személyes adatok, amelyeket *„egészségügyi szolgáltatások céljából történő nyilvántartásba vétel, vagy ilyen szolgáltatások nyújtása során gyűjtöttek, a természetes személy egészségügyi célokból történő egyéni azonosítása érdekében hozzá rendelt szám, jel vagy adat, valamely testrész vagy a testet alkotó anyag – beleértve a genetikai adatokat és a biológiai mintákat is – teszteléséből vagy vizsgálatából származó információk, és bármilyen, például az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, klinikai kezelésével vagy fiziológiai vagy orvosbiológiai állapotával kapcsolatos információ, függetlenül annak forrásától, amely lehet például orvos vagy egyéb egészségügyi dolgozó, kórház, orvostechnikai eszköz vagy in vitro diagnosztikai teszt”*.[17]

A különleges adatok körében kiemelendő az általános adatvédelmi szabályozás szempontjából újdonságnak számító genetikai adatok meghatározása. Ezek az információk az egyén örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adatot felölelnek, amelyek *„az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered”*.[18] Az említett adatok kiemelt helyzetének oka, hogy a modern technológiák révén átfogó ismeretekkel rendelkezünk az emberi génállományról, a génekről és szerepükről. A genetika meghatározóvá vált az orvosbiológia terén. *„Alapvető jelentőségűvé váltak a genetikai tesztek és szűrővizsgálatok a diagnosztikában, lehetőség nyílik a génterápiára, igényes kutatások folynak betegségek kórokának, kialakulási lépéseinek feltárására, új és az eddigieknél hatékonyabb kezelési lehetőségek kimunkálására, egyedi gyógyszeres kezelés alkalmazására új genetikai ismeretek segítségével”*.[19] Másrészt viszont lehetőség nyílt teljes populációk génállományának feltérképezésére, amely viszont akár káros következményekhez is vezethetnek, amennyiben az adatok kezelésével visszaélnek. Elég csak az egyes népcsoportokhoz tartozó személyek diszkriminációjára gondolni, amelyet az eugenika a 19-20. század fordulója óta képvisel. Emellett külföldi példák igazolják az említett információk alkalmazhatóságát például a munkavállalók alkalmazása vagy a biztosítások terén is, amely szintén az esélyegyenlőség csökkentéséhez vezethet.

A genetikai adatokhoz hasonlóan a biometrikus adatok is fokozottabb védelemben részesülnek. Ebbe a körbe tartozik az egyén *„testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat”*.[20] Kiemelendő továbbá, hogy a modern biometrikus technológiák általában nem a nyers formában lévő biometrikus adatokat, hanem az azokból generált, a biometrikus adatok kulcsfontosságú jellemzőiből alkotott biometrikus sablonok révén működnek.[21] A védelem szempontjából azonban irreleváns, hogy egy rendszer biometrikus adatok vagy biometrikus sablont kezel. Mindkét esetben felmerül ugyanis a magánszféra bizonyos szintű érintettsége: a biometrikus adat, illetve az abból képzett bármely számsor minden esetben az érintettől elválaszthatatlan információ, ennek megfelelően az érintett fizikai jelenlétére és személyes adatának szolgáltatására mindig szükség van az adott rendszer működéséhez.

2.1.4.2. A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok

A hazai szabályozás korábban a különleges adatok körébe sorolta az úgynevezett bűnügyi személyes adatokat. E fogalom felölelte *„a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel*

[17] GDPR (35) preambulumbekezdés.

[18] GDPR 4. cikk 13. pont.

[19] L. a humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvény indokolását.

[20] GDPR 4. cikk 14. pont.

[21] Article 29 Data Protection Working Party, 2012.

vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó" személyes adatokat.[22] A GDPR fogalomrendszerében ugyanakkor az említett információk már nem szerepelnek a szenzitív adatok között. A rendelet ugyanakkor a *„büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó"* személyes adatok kezelése vonatkozásában további garanciákat tartalmaz.[23]

2.1.4.3. A közérdekből nyilvános személyes adatok

A közérdekből nyilvános adatok speciális csoportját alkotják a közérdekből nyilvános személyes adatok. Ebbe a körbe sorolandók azok a személyes adatok, amelyek *„nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli"*.[24] Az információk nyilvánosságának jellemző oka az, hogy a közhatalmat gyakorlók vagy a politikai közszereplést vállalók esetében az információszabadság elsőbbséget élvez az olyan személyes adatainak védelméhez képest, amelyek köztevékenységük és annak megítélése szempontjából jelentősek lehetnek. Az e körbe eső személyes adatok megismerhetőségére nem csupán az állami és a politikai közélet informált megvitatása érdekében van szükség, hanem az állami szervek helyes megítéléséhez és a működésükbe vetett bizalom megalapozásához is.[25]

Kiemelendő ebben a körben, hogy számos jogviszonyt meghatározó törvény is több, a közfeladat ellátása szempontjából releváns személyes adatot nyilvánossá minősít. Példaként említhető, hogy a kormánytisztviselő neve, állampolgársága, az őt alkalmazó államigazgatási szerv neve, az érintett kormányzati szolgálati jogviszonyának kezdete, a kormánytisztviselő besorolása, a munkakörének megnevezése és a betöltés időtartama, a vezetői kinevezés és annak megszűnésének időpontja, a címadományozás adatai, valamint a kormánytisztviselő illetménye nyilvános adat.[26] A köztulajdonban álló gazdasági társaságok esetében pedig széles körben nyilvánosak a vezető tisztségviselők, felügyelőbizottsági tagok, vezető állású munkavállalók, valamint az önállóan cégjegyzésre vagy a bankszámla feletti rendelkezésre jogosult munkavállalók személyes adatai (név, tisztség, munkakör, munkaviszony alapján folyósított pénzbeli juttatások).[27]

2.1.4.4. Az osztott személyes adatok

A gyakorlat ismeri és elismeri az úgynevezett osztott személyes adatok intézményét. Ebbe a körbe mindazon információk tartoznak, amelyek nem vagy nem kizárólag csak egy természetes személyre vonatkoznak, illetve – adott esetben – több személy azonosíthatását teszik lehetővé. *„Ugyanazon információ vonatkozhat ugyanis több természetes személyre is, és azok tekintetében, feltéve hogy azonosított vagy azonosítható személyekről van szó, […] személyes adatnak minősül."*[28]

Tipikus példái az osztott személyes adatoknak a természetes személyazonosító adatok között nevesített anya születési családi és utóneve.[29] A név ugyanis már önmagában is azonosít egy természetes személyt, ebben az esetben az érintett anyját, egyúttal – a törvényi előírás erejénél fogva – az

22 L. az Infotv. korábban hatályos 3. § 4. pontját.
23 GDPR 10. cikk.
24 Infotv. 3. § 6. pont.
25 L. 60/1994. (XII. 24.) AB határozat.
26 L. például a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény 179. §-át.
27 A köztulajdonban álló gazdasági társaságok takarékosabb működéséről szóló 2009. évi CXXII. törvény (Kgtv.) 2. § (1) bekezdés.
28 2017. július 20-i Nowak ítélet, C434/16, EU:C:2017:582, 45. pont.
29 A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény 4. § (4) bekezdés d) pont.

adatalanyra vonatkozó, általánosságban használt információ is lesz egyben. Az egészségügyi, illetve a genetikai adatok is tartalmazhatnak információkat az egyes öröklődő betegségekkel kapcsolatban, ezáltal az információk a vérrokonokra vonatkozó adatoknak is minősülnek.[30] Az egyénekre jellemző génállomány azonban személyhez fűződő adatok halmaza, ráadásul olyan módon, hogy a személyes adatok is tartalmaznak információkat.

A vélemények is tipikus osztott személyes adatok. A vizsgáztatónak a vizsgázó válaszaihoz írott esetleges megjegyzései egyrészt előbbire vonatkozó információnak tekinthetők. Másrészt pedig, tartalmuknál, céljuknál és hatásuknál fogva vizsgázóhoz is kapcsolódnak, hiszen az ő vizsga során nyújtott egyéni teljesítményére, ismereteire és tudására vonatkozó véleményt vagy értékelést tükröznek.[31]

2.2. Adatkezelés

A GDPR értelmében adatkezelésnek minősül *„a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége”*.[32] E körben vizsgálandó tehát az adatkezelés tárgya és módja, illetőleg a megvalósított adatkezelési műveletek fajtái.

2.2.1. Az adatkezelés tárgya és módja

Az adatkezelés fogalma szempontjából mind a személyes adatok mennyisége, mind pedig azok rendelkezésre állásának módja irreleváns. Mindaddig ugyanis, amíg az adatkezelési műveleteket személyes adatokon végzik, lényegtelen, hogy egy vagy több személyes adat érintett, vagy, hogy azok milyen – gyűjteményes vagy más – formában állnak rendelkezésre. Az adatkezelés módja sem meghatározó tényező: akár automatizált (például digitális) eszközökkel végzik, akár papír alapon kezelik a személyes adatokat, a vonatkozó előírásokat ugyanúgy be kell tartani. Kizárólag csak speciális esetekben, például az érintetti jogok gyakorlása vonatkozásban találhatók eltérések a tekintetben, hogy automatizált vagy manuális adatkezelést végeznek.[33]

2.2.2. Adatkezelési műveletek

Adatkezelésnek tekintjük a személyes adatokon végzett bármely műveletet vagy e műveletek összességét. A nevesített adatkezelési műveletek közé tartozik különösen *„a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés”*.[34] Ebben a vonatkozásban kiemelendő, hogy a szabályozás csak exemplifikatív módon sorol fel bizonyos konkrét adatkezelési műveleteket. Ennek az az oka, hogy a szabályozás minden lehetséges műveletet a hatálya alá kíván vonni, amelyet azonban

30 L. humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvény indokolását.

31 2017. július 20-i Nowak ítélet, C434/16, EU:C:2017:582, 44. pont.

32 GDPR 4. cikk 2. pont.

33 L. például a GDPR 20. cikkében foglalt adathordozhatósághoz való jogot.

34 GDPR 4. cikk 2. pont.

egy tételes felsorolás kiüresíthetne, ráadásul a technológiai fejlődés által lehetővé tett újabb és újabb adatkezelési műveletek esetén sem érvényesülnének az adatvédelmi garanciák.

A nevesített adatkezelési műveletek közül kiemelendő:

- adattovábbítás: a személyes adat meghatározott harmadik személy számára történő hozzáférhetővé tétele,
- nyilvánosságra hozatal: a személyes adat bárki számára történő hozzáférhetővé tétele,
- korlátozás: *„a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából”*,[35]
- törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges,
- megsemmisítés: a személyes adatot tartalmazó adathordozó teljes fizikai megsemmisítése,[36]
- profilalkotás: *„személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják”*.[37]

Az adatkezelési műveletek összességére mint adatkezelésre példa, a keresőmotorok tevékenysége, amelyek automatikus, állandó és rendszerezett módon kutatják a világhálót, amelynek során személyes adatokat gyűjtenek.[38] Ezt követően az érintettre vonatkozó információkat különféle indexáló programok keretei között visszakeresik, rögzítik és rendszerezik, szervereiken tárolják, és a keresés találati listájaként megjelenítik, és a felhasználók számára hozzáférhetővé teszik. E tevékenységek, azon túl, hogy önmagukban is adatkezelési műveleteket valósítanak meg, adatkezelésnek minősülnek.

2.3. Adatkezelő

A GDPR csupán általánosságban határozza meg az adatkezelő fogalmát. Eszerint az a természetes személy, jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv lehet adatkezelő, aki vagy amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.[39] A tág definíció célja az, hogy a felelősséget oda helyezze, ahol a tényleges befolyás található, és így e minőség inkább ténybeli, mint formális elemzésen alapul. Azt tehát, hogy konkrét esetben ki minősül adatkezelőnek, csak az adott eset körülményeinek alapos mérlegelésével lehet eldönteni.

2.3.1. Az adatkezelő személye

Az adatkezelői minőség szempontjából nem lényeges, hogy az adatkezelésért a felelősséget egyetlen személy, a személyek egy csoportja, vagy valamely szervezet viseli. Bárki, akire nézve adott esetben teljesül fogalommeghatározásban foglalt valamely feltétel, vagyis meghatározza az adatkezelés célját vagy eszközeit, adatkezelőnek minősül. Kivételek ugyanakkor azok az esetek, amikor jogszabály határozza meg ezeket a tényezőket. Példaként említhető az, ha a közigazgatási szervek jogszabályi

35 GDPR 4. cikk 3. pont.
36 L. az Infotv. korábban hatályos 3. § 13. ponját.
37 GDPR 4. cikk 4. pont.
38 2014. május 13-i Google Spain ítélet, C131/12, EU:C:2014:317, 28. pont.
39 GDPR 4. cikk 7. pont.

kötelezettségek teljesítése vagy közhatalmi jogosítvány gyakorlása érdekében kezelnek személyes adatokat. Esetükben az adatkezelés célját és eszközeit meghatározó jogszabály tartalmazhatja az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat.[40]

2.3.2. Többes adatkezelés

A modern világban egyre több olyan esettel találkozni, amelyben egyazon adatkezelés szempontjából különböző szereplők töltenek be adatkezelői szerepet. Egyetlen adatkezelés művelet vagy a műveletek csoportja vonatkozásában több, akár számos fél is közösen határozhatja meg az adatkezelés célját és eszközeit. Ilyen esetekben minden egyes szereplő adatkezelőnek minősül, és amelyek esetében érvényesülnie kell az adatvédelmi előírásoknak.[41]

Az egyes felek közreműködése az adatkezelés céljainak és eszközeinek meghatározásában különböző formákat ölthet, nem kell azonban az, hogy részvétel egyenlő arányban történjen. Az egyes adatkezelők lehetnek egymással nagyon szoros viszonyban, ha például az adatkezelés minden célja és eszköze közös. Ugyanakkor állhatnak lazább kapcsolatban is egymással, amennyiben csak a célok vagy az eszközök, illetve csak azok egy része közös.[42]

Többes adatkezelés esetén kulcsfontosságú az egyes adatkezelők feladatainak és felelősségi körének meghatározása. Ennek hiánya ugyanis könnyen a felelősség kezelhetetlen elosztásához vezethetne. A többes adatkezelés bizonyos körülmények között vezethet egyetemleges felelősséghez, de nem szükségszerűen, így az adatkezelés adott szakaszához mérten eltérő is lehet az egyes adatkezelők felelőssége. *„A lényeg annak a biztosítása kell, hogy legyen, hogy […] egyértelműen megállapítsák az adatvédelmi szabályok betartásáért és az e szabályok esetleges megszegéséért való felelősséget.”*[43]

2.3.3. Az adatkezelés céljának és eszközeinek meghatározása

„Az adatkezelő minőség elsősorban annak a ténybeli körülménynek a következménye, hogy egy jogalany úgy döntött, hogy a saját céljaira személyes adatokat dolgoz fel.”44 Az adatkezelői szerep megállapítása szempontjából nagyobb hangsúlyt kell helyezni a célok meghatározásával kapcsolatos mérlegelési jogkörre és a döntéshozatal körére. Az adatkezelés céljának meghatározása az adatvédelem szabályozásának középpontjában áll: szükséges előfeltétele annak, hogy megállapítható legyen az adatkezelés jogszerűsége, illetőleg az alkalmazandó adatvédelmi garanciák.[45] Ebből következően az adatkezelési céljának meghatározása minden esetben adatkezelői minőséget eredményez.

Az adatkezelés eszközei kifejezés nemcsak a személyes adatok feldolgozásának technikai módozataira utal, hanem a feldolgozás miként jére is. Ennek meghatározásába olyan technikai és szervezeti kérdések is beletartoznak, amelyek esetén a döntést át lehet ruházni az adatfeldolgozókra, és olyan alapvető elemek is, amelyekről hagyományosan és természetüknél fogva az adatkezelő határoz.[46] Az adatkezelés módjának meghatározása ezért – szemben a céllal – csak akkor utal adatkezelésre, ha a mód alapvető elemeit határozzák meg.

40 GDPR 4. cikk 7. pont.
41 Article 29 Data Protection Working Party, 2012.
42 Article 29 Data Protection Working Party, 2012.
43 Article 29 Data Protection Working Party, 2012, 22.
44 Article 29 Data Protection Working Party, 2012, 8.
45 Article 29 Data Protection Working Party, 2013.
46 Article 29 Data Protection Working Party, 2012

2.4. Adatfeldolgozó

Adatfeldolgozó „*az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel"*. E fogalommeghatározásból következően az adatfeldolgozó léte az adatkezelő döntésétől függ. Utóbbi határozhat úgy, hogy az adatkezelési tevékenységek egészét vagy egy részét egy külső szervezetre ruházza át, vagyis az adatkezelést egy „jogilag különálló, a nevében eljáró személy" útján végzi.[47] Az adatfeldolgozás ezért tulajdonképpen az adatkezeléshez tartozó egyes műveletek kiszervezése, harmadik személlyel történő elvégeztetése.

Az adatfeldolgozói minőség alapvető feltétele az, hogy az adatfeldolgozó az adatkezelőtől különálló jogalany legyen. Irreleváns viszont, hogy az adatkezelő nevében egyetlen személy, a személyek egy csoportja, vagy valamely szervezet jár el. Egyes jogszabályok azonban kijelölhetnek adatfeldolgozót vagy azok körét, amelyek egy konkrét adatkezelés tekintetében eljárhatnak.

Az adatfeldolgozó tevékenysége korlátozódhat egy pontosan meghatározott feladatra, de lehet általánosabb és kiterjedtebb is. Az nem korlátozódik a személyes adatokon végzett technikai műveletekre, például tárhelyszolgáltatásra vagy szállítási tevékenységekre, hanem kiterjed az említett információkkal végzett bármely tevékenységre. Emellett az adatfeldolgozó rendelkezhet bizonyos – minimális – befolyással az adatkezelés elemeit illetően. Az adatkezelés eszközeinek alapvető elemein kívül eső technikai és szervezeti paraméterek megválasztása tekintetében ugyanis bizonyos mérlegelési és döntéshozatali joga van.[48]

2.5. Ellenőrző kérdések

Mi a személyes adat fogalma?
Melyek a személyes adat fogalmának legfontosabb fogalmi elvei?
Melyek a személyes adatok különleges kategóriái?
Mi az adatkezelés fogalma?
Mi az adatkezelő fogalma?

[47] Article 29 Data Protection Working Party, 2012, 25.
[48] Article 29 Data Protection Working Party, 2012.

3. ALAPELVEK

A személyes adatok védelméhez fűződő jog jogi szabályozásában nagy szerepük van az alapelveknek, az alapelvi szemléletmódnak. Az adatvédelem kialakulásának folyamata és a szabályozás egységesülése az alapelvek kialakulásával is járt. Már 1980-ban az OECD-irányelvek[49] tartalmaztak adatvédelmi alapelveket, ajánlásként a tagállamok számára, mégpedig az alábbiakat:

- korlátozott adatgyűjtés alapelve,
- adatminőség alapelve,
- cél meghatározásának alapelve,
- felhasználás korlátozásának alapelve,
- biztonság alapelve,
- nyíltság alapelve,
- személyes részvétel alapelve
- elszámoltathatóság alapelve.

Ezen OECD-irányelvhez hasonló tartalommal került elfogadásra 1981-ben az Európa Tanács Adatvédelmi Egyezménye.[50] Tehát az adatkezelés elvei már korán megjelentek az adatvédelmi jogban. Az adatvédelmi irányelv is – irányelv minőségénél fogva is – tartalmazta az adatkezelési alapelveket.

Hazai vonatkozásban elmondható, hogy az adatvédelmi szabályok kialakulásában iránymutató volt a 15/1991. (IV. 13.) AB-határozat, mely meghatározta az információs önrendelkezési jog lényegét, és az adatkezelés főbb elveit is. Mind az Avtv., mind az Infotv. alapelvi rendelkezéseket is szabályozott, melyek tartalommal való megtöltése, értelmezése a jogalkalmazás feladata.

Az adatvédelmi reform során a korábbi alapelvek is felülvizsgálatra kerültek. Az uniós jogalkotó láthatóan azok többségének megtartása mellett döntött. Tehát elmondható, hogy az irányelv és az Infotv. szabályozásához képest a GDPR az alapelvek tekintetében nagy újítást nem hozott, nagy változást nem okozott. Az alapelvi rendelkezések egyes részletei, megfogalmazásuk változott, egyes részletei pontosabbá, hangsúlyosabbá váltak. Viszont látszódik a szabályozásból a jogalkotó azon szándéka, hogy az alapelveknek nagy hangsúlyt adjon, azok érvényesülését kikényszerítse: ezt egyrészt az elszámoltathatóság elve, másrészt a szankcionálás biztosítja. A rendelet központi jelentőségű rendelkezéseinek, így az adatkezelés alapelveinek megsértése esetére a súlyosabb, nagyobb összegű bírság (legfeljebb 20 millió EUR) szabható ki.

A Rendelet a (26) preambulumbekezdésében rögzíti, hogy *„az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell”,* továbbá *„az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni.”* Vagyis a GDPR hatálya ennek megfelelően értelmezendő az alapelvek tekintetében is.

A GDPR a hatály tisztázása és a fogalommagyarázat után rögtön a II. fejezetben, az 5. cikkben sorolja fel az adatvédelmi jog azon főbb alapelveit, melyek mintegy megkerülhetetlen szempontrendszerként egyfajta keretet szabnak az adatok kezelésének, iránymutatásul szolgálnak egy-egy adatkezelés megítélésénél. Alapelvet illetve alapelv jellegű rendelkezést a rendelet más részeiben is

---

[49] Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) irányelvei a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról.

[50] Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során.

találhatunk – például beépített és alapértelmezett adatvédelem (25. cikk), adattovábbításra vonatkozó általános elv (44. cikk), azonban ezen elvek az adott témakörnél tárgyalandóak.

A GDPR az alábbi főbb alapelveket nevesíti:

- Jogszerűség, tisztességes eljárás, átláthatóság,
- Célhoz kötöttség,
- Adattakarékosság,
- Pontosság,
- Korlátozott tárolhatóság,
- Elszámoltathatóság.

3.1. A jogszerűség, tisztességes eljárás és átláthatóság elve

Az alapelvek között az első helyen fogalmazódik meg a GDPR-ban ez a jogelv, mely három, különállóan is értelmezhető elvet foglal magában, és mindegyik eleme olyan alapvető követelmény, mely áthatja az adatvédelmi szabályozást: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.[51]

A jogszerűség értelme a fogalomból eredően nyilvánvaló: jogellenes célból, jogellenes módon személyes adatok nem gyűjthetőek, azokkal semmiféle művelet nem végezhető. Ez a követelmény lényegében azt jelenti, hogy a kötelezően alkalmazandó jogi szabályozás minden előírása teljesítendő az adatkezelő által, mert enélkül az adatkezelés nem tekinthető jogszerűnek. A korábbi hazai szabályozás a törvényességet jelölte meg mint alapvető kritériumot – e vonatkozásban a jogszerűségnek még kiterjesztőbb értelmezése van, nem csak törvényi szintű, hanem mindenfajta jogi előírás betartását és betartatását feltételezi.

Megjegyzendő, hogy a hazai eljárásjogi szabályozásban, az Ákr-ben is megjelenik alapelvi szinten a jogszerűség elve,[52] de itt ez eljárási, és nem anyagi jogi alapelvként értelmezendő.

A tisztességesség elve részben párhuzamba vonható a polgári jognak a rendeltetésszerű joggyakorlásra, jóhiszeműségre és tisztességre vonatkozó elvével.

Sok esetben az adatkezelés látszólag jogszerű, van célja és jogalapja is, az adatkezelő formálisan betartja az adatkezelésre vonatkozó szabályokat, az adatok felvétele, kezelése mégis kifogásolható. A jogalkotó a tisztességes adatkezelés elvével egyfajta morális, erkölcsi színezetet ad a látszólag csak technikai jelleg adatkezelési folyamatoknak. Az adatkezelés egészének tisztességessége is az adatkezelés jogszerűségének feltételei közé sorolódott, és ez az emberi méltóság védelmével hozható összefüggésbe.

Példa: Tisztességtelen az adatkezelés olyan online adatkezelések esetén, amikor a weboldal kompromittáló fotókat tesz közzé lejárató jelleggel (például volt barátnők intim fényképei).

Példa: A tisztességtelen adatkezelés körébe sorolandóak a rejtett kamerás megfigyelések is.

Példa: A követeléskezeléssel foglalkozó cégek adatkezelésével kapcsolatban a Hatóság több alkalommal kimondta, hogy tisztességtelennek tartja, ha a követeléskezelő a követelésben nem érintett, az adós környezetében élő más személyektől gyűjt személyes adatokat az adósáról, mert a saját adatairól mindenki csak maga rendelkezhet. Az ilyen adatgyűjtés különösen sérti a személyiségi jogot, mert kiszolgáltatottá teszi az adatalanyokat, egyenlőtlen helyzetet eredményez, amelyben az adatalany nem tudja, hogy az adatkezelő mit tud róla. Az így gyűjtött adatok minősége, valóságtartalma is megkérdőjelezhető az adatforrásnak az adatalanyhoz fűződő viszonyától függően. Az adatgyűjtés az adatalany személyének megítélését a mikrokörnyezetében, az érintett által ápolt vagy nem ápolt ismeretségi, illetve rokoni körében hátrányosan befolyásolhatja.

[51] GDPR 5. cikk (1) bekezdés a/ pont.

[52] Ákr. 2. §.

Az átláthatóság, vagy transzparencia elve még nagyobb hangsúlyt kapott a GDPR-ban a korábbi szabályozáshoz képest. Az átláthatóság az érintett szempontjából vizsgálandó: azt a követelményt testesíti meg, hogy az adatalany követni tudja az adatai sorsát, hogy információja legyen az adatkezelés folyamatáról. Az átlátható adatkezelés biztosítása érdekében a GDPR szabályozza, hogy az adatkezelőknek proaktív módon megfelelő tájékoztatást kell adniuk az érintettek számára még az adatkezelés megkezdése előtt, az adatalanyok pedig a tájékoztatáshoz és a hozzáféréshez való joguk által érvényesíttethetik ezt az elvet. Ezen témák részletes kifejtése másik fejezetben található.

Ezen alapelv értelmezéséhez a (39) preambulumbekezdés nyújt segítséget. Ebben a jogalkotó kiemeli, hogy az átláthatóság tekintetében a tájékoztatásnak világosnak, egyszerű nyelvezetűnek, közérthetőnek kell lennie, és könnyen hozzáférhető kell legyen. Kiemeli az adatkezelő személyéről és az adatkezelés céljáról való tájékoztatás fontosságát.

A GDPR (60) preambuluma alapján a tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól.

3.2. A célhoz kötöttség elve

A 15/1991. (IV. 13.) AB-határozat az információs önrendelkezési jog legfontosabb garanciájaként nevezte meg a célhoz kötöttség követelményét. A határozat szerint személyes adatot kezelni/feldolgozni csak pontosan meghatározott és jogszerű célra lehet, és minden szakaszban meg kell felelni ennek a célnak. Az adatkezelés/adatfeldolgozás célját – és annak megváltozását is – közölni kell az érintettel, hogy megalapozottan dönthessen az adatok kiadásáról, megítélhesse az adatkezelés/feldolgozás hatását a jogaira. A célhoz kötött adatkezelés elvéből az következik, hogy a meghatározott cél nélküli, előre nem meghatározott jövőbeni felhasználásra, vagyis készletre való adatgyűjtés és -tárolás alkotmányellenes.

Az Avtv. és az Infotv. – az adatvédelmi irányelvet átültető törvényként – is következetesen tartalmazta a célhoz kötöttség elvét. A 29-es adatvédelmi munkacsoport a 3/2013. számú véleményében részletesen elemezte ezt az elvet. A GDPR szabályozása is egyik fő vezérelvének tekinti a célhoz kötöttséget, melynek lényegi tartalma változatlan a korábbi szabályozáshoz képest. Ezen elvből következően minden adatkezelésnek jogszerű célja kell legyen, a célt előre meg kell határozni. Nem elegendő az, ha egy adatkezelésnek megfelelő jogalapja van, ezzel együtt a célhoz kötöttségnek is érvényesülnie kell. Vagyis például önmagában az érintett hozzájárulása esetén még nem jogszerű az adatkezelés, mert elfogadható adatkezelési célnak is fenn kell állnia a célhoz szükséges adatok kezelése vonatkozásában. Adatkezelési cél megjelölése nélküli érintetti hozzájárulás az adatvédelmi jogi szabályozás szempontjából nem lehetséges.

Fontos, hogy a cél jogszerű legyen, jog gyakorlását vagy kötelezettség teljesítését szolgálja. Az adatkezelésnek a folyamat minden szakaszában, illetve minden adatkezelési műveletet tekintve meg kell felelnie az adatkezelési célnak, tehát például az adat felvételekor, nyilvántartásakor, felhasználásakor, továbbításakor is.

A célhoz kötöttség követelménye szoros összefüggésben van az adatminimalizálás elvével, ugyanis csak az adatkezelési cél megvalósulásához szükséges, e cél elérésére alkalmas személyes adatok kezelhetőek. Vagyis mindig az adott célhoz kell viszonyítani az adott adatot, és eldönteni, ténylegesen szükséges-e a cél eléréséhez, és valóban alkalmas-e erre.

Ha egy adatgyűjtésnek nincs célja, vagy nincs konkrétan meghatározott célja, vagy jövőbeni, illetve bizonytalan célra irányul, akkor készletező adatgyűjtésről beszélünk.

A célhoz kötöttség elvének nem felel meg, ha az adatkezelés céljának megjelölése túl általános, semmitmondó, és ezáltal nem alkalmas arra, hogy az adatalany meg tudja ítélni az adatai felhasználását. Ez átvezet az adatkezelő kötelezettségeihez és az előzetes tájékoztatás követelményéhez, ugyanis az adatkezelési célról is megfelelő tájékoztatást kell adni.

A már nyilvánosságra hozott személyes adatok további közzététele, felhasználása esetén sem hagyható figyelmen kívül a célhoz kötöttség követelménye, az ilyen továbbfelhasználás akkor jogszerű, ha az eredeti céllal összhangban van. Megemlítendő, hogy ezzel ellentétben az információszabadság jogának érvényesülése érdekében kifejezetten jogellenes a közérdekű adatigénylések során célmegjelölést kérni és az adatigénylés célját vizsgálni.

Ha az adatkezelés célja megváltozik, akkor e célnak megfelelően kell megítélni a jogalap kérdését, a szükségesség elvét és az egyéb garanciák érvényesülését. Ha az adatkezelési cél megszűnik, akkor törlési kötelezettség áll fenn.

A GDPR 5. cikk (1) bekezdésének b/ pontja tartalmazza a célhoz kötöttség követelményét. Eszerint személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és az adatok csak e célokkal összeegyeztethető módon legyenek kezelve. A rendelet kifejezetten nevesít olyan adatkezelési célokat, melyeket összeegyeztethetőnek tekint az eredeti adatkezelési céllal, ezek: közérdekű archiválás, tudományos és történelmi kutatás, statisztikai cél. Ez esetben is csak megfelelő garanciák mellett végezhető az adatkezelés, továbbá az uniós vagy tagállami jog eltéréseket állapíthat meg e tekintetben.[53]

A Rendelet (39) preambulumbekezdése hangsúlyozza, hogy az adatkezelés céljáról megfelelő tájékoztatást kell adni, és az adatkezelés konkrét céljainak explicit módon megfogalmazottaknak és jogszerűeknek, továbbá már az adatgyűjtés időpontjában meghatározottaknak kell lenniük.

Példa: Egy weboldalhoz kapcsolódó adatkezelés vizsgálata során a NAIH megállapította, hogy az adatkezelő célja nem a honlapon megjelölt játékszolgáltatás nyújtása, hanem a valós cél személyes adatok gyűjtése, adatbázis építése és értékesítése érdekében, és ezért a cég valótlan adatkezelési célt jelölt meg és elhallgatta a tényleges célt. Az adatkezelő bírósághoz fordult, kifogásolva, hogy az üzleti érdekével ellentétes az, hogy fel kell tárnia az értékesítési tevékenységét e vonatkozásban. A bíróság az adatvédelmi hatóság jogértelmezését erősítette meg ítéletében.

3.3. Az adattakarékosság elve

Csak olyan személyes adat kezelhető, mely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Ezt jelenti az adattakarékosság elve, másképpen fogalmazva az adatminimalizálás elve vagy szükségesség elve.

Eszerint az adatkezelőnek vizsgálnia kell még az adatkezelés tényleges megkezdése előtt, hogy szükségesek-e, illetve mely adatok szükségesek az adott célhoz, és egyáltalán szükség van-e személyes adatok kezelésére az adott tevékenység végzéséhez.

A szükségesség elvére számos jogszabály utal, és sok szektorális, ágazati szabályozás meghatározza a kezelendő adatok körét.

A GDPR adattakarékosság elveként nevesíti ezt az alapelvet, mely szerint személyes adatok megfelelőek és relevánsak kell legyenek az adatkezelés céljához képest, továbbá a szükségesre kell korlátozódniuk.[54]

Az adattakarékosság elve szorosan összefügg a célhoz kötöttség elvével, mivel a szükséges adatkör meghatározása során mindig az adatkezelés céljához kell viszonyítani. De különbséget is kell tenni a két elv között: a célhoz kötöttség az adatkezelési cél konkrét meghatározásának igényét jelenti, az adattakarékosság elve pedig az adott cél eléréséhez ténylegesen szükséges adatok kezelését engedi.

[53] GDPR 89. cikk.

[54] GDPr 5. cikk (1) c/ pont.

A szükségesség elvének korábbi szabályozása kismértékben változott amiatt, hogy a GDPR szerint az adatkezelési célhoz képest megfelelő és releváns adatok kezelése tekinthető jogszerűnek. A szükséges, megfelelő, releváns adatok körének meghatározása sok esetben nem is olyan egyszerű kérdés, és esetről esetre mérlegelendő. Ennek eldöntéséhez az adatkezelési cél pontos, konkrét megnevezése nélkülözhetetlen, mert ehhez viszonyítottan vonható meg az adatkezelés által érintett adatok határa.

Az uniós jogalkotó a beépített adatvédelem és az alapértelmezett adatvédelem elvének meghatározásakor további szempontokat adott a szükségesség elvének érvényesüléséhez.[55] A beépített adatvédelem elve szerint az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell végrehajtania az adatvédelmi elvek és követelmények érvényesülése érdekében, például az adattakarékosság hatékony megvalósítása érdekében. Az alapértelmezett adatvédelem elve pedig azt mondja, hogy az adatkezelőnek az intézkedéseivel biztosítania kell, hogy kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. A szükségesség e szempontja kell érvényesüljön az adatok mennyisége, kezelésük mértéke, tárolási időtartama és hozzáférhetősége tekintetében is.

A GDPR (39) preambulumbekezdése előírja, hogy az adatok körét a célhoz szükséges minimumra szükséges korlátozni, és ezért a tárolásuk a lehető legrövidebb ideig történjen. Ennek érdekében az adatkezelőnek törlési vagy rendszeres felülvizsgálati határidőket kell megállapítania.

3.4. A pontosság elve

A pontosság elve szerint[56] a személyes adatoknak pontosnak és szükség esetén naprakésznek is kell lenniük. A pontatlan személyes adatokat – haladéktalanul – törölni vagy helyesbíteni kell, de legalábbis észszerű intézkedéseket kell tenni ennek érdekében.

A pontos adatrögzítésre is kiemelten figyelni kell, különösen az adatfelvételnél, mert az elírás, a hibás adatok további problémákat okozhatnak az adatkezelési folyamat során. A személyek azonosítása és azonosíthatósága is csak pontos adatok rendelkezésre állása esetén lehetséges. Egyes adatelírási, egyéb adminisztratív problémák adatvédelmi incidens bekövetkezéséhez is vezethetnek.

A naprakészség követelménye az adatok frissességére, karbantartására, az adatmódosulások átvezetésére utal. Ez nem abszolút követelmény, hanem szükség szerint kell gondoskodni erről, és esetről esetre mérlegelendő. Az adatok naprakészsége azért lehet fontos elv bizonyos esetekben, hogy elavult adatokon ne alapuljon döntés, a már nem aktuális adatok ne legyenek felhasználva. Emellett nyilván üzleti érdek is lehet az adatbázis aktualizálása, frissítése.

Példa: Követeléskezeléssel foglalkozó cégek esetében gyakran volt tapasztalható, hogy adatbázisaikban az adósok korábbi, már megváltozott telefonszámait, lakcímeit is továbbra is nyilvántartják annak ellenére, hogy azokon az érintett már nem érhető el, és annak ellenére, hogy új, aktuális elérhetőségi adatokkal is rendelkeznek. A lakcímadat kezelésének célja a követeléskezelési tevékenység során az adóssal való kapcsolattartás. A kapcsolattartási cél eléréséhez elegendő az adott személy aktuális állandó lakcím adatának kezelése. Az elavult, nem naprakész állandó lakcím és levelezési cím adatok nem alkalmasak e cél elérésére.

A teljesség követelménye – az Infotv.-nyel ellentétben – a GDPR-ban már nem szerepel.

[55] GDPR cikk.

[56] GDPR 5 cikk (1) bekezdés d/ pont.

3.5. A korlátozott tárolhatóság elve

Ezen elv szerint az érintettek azonosítása csak az adatkezelés céljainak eléréséhez szükséges ideig lehetséges, az adattárolás formája ennek megfelelő kell legyen.[57] Kivétel ezen alapelv érvényesülése alól a 89. cikk szerinti közérdekű archiválás, tudományos és történelmi kutatás vagy statisztikai cél.

3.6. Az integritás és bizalmas jelleg elve

Eszerint személyes adatok kezelésénél megfelelő technikai és szervezési intézkedésekkel biztosítani kell az adatok biztonságát, kifejezetten ideértve az adatok jogellenes vagy jogosulatlan kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet.[58]

3.7. Az elszámoltathatóság elve

Az elszámoltathatóság elve egyfajta *szuperelv*, általános elvárás az adatkezelőkkel szemben lényegében az összes adatvédelmi alapelv, garancia érvényesülése érdekében. Az elszámoltathatóság elve által az uniós jogalkotó az adatkezelők felelősségét deklarálta valamennyi adatkezelési alapelvre vonatkoztatva. Vagyis az adatkezelő viseli a felelősséget az alapelveknek való megfelelésért, és ráadásul úgy, hogy képesnek kell lennie e megfelelés igazolására.[59]

A rendelet egyik fontos újítása, hogy alapelvi szintre emelte az elszámoltathatóság koncepcióját. Az adatkezelőknek 2018 májusától sokkal nagyobb tudatosság mellett kell az adatkezeléseiket végezni. Valamennyi adatkezelési műveletet úgy kell megvalósítaniuk, hogy mindig bizonyítani tudják, miként felelnek meg az előírásoknak. Az elszámoltathatóság elve lényegében azt jelenti, hogy az adatkezelőknek mind a szervezeti kultúrájukat, mind tevékenységeiket az adatvédelmi megfontolásokra tekintettel kell kialakítaniuk. Tehát az adatvédelmi alapelvek, a „szuperelv", vagyis az elszámoltathatóság elve segítségével kikényszeríthetőek, és túllépnek a papírra vetett általánosságokon, melyeket senki nem vesz komolyan, vagy amelyek túl elvontaknak tűnnek a hétköznapi valóság szempontjából.

Az alapelvek érvényesülését a jogalkotó azáltal is elősegíti, hogy az érintetteknek különféle jogosítványokat biztosít, és e jogérvényesítésen keresztül teljesülnek az alapelvi kritériumok. Például egyes érintetti jogok a pontosság elvének érvényesülését, más jogok az átláthatóság elvének, vagy éppen az adattakarékosság elvének érvényesülését szolgálják (lásd érintetti jogokról szóló fejezet).

A GDPR megengedi az alapelvekkel kapcsolatban bizonyos mértékig az eltérést. Ahogyan a (73) preambulumbekezdés ezt magyarázza, az uniós és a tagállami jog olyan mértékig korlátozhat bizonyos elveket, amilyen mértékig ez egy demokratikus társadalomban szükségesnek és arányosnak tekinthető a közbiztonság védelme érdekében, továbbá valamely egyéb uniós vagy tagállami közérdek jelentős céljai érdekében. E korlátozásoknak tiszteletben kell tartaniuk a Charta, valamint az emberi jogok és alapvető szabadságok védelméről szóló európai egyezmény rendelkezéseit.

[57] GDPR 5. cikk (1) bekezdés e/ pont.
[58] GDPR 5. cikk (1) bekezdés f/ pont.
[59] GDPR 5. cikk (2) bekezdés.

3.8. Ellenőrző kérdések

Melyek a GDPR-ban nevesített alapelvek?
Mutassa be a célhoz kötöttség elvét!
Mutassa be az adattakarékosság elvét!
Mutassa be a tisztességes adatkezelés alapelvét!
Mutassa be az elszámoltathatóság elvét!

4. JOGALAPOK

4.1. Bevezető

Alapvető adatvédelmi alapelv az európai és a magyar adatvédelmi jogban, hogy ahhoz, hogy az adatkezelő személyes adatokat kezeljen, rendelkeznie kell megfelelő jogalappal.

Az adatkezelés jogalapja azon absztrakt módon megfogalmazott eseteknek a köre, amikor a jogalkotó jogszerűnek tekinti meghatározott személyes adatok kezelését. A jogalap megléte azonban nem elegendő ahhoz, hogy az adatkezelés egészét jogszerűnek tekinthessük, hiszen az adatkezelésnek meg kell felelnie további jogszabályi feltételeknek. Jelen fejezetben azokat az eseteket tekintjük át, amelyeket az európai jogalkotó alkalmazhatónak ítélt személyes adatok kezelésére.

4.2. Általános jellemzés

A jogalapok listáját mindenekelőtt a GDPR 6. cikkének (1) bekezdésében találjuk. Összehasonlítva az Adatvédelmi Irányelv 7. cikkével, megállapíthatjuk, az új szabályozás jelentős mértékben épít a Rendelettel hatályon kívül helyezett Adatvédelmi Irányelvre, sok esetben szó szerint átveszi az új szabályozás a korábbi megfogalmazást. Elmondható tehát, hogy alapvetően az eddigi ismert jogalapok élnek tovább.

Speciális rendelkezések találhatóak a GDPR 7-10. cikkeiben, melyek kiegészítik a 6. cikkben felsorolt hat alapelvet. Itt találhatóak a hozzájárulás további feltételei, a gyermekek hozzájárulásával kapcsolatos speciális esetkör, továbbá itt kerültek szabályozásra a személyes adatok különleges kategóriáinak kezelésére, valamint a büntetőjogi felelősség megállapítását tartalmazó határozatokra vonatkozó adatkezelési szabályok.

Általános elvként lehet kiemelni, hogy egy meghatározott célból végzett adatkezelési művelet nem alapulhat többféle jogalapon. Ennek ellenére lehetséges, hogy több jogszerű jogalapra támaszkodjon az adatkezelés, így ha több célra történik az adatkezelés, minden célhoz kapcsolódhat egy jogalap. Azonban az adatkezelőnek meg kell határoznia ezeket az adatkezelési célokat és a hozzá kapcsolódó megfelelő jogalapot. A jogalap nem változtatható meg az adatkezelés során. Az sem lehetséges, hogy az adatalany hozzájárulása mellett biztonsági tartalékként egyéb jogalapokat is megjelöljön az adatkezelő a hozzájárulás visszavonása esetére.

4.3. A hozzájárulás

A GDPR 6. cikk (1) bekezdése elsőként a hozzájárulást említi a jogalapok között. Eszerint személyes adatok kezelése jogszerű, ha „az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez”.

A hozzájárulás fogalmát a GDPR 4. cikke a következőképpen határozza meg: *„az érintett akaratának:*

- önkéntes,
- *konkrét*
- *megfelelő tájékoztatáson alapuló és*
- *egyértelmű kinyilvánítása,*

amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez”.

Az érintett hozzájárulása a legjobban elterjedt és általánosan alkalmazott jogalap. Alapja az érintett önálló döntése. Az érintett hozzájárulása az emberi méltósághoz való jogból eredeztethető személyes adatok védelméhez való jog, az adatalany információs önrendelkezési jogának a megtestesülése. A középpontban tehát az adatalany és döntése áll, azonban a hozzájárulás alább bemutatott elemei komoly kötelezettségeket és feladatot jelentenek az adatkezelők számára annak biztosítására, hogy az érintett döntése megalapozott legyen és valóban az egyén valós akaratát fejezze ki.

4.3.1. Önkéntesség

A hozzájárulás akkor önkéntes, ha az érintettnek valódi választási lehetősége van, azaz szabadon dönthet arról, hogy az adatkezeléshez megadja-e a hozzájárulását vagy sem. Ezt erősíti meg az Adatvédelmi Munkacsoport hozzájárulásról szóló 15/2011. számú véleménye[60] is, melyben az olvasható, hogy a hozzájárulás jogalapként csak akkor jöhet szóba, ha valódi választási lehetőség áll az érintett rendelkezésére, és nem áll fenn a megtévesztés, a megfélemlítés, a kényszerítés vagy más jelentős negatív következmény veszélye a hozzájárulás megtagadása esetén.

Az önkéntesség a hozzájárulás azon fogalmi eleme, ami szorosan kapcsolódik a megfelelő jogalap megválasztásának kérdéséhez. Egy olyan alkotórész, melynek megléte közvetlen kihatással van az adatkezelés jogszerűségére, hiszen ha az önkéntesség nem valósul meg, úgy az azt jelenti, hogy a hozzájárulás nem a megfelelő jogalap az adott adatkezelés esetében.

Annak megállapítása során, hogy a hozzájárulás önkéntes-e, figyelembe kell venni a GDPR 7. cikk (4) bekezdésében foglalt kérdést is, nevezetesen, hogy „a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez”. Ennek megértéséhez egy példát is hoz az Adatvédelmi Munkacsoport új, a hozzájárulás fogalmát értelmező, WP259 jelzésű iránymutatása.[61] Eszerint adott egy fényképszerkesztő alkalmazás, amely arra kéri a felhasználókat, hogy a szolgáltatás használatához adjanak hozzáférést GPS szerinti helyzetükhöz, melyet viselkedésalapú reklám céljára kíván használni. Mivel sem a tartózkodási hely, sem a viselkedésalapú reklám nem szükséges a fényképszerkesztéshez és túlmegy az alapvető szolgáltatás biztosításán, a hozzájárulás nem tekinthető önkéntesnek.

A (42) és (43) preambulumbekezdések több olyan esetet is felsorolnak, ahol a hozzájárulás önkéntessége nem valósul meg, így ezekben az esetekben a hozzájárulás nem szolgálhat érvényes jogalapként a személyes adatok kezeléséhez. Ezek az esetek az alábbiak:

Amikor az érintett és az adatkezelő között egyértelműen egyenlőtlen viszony áll fenn, például ha az adatkezelő közhatalmi szerv, vagy másik tipikus egyenlőtlen viszony a munkáltatók-munkavállalók viszonya. Az Adatvédelmi Munkacsoport és a NAIH gyakorlatában is régóta jelen van a munkáltató és a munkavállaló közötti kapcsolat természetére visszavezethető korlátozás, hiszen a munkáltató

[60] Lásd: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_hu.pdf (utolsó letöltés: 2018. szeptember 10.)

[61] Lásd: http://naih.hu/files/wp259rev.01_EN_Guidelines_on_Consent.pdf (utolsó letöltés: 2018. szeptember 10.)

és a munkavállaló közötti alá-fölérendeltségi viszonyban könnyen belátható, hogy ha az alkalmazott a hozzájárulását megtagadja, az anyagi vagy nem anyagi természetű hátrányt okozhat neki, ezért nem értelmezhető a hozzájárulás önkéntessége.

Kivételes esetekben mégis alkalmazható a hozzájárulás ezekben a viszonyokban. Alapvetően akkor, amikor egyértelmű, hogy az adatkezelés során feltétel nélküli előnyöket szerez az érintett, és nem érheti őt semmilyen hátrány az adatkezelés megtagadása esetén.

A hozzájárulás így megfelelő jogalap lehet, ha az adatkezelésre nem a munkaviszonnyal, illetve munkáltatói jogok gyakorlásával kapcsolatban kerül sor. Például, ha egy munkáltató az alkalmazottjaiból csapatot szervez egy futóversenyre, amelyhez a munkáltatónak továbbítania kell a szervezők részére azon munkavállalóinak az adatait, akik részt vennének a versenyen, mivel a munkáltató állja a nevezés költségeit. Emellett a munkáltató pólókat is biztosít a versenyre, ezért a munkavállalók pólóméretét továbbítania kell egy pólót készítő vállalkozás részére.

Ez két különböző adattovábbítást jelent, és mindkettőhöz egymástól függetlenül önkéntes hozzájárulást tud adni a munkavállaló anélkül, hogy ennek bármilyen következménye lenne a munkaviszonyára nézve.

Nem kívánatosak az olyan esetek sem, amelyek a 7. cikk (4) bekezdésben szerepelnek, vagyis ahol össze van kötve a szerződési feltételek elfogadása a hozzájárulás megadásával, vagy egy szerződés vagy szolgáltatás teljesítését összekapcsolják a hozzájárulási kérelemmel annak érdekében, hogy olyan adatot kezeljenek, ami nem szükséges a szerződés vagy szolgáltatás teljesítéséhez. A (43) preambulumbekezdés konkrétan kimondja azt, hogy a hozzájárulás nem tekinthető önkéntesnek, ha az adatkezelő nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez, illetve ha egy – például szolgáltatási – szerződés teljesítését a hozzájárulástól teszik függővé, annak ellenére, hogy a hozzájárulás nem szükséges a szerződés teljesítéséhez. Ez az eset ugyanis ahhoz a mindennapokban gyakran előforduló választás elé állíthatja az érintettet, hogy vagy megadja a hozzájárulását személyes adatai kezeléséhez, vagy azt kockáztatja, hogy a szolgáltató megtagadja tőle a kívánt szolgáltatás nyújtását.

A GDPR törekszik annak biztosítására, hogy a személyes adatok kezelése ne történjen ilyen burkolt célokból, illetve, ha nem szükséges, akkor ne történjen ilyenkor adatkezelés, ennek során pedig igyekszik biztosítani azt, hogy a személyes adatok ne váljanak közvetlenül vagy közvetve a szerződés ellenszolgáltatásává.[62]

A 6. cikk szerint az érintett hozzájárulását adhatja személyes adatainak egy vagy több konkrét célból történő kezeléséhez is. A szolgáltatás ugyanis több adatkezelési műveletet is magába foglalhat, melyek több adatkezelési célhoz köthetőek. Ilyen esetekben a (43) preambulumbekezdés értelmében az adatalanynak szabadon kell tudnia választani melyik adatkezelési célt fogadja el. Adott esetben indokolt lehet több hozzájárulás a szolgáltatás nyújtásához/kínálásához.

A már említett WP259 jelzésű iránymutatás szerint, ha az adatkezelő összekapcsol több adatkezelési célt, és nem próbál külön hozzájárulást beszerezni az egyes célokhoz, akkor az az önkéntesség hiányát jelenti.

Példaként az iránymutatás azt az esetet említi, amikor egy kiskereskedő ugyanazon hozzájárulás kérés során kéri az érintettek hozzájárulását ahhoz, hogy marketing célú e-maileket küldjön, valamint ahhoz, hogy megossza az adatokat a csoportjába tartozó más társaságokkal, akkor az nem megfelelő gyakorlat, mivel a két különböző célhoz két külön hozzájárulásnak kellene lennie.

A (42) preambulumbekezdés egy további fontos kötelezettséget ró az önkéntesség kapcsán az adatkezelőre, nevezetesen, ha az adatkezelés az érintett hozzájárulásán alapul, tudnia kell bizonyítani, hogy az érintett hozzájárult az adatkezelési művelethez, ezen belül pedig azt is, hogy az érintett megtagadhatja, illetve visszavonhatja a hozzájárulását anélkül, hogy az kárára válna (például extra költségekkel járna). Ha az adatkezelő be tudja bizonyítani, hogy a szolgáltatás igénybevétele során a hozzájárulás visszavonása semmilyen negatív következményt nem jelent az érintettre nézve, akkor ez azt mutatja, hogy a hozzájárulást önkéntesen adták.

[62] Lásd: http://naih.hu/files/wp259rev.01_EN_Guidelines_on_Consent.pdf (utolsó letöltés: 2018. szeptember 10.)

4.3.2. Konkrét

Ez a hozzájárulásnak az az aspektusa, mely azt jelzi, hogy az érintett a körülmények alapján egyértelműen tudott arról, hogy milyen célú adatkezeléshez járul hozzá, vagyis nincs kétség a beleegyezés „tudatossága" felől.

Egy általános hozzájárulás, tehát amikor az érintett az adatkezelő adatkezelési tevékenységéhez általában járul hozzá, nem fogadható el, mert az nem tartalmazza az adatkezelés pontos célját vagy céljait, és így az érintett gyakorlatilag nem tudja, hogy mihez is járul hozzá, így az félreérthető lehet. A célhoz kötöttség elve, valamint a (32) preambulum bekezdés alapján, a hozzájárulás mindaddig kiterjedhet különböző műveletekre, amíg ezek a műveletek ugyanazt a célt szolgálják. Azonban ha az adatkezelő a személyes adatokat új célra kívánja felhasználni, az adatkezelőnek új hozzájárulást kell beszereznie az új adatkezelési célra.

Erre az esetre a WP259 egy olyan példát említ, amelyben egy kábelszolgáltató a fogyasztóknak – hozzájárulásuk alapján – filmeket ajánl a korábbi nézettségi adataikat alapul véve. A későbbiekben azonban úgy dönt, hogy szeretné harmadik személyek részére engedélyezni, hogy ezen adatok alapján célzott reklámot küldjenek a fogyasztóknak. Tekintve azonban, hogy e tevékenység új célnak minősül, ezért új hozzájárulást kell beszereznie.

Annak érdekében, hogy a hozzájárulás egyértelmű legyen, az adatkezeléssel kapcsolatos tájékoztatásnak, valamint a hozzájárulás szövegének, hozzájárulás beszerzésére használt jelölőnégyzet (checkbox) mellé írt szövegrésznek érthetőnek kell lennie, egyértelműen és pontosan utalnia kell az adatkezelés hatókörére és következményeire.

Megállapítható tehát, hogy az adatkezelőnek, aki különböző adatkezelési célokhoz gyűjt hozzájárulást és különböző célokból kezel adatot, biztosítania kell különálló opt-in hozzájárulást[63] mindegyik célhoz, annak biztosítására, hogy a fogyasztók megadhassák a kifejezett hozzájárulásukat az egyes konkrét adatkezelési célokhoz.

4.3.3. Megfelelő tájékoztatáson alapuló

Az érintett az előzetes, megfelelő tájékoztatás alapján képes felismerni azt, hogy az adott adatkezelés milyen hatással van az információs önrendelkezési jogára és a magánszférájára. Megfelelő tájékoztatás hiányában az adatkezelő oldalán olyan információs erőfölény alakulhat ki, amelynek felhasználásával az érintett jogai, érdekei sérülhetnek.

A GDPR 12. cikk (1) bekezdése alapján *„az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében".*

A tájékoztatás tartalma tekintetében aszerint tesz különbséget a GDPR, hogy honnan származnak a kezelt adatok. Amennyiben a személyes adatokat az érintettől gyűjtik, úgy a 13. cikk szerinti, míg ha a személyes adatokat nem az érintettől szerezték meg, a 14. cikk szerinti tartalommal kell megadni a tájékoztatást. Ezek alapján jellemzően az alábbi adatokról kell tájékoztatást nyújtani:

- az adatkezelő személye;
- adatkezelés célja és jogalapja;
- kezelt adatok köre;

[63] Jelentése előzetesen megadott hozzájárulás. Ellentéte az opt-outszabályozási mód, ahol előzetes hozzájárulás nélkül kezelhető a személyes adat és csak tiltakozási/leiratkozási lehetőséget biztosítanak az érintett számára.

- az adatkezelés időtartama;
- érintetti jogok;
- tájékoztatás automatizált döntéshozatalról, beleértve a profilalkotást is;
- ha a hozzájárulás adattovábbításhoz kapcsolódik;
- az adatvédelmi tisztviselő elérhetőségei;
- jogorvoslati lehetőségek.

A megfelelő, előzetes tájékoztatás legegyszerűbb formája egy adatkezelési tájékoztató megalkotása, és annak biztosítása, hogy az érintettek az adatkezelést megelőzően a tájékoztatót megismerhetik. A GDPR azonban nem írja elő, hogy milyen formában kell megadni a tájékoztatást, vagyis arra többféle mód is megfelelő lehet, úgy mint írásos – különféle nyomtatványokon, szabályzatokban – vagy szóbeli nyilatkozat. Fontos azonban, hogy az adatkezelőnek tudnia kell igazolni a tájékoztatás megtörténtét, így – egyes kivételektől eltekintve – az írásbeli, dokumentált tájékoztatási forma a főszabály.

A tájékoztatás megfelelő módjának követelményeit több dokumentum is értelmezte már,[64] ezen dokumentumok az alábbi követelményeket támasztják az adatkezelővel szemben:

- világos és egyszerű nyelvezettel kell megfogalmazni a tájékoztatást, így nem fogadható el az a gyakorlat, amikor az adatkezelő pusztán szó szerint megismétli a jogszabályok szövegét;
- a szövegnek könnyen érthetőnek kell lennie a hétköznapi ember számára is;
- nem használható hosszú, értelmezhetetlen és szakzsargonnal teli adatkezelési tájékoztató, amennyiben egy összetettebb adatkezelésről van szó, annak megértését jelentősen elősegíti, ha az adatkezelő táblázatos formában, illetve példákon keresztül mutatja be az adatkezelést;
- mindig fel kell mérni, hogy kikből áll a célközönség, ehhez kell alakítani a tájékoztató szövegét;
- a hozzájárulás iránti kérelmet más ügyektől egyértelműen megkülönböztethető módon kell előadni, vagyis nem lehet elrejtve az általános szerződési feltételek közzé;
- tagolt és áttekinthető információátadás biztosítja a teljes és könnyen érthető tájékoztatást
- a tájékoztatót a legfontosabb adatkezelési lépések mindegyikénél megismerhetővé kell tenni (például egy regisztráció esetében a regisztráció előtt, a regisztráció folyamatánál, de az információs társadalom jelenlegi, technikailag magas szintű környezetében alapvetően elvárható az is, hogy nem csak a hozzájárulás megszerzésekor tegye közvetlenül elérhetővé az adatkezelő a tájékoztatót, hanem biztosítsa annak folyamatos elérhetőségét).

4.3.4. Az érintett akaratának egyértelmű kinyilvánítása

A GDPR a hozzájárulás fogalmában egyértelművé teszi, hogy az érvényes hozzájáruláshoz az érintett nyilatkozata vagy a megerősítést félreérthetetlenül kifejező cselekedet szükséges. Ez utóbbi az érintett szándékos cselekedetét teszi szükségessé, melyet a (32) preambulum bekezdés pontosít. Eszerint a hozzájárulás formája lehet írásos vagy rögzített szóbeli nyilatkozat, beleértve az elektronikus utat is.

A (32) preambulumbekezdés szerint ilyen hozzájárulásnak minősül az is, ha *„az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó jelölőnégyzetet [checkbox], az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi”.* Az adatkezelőnek olyan rendszert kell kialakítania, amelyben az érintett az adatkezelésre vonatkozó hozzájárulását aktív, tevőleges magatartással tudja kinyilvánítani. Erre jól bevált megoldás a jelölőnégyzet alkalmazása, ahol az érintettnek kell bepipálnia a négyzetet, vagy például egy megerősítő emailben elhelyezett linkre való kattintás, hiszen ez is egy aktív, tevőleges magatartásra készteti az érintettet.

[64] Az Adatvédelmi Munkacsoport már említett 15/2011-es véleménye, a WP259 jelzésű iránymutatás, valamint az átláthatóságról szóló WP260 jelzésű iránymutatás, valamint az adatvédelmi hatóság 2016-os ajánlása.

A hallgatás, illetve egy tevőleges magatartás elmulasztása azonban nem tekinthető kifejezett hozzájárulásnak, így például a checkbox-ban előre elhelyezett jelzés ki nem kapcsolása nem eredményez kifejezett hozzájárulást, vagyis jogszerűtlen a GDPR alapján.

Az Adatvédelmi Munkacsoport WP259 jelű iránymutatása több olyan újabb technológiákra alkalmazható példát is említ az elektronikus úton gyűjtött hozzájárulásra, mint például a kijelzőn való „csúsztatással", okos kamerába integetéssel, vagy az okostelefont meghatározott módon mozgatva tudja megerősíteni az érintett a hozzájárulását.

4.3.5. A hozzájárulás további követelményei

Lényeges kötelezettséget fogalmaz meg a 7. cikk (1) bekezdése az adatkezelőkre nézve. Eszerint az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett hozzájárult az adatkezeléshez. Ezen rendelkezésen túl az elszámoltathatóság elve miatt is nagyon fontos lesz a nyilvántartások vezetése, az adatkezelési műveleteknek rögzítése.

A 7. cikk (3) bekezdése alapján az adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását. Ez azt jelenti, hogy ha a hozzájárulást online adta, akkor lehetővé kell tenni számára azt is, hogy online is visszavonhassa hozzájárulását.

4.4. Szerződéses viszonyon alapuló adatkezelés

A GDPR 6. cikk (1) bekezdésének b) pontja a következőképpen szabályozza a szerződéses jogalapot: *„az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges".*

Ehhez kapcsolódik a (44) preambulumbekezdés, amely megerősíti, hogy *„az adatkezelés jogszerűnek minősül, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség".*

4.4.1. Az érintett szerződő fél

A fenti definíció két esetet szabályoz. Az elsőben a szerződésben szereplő egyik fél az érintett. Ez a megfogalmazás egy olyan érvényes szerződés meglétét feltételezi, amelyben az egyik fél az érintett. Példaként említhető erre a jogalapra az az adatkezelés, amikor az érintett lakcímének kezelésére azért van szükség, hogy az online vásárolt áru kiszállítható legyen, vagy az érintett hitelkártya adatainak kezelésére a biztonságos fizetés végrehajtásához. Szintén általánosan előforduló gyakorlati példa a munkáltatók azon adatkezelése, melynek során munkavállalóik bér és bankszámla adatait kezelik a fizetések átutalásához. Abban az esetben azonban, amikor nincs ilyen szerződés a felek között, például amikor az előbb említett online vásárlás és a termék kiszállítása esetében profilalkotás is történik, tehát amikor az adatkezelő kifejezetten erre irányuló szerződés nélkül összegyűjti és rögzíti az érintett vásárlásait és internethasználati szokásait, nem alkalmazhatja ezt a jogalapot a profilalkotásra, hiszen nem szükséges a szerződés teljesítéséhez.[65]

[65] Lásd: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf (utolsó letöltés: 2018. szeptember 10.)

4.4.2. A szerződés megkötése előtt végzett adatkezelés

A szerződéses jogalap olyan esetben is alkalmazható, amikor a felek között még nem jött létre szerződés. Fontos kritérium azonban, hogy ezen – szerződés megkötését megelőző – lépésekre az érintett érdekében, kezdeményezésére kerüljön sor. Tipikus példa erre az adatkezelésre az árajánlat kérése. Ekkor ahhoz, hogy a szolgáltató meg tudja tenni az érintett felé az ajánlatát, szükséges lehet ideiglenesen kezelnie az érintett elérhetőségi adatain túl akár több adatát is (élet- vagy gépjárműfelelősségbiztosítás esetében meglehetősen széles adatkört). A célhoz kötött adatkezelés elvét azonban itt is érvényesíteni kell, és csak olyan adatot lehet kezelni, ami valóban szükséges a megjelölt cél eléréséhez.

4.5. Jogi kötelezettség és a jogszabályon alapuló adatkezelés

A magyar jogalkotó az Adatvédelmi Irányelv átültetése során nem vette át tételesen az Irányelv 7. cikkében szereplő jogalapokat. Az Infotv. 5. § (1) bekezdés b) pontjában például két jogalap összevonva került szabályzásra, a jogi kötelezettségen alapuló jogalap és a jogszabályon alapuló adatkezelés. Az eddig egységes jogalapként kezelt törvényi jogalapot két külön jogalapként találjuk meg a GDPR szabályai között.

4.5.1. Jogi kötelezettség teljesítéséhez szükséges adatkezelés

A 6. cikk (1) bekezdés c) pontja szerint jogszerű az adatkezelés, ha az *„az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges”.* Törvényen alapuló, kötelező adatkezelést széles körben rendelnek el az adókötelezettségre, társadalombiztosításra vonatkozó jogszabályok, amikor előírják, hogy a munkáltatónak be kell jelentenie munkavállalói béradatait a társadalombiztosítási vagy adóhatóságnak. Ezen jogszabályok rendelkezései a munkáltatók és a munkavállalók számára kötelezettségként jelennek meg, vagyis ezek ténylegesen kötelező adatkezelések. Ez a jogalap alkalmazandó pénzügyi szolgáltatók esetében is, amikor ezek a szervezetek kötelesek a gyanús tranzakciókat jelenteni az adóhatóságnak a pénzmosás elleni szabályoknak megfelelően.

Ahhoz, hogy a 7. cikk c) pontja alkalmazható legyen, a jogi kötelezettséget jogszabálynak kell előírnia. A jogszabálynak meg kell felelnie az adatvédelmi jogszabályoknak, kellően egyértelműnek kell lennie a kezelt adatok meghatározásában és a jogi kötelezettségnek való megfelelés módját illetően. Emellett lényegében egy érdekmérlegelési tesztet kell elvégeznie a jogalkotónak, vagyis értékelnie kell az adatkezelés szükségességét, arányosságát és figyelemmel kell lennie a célhoz kötött adatkezelés követelményére is.

4.5.2. A közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés

A 6. cikk (1) bekezdés e) pontja szerint jogszerű az adatkezelés, ha *„közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges”.*

A 7. cikk e) pontja alkalmazandó olyan esetekben, amikor az adatkezelő rendelkezik hivatali hatáskörrel, vagy van közérdekből elvégzendő feladata, de nincs minden esetben jogi kötelezettsége az adatkezelésre, és az adatkezelés hivatali hatáskörének gyakorlásához, vagy közérdekből elvégzendő feladata végrehajtásához szükséges. Példaként említhető az adóhatóság azon adatkezelése, melynek során összegyűjti és kezeli a befizetendő adó mértékének megállapításához és igazolásához az adózók adóbevallását. De ilyen szervezetnek minősülnek az önkormányzatok, könyvtárak, iskolák is, amelyek adatot kezelnek közérdekű, vagy a rájuk ruházott közhatalmi jogosítvány gyakorlásának keretében.

Kiemelendő esetkör azon adatkezelések köre is, ahol az adatkezelőnek nincs hivatali hatásköre az adatok közzétételére, ám például valamely hivatali hatáskörrel rendelkező szerv részére teszi hozzáférhetővé az adatokat. Ilyen eset lehet például, amikor az adatkezelő bűncselekményt észlel és az ezzel kapcsolatos információkat továbbítja az illetékes bűnüldöző hatóságok részére.

4.5.3. Közös szabályok

A GDPR 6. cikk (2) bekezdése felhatalmazza a tagállamokat, hogy jogszabályokat alkothatnak a 6. cikk (1) bekezdés c) és e) pontjában szabályozott jogalapok pontosítása érdekében: *„a tagállamok […] fenntarthatnak vagy bevezethetnek a személyes adatok kezelésére vonatkozó rendelkezéseket, amelyekben pontosabban meghatározzák az adatkezelésre vonatkozó konkrét követelményeket, és amelyekben további intézkedéseket tesznek az adatkezelés jogszerűségének és tisztességességének biztosítására […]”.*

A GDPR 6. cikk (3) bekezdése szerint a 6. cikk (1) bekezdés c) és e) pontjában szabályozott adatkezelések esetében a jogalapot uniós jog, illetve azon tagállami jog szerint lehet megállapítani, amelynek hatálya alá az adatkezelő tartozik. A jogalap meghatározása során többek között az alábbi követelményekre lehet korrekciót alkalmazni:

- az adatkezelés jogszerűségére vonatkozó általános feltételek tekintetében;
- az adatkezelés tárgyát képező adatok típusára nézve;
- az érintetteket, azokat a jogalanyokat, amelyekkel a személyes adatok közölhetők, illetve az ilyen adatközlés céljaira;
- az adattárolás időtartamára és az adatkezelési műveletekre
- az adatkezelés céljára vonatkozó korlátozásokra.

4.6. Vis maior jellegű adatkezelés

A 6. cikk (1) bekezdés d) pontja értelmében jogszerű az adatkezelés, ha *„az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges”.*

Ezen jogalap olyan helyzetekben biztosít jogalapot személyes adatok kezelésére, amikor az érintett hozzájárulásának beszerzése valamilyen rendkívüli esemény folytán nem szerezhető be. Az adatkezelésre tehát nem az érintett, hanem mások döntése alapján kerül sor, mégpedig vagy az érintett, vagy más természetes személy létfontosságú érdekének védelmében – szűk körben pedig közérdekből (például járványok megelőzése esetében). Példaként leginkább egészségügyi adatkezelések említhetőek, ahol az érintett nincs abban az állapotban, hogy hozzájárulását adhatná egy adatkezeléshez.

A GDPR (46) preambulumbekezdése alapján más természetes személy vonatkozásában ez egy szubszidiárius jogalap: adatkezelésre *„csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető”.*

4.7. Jogos érdek mérlegelésén alapuló adatkezelés

A GDPR 6. cikk (1) bekezdés f) pontja alapján az adatkezelés egyik lehetséges jogalapja az, ha *„az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek”.*

A jogos érdek mérlegelésén alapuló jogalap az a jogalap, ami sok esetben alkalmazható lehet olyan esetekben, ahol nem teljesül a hozzájárulás önkéntességének fogalmi eleme és ennélfogva nem adható érvényes hozzájárulás az adatkezeléshez.

A GDPR kevés fogódzót ad ahhoz, hogy milyen életviszonyokban lehet alkalmazni ezt a jogalapot. A GDPR (47) preambulumbekezdése általánosságban azt mondja ki, hogy *„a jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e* észszerűen *arra, hogy adatkezelésre az adott célból kerülhet sor.”*

Ennek értékelésében iránymutató lehet az érintettnek az adatkezelővel való kapcsolata. Szintén a (47) preambulumbekezdés ebben a tekintetben azt is kimondja, hogy *„jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll”.* Tehát a felek között fennálló ügyfélkapcsolat mindenképpen megalapozhatja a jogos érdek mérlegelésén alapuló jogalap alkalmazását és az adatkezelő a fennálló ügyfélviszony keretében például hasonló termékekről, szolgáltatásokról hirdetést vagy kedvezményekre jogosító kuponokat küldhet az érintettnek.

További alkalmazási lehetőséget tartalmaz a (47) preambulumbekezdés utolsó mondata, mely lehetővé teszi marketing célú adatkezelések esetén való hivatkozását, amikor kimondja, hogy: *„a személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető”.*

Fontos változás az adatvédelmi hatóság eddigi gyakorlatához képest, hogy ahol észszerűen várhatja az érintett, hogy megkeressék hírlevelekkel, ott nem kell majd külön jelölőnégyzet bepipálásával hozzájárulnia a marketing célú adatkezeléshez. Azonban továbbra is szükség lesz megfelelő előzetes tájékoztatásra, melyben az érdekmérlegelési tesztet kell bemutatnia az adatkezelőnek.

A Rendelet (47)-(50) preambulumbekezdései további négy példát említenek, amelyek esetében alkalmazható e jogalap:

- csalások megelőzése céljából végzett adatkezelés;
- vállalkozáscsoporton belül belső adminisztratív célból az ügyfelek és alkalmazottak személyes adatainak továbbítása;
- a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos adatkezelés (túlterheléses támadások, kémprogramok telepítésének megelőzése);
- a bűncselekményekhez vagy a közbiztonságot fenyegető veszélyekhez kapcsolódó, az illetékes hatóságok felé történő adattovábbítás.

Fontos rendelkezés a jogalap alkalmazhatósága szempontjából a 6. cikk (1) bekezdés f) pontjának utolsó mondata, miszerint nem alkalmazható e jogalap közhatalmi szervek által feladataik ellátása során végzett adatkezelésre. Ezen korlátozás alól kivétel lehet egy olyan adatkezelés, ahol nem a közhatalmi szerv feladatának ellátásához kapcsolódik az adatkezelés, mint például egy vagyonvédelmi kamera alkalmazása.

A jogos érdek mérlegelésének középpontjában az érdekmérlegelési teszt áll, amelyben az adatkezelő azt dokumentálja, hogy az adatkezelés miért korlátozza arányosan az érintett jogait.

Az érdekmérlegelési teszt bárhogyan elvégezhető, alkalmazható például az adatvédelmi hatóság

2016-os ajánlásában[66] szereplő öt lépéses teszt, vagy az Adatvédelmi Munkacsoport 6/2014. számú munkacsoporti véleménye[67] is bemutat egy hét lépésből álló tesztet.

Az adatvédelmi hatóság tesztje a következő lépéseket tartalmazza:

1. lépés: szükségesség vizsgálata, azaz annak a felmérése, hogy rendelkezésre állnak-e olyan alternatív megoldások, amelyek alkalmazásával a tervezett cél adatkezelés nélkül megvalósítható (például kamera felhelyezése helyett utasítás, belső szabályozás alkalmazása a nem kívánt magatartás megelőzésére).
2. lépés: az adatkezelő, illetve a harmadik fél jogos érdekének lehető legpontosabb meghatározása, illetve a jogos érdek igazolása (például korábbi jogellenes cselekmények felsorolása vagy azon következmények felvázolása, amelyekkel reálisan számolni kell, és amelyek miatt nem lehet eltekinteni az adatkezeléstől).
3. lépés: Az adatkezelési körülmények kialakítása, előzetes terv készítése.
4. lépés: Az érintetti érdekek, elvárások felmérése az adott adatkezelés vonatkozásában, azaz milyen ellenérveket lehet felsorakoztatni az adatkezeléssel szemben.
5. lépés: Annak meghatározása, hogy miért korlátozza arányosan az adatkezelő jogos érdeke a 4. lépésben meghatározott érintetti elvárásokat. Szükség esetén különböző garanciák építhetők be az adatkezelés folyamatába (adatkezelés időtartama, adatok felhasználásának korlátozott esetei, az adatokhoz hozzáférők korlátozott száma, átláthatóság biztosítása).

Az elszámoltathatóság elve a GDPR egyik új alapelve, amely azt jelenti, hogy az adatkezelőknek be kell tudniuk bizonyítaniuk azt, hogy az adatkezelésük megfelel a GDPR-nak, illetve a tagállami jognak. Ez az alapelv szükségessé teszi, hogy az adatkezelő az egyes döntéseit dokumentálja, de egyébként magából az érdekmérlegelési jogalapból eleve az a kötelezettség fakad az adatkezelők számára, hogy írásban rögzítsék a jogalaphoz szükséges érdekmérlegelési tesztet.

4.8. Személyes adatok különleges kategóriáinak kezelése

A GDPR 9. cikk (1) bekezdése értelmében *„a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos”.*

A 9. cikk (2) bekezdése fenti tilalom alól számos kivételt szabályoz. Ilyen kivétel az érintett kifejezett hozzájárulása a fent említett személyes adatok egy vagy több konkrét célból történő kezeléséhez. Ezen kivétel alkalmazását azonban uniós vagy tagállami jog kizárhatja, ha úgy rendelkezik, hogy az (1) bekezdésben említett tilalom nem oldható fel az érintett kifejezett hozzájárulásával.

A 9. cikk (4) bekezdése szerint a tagállamok további feltételeket – köztük korlátozásokat – tarthatnak hatályban, illetve vezethetnek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.

[66] Lásd: https://www.naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf (utolsó letöltés: 2018. szeptember 10.)

[67] Lásd: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_hu.pdf (utolsó letöltés: 2018. szeptember 10.)

4.9. Bűnügyi személyes adatok kezelése

A GDPR 10. cikke értelmében *„a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatoknak a 6. cikk (1) bekezdése alapján történő kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi. A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet”.*

4.10. Ellenőrző kérdések

Soroljon fel olyan eseteket, amikor a hozzájárulás nem szolgálhat érvényes jogalapként személyes adatok kezeléséhez!

Az adatkezelés mely körülményeiről kell előzetesen tájékoztatnia az adatkezelőnek az érintettet hozzájáruláson alapuló adatkezelés esetén?

A tájékoztatás megfelelő módja tekintetében milyen alapvető elvárások fogalmazhatóak meg egy adatkezelési tájékoztatóval szemben?

Melyek az érdekmérlegelési teszt lépései?

Soroljon fel olyan adatkezeléseket, ahol a jogos érdek mérlegelésén alapuló jogalapot alkalmazná és nevezzen meg olyan esetet, amikor nem alkalmazható ezen jogalap!

5. AZ ÉRINTETTI JOGOK

Az információs társadalom korában az adatalanyok adatkezelésre gyakorolt befolyása rendkívüli mértékben visszaszorult. Az érintettek sok esetben nincsenek teljesen tudatában annak, hogy személyes adataikat ki, milyen célból és milyen körülmények között használja fel. A GDPR-ban foglalt érintetti jogoknak ezért éppen az a kifejezett célja, hogy gyakorlásuk révén kompenzálják az adatkezelők és adatalanyok közötti aszimmetrikus hatalmi viszonyt, garantálják utóbbiak ellenőrzését az adatkezelés vonatkozásában, illetve hogy egyfajta közvetlen jogorvoslati lehetőséget is biztosítsanak az egyének számára abban az esetben, ha az adatok felhasználása nem felel meg a GDPR-ban foglaltaknak.[68] Az érintetti jogok így tehát az információs önrendelkezési jogunk elemi aspektusai.

5.1. Az átláthatóság elvét érvényre juttató jogok

A transzparencia elve azt a követelményt testesíti meg, hogy az adatalany számára átlátható legyen az adatkezelés.[69] Egyrészt előírásokat fogalmaz meg az adatkezelők számára az érintettekkel közölt információk tartalma vonatkozásában, amelyeket elsősorban a tájékoztatáshoz és a hozzáféréshez való jogra vonatkozó rendelkezések tartalmazzák.[70] Másrészt formai és minőségi szempontok érvényre juttatását is szolgálja a tájékoztatás, illetve az érintettel folytatott mindenféle kommunikáció terén. Az adatkezelők e tekintetben fennálló kötelezettségeit az érintetti jogok érvényesítését szolgáló intézkedések között lehet megtalálni.

5.1.1. A tájékoztatáshoz való jog

A tisztességes és átlátható adatkezelés biztosítása érdekében az adatkezelők főszabály szerint kötelesek – proaktív módon – megfelelő tájékoztatást nyújtani az érintettek részére az adatkezelés megkezdése előtt.[71] E jog elsődlegesen azt hivatott tudatosítani az adatalanyokban, hogy az adatkezelő velük kapcsolatban személyes adatokat kíván kezelni. Ennek megfelelően a tájékoztatás tartalma aszerint differenciált, hogy a kezelendő személyes adatokat közvetlenül az érintettől gyűjtik-e, vagy pedig azokat más forrásból szerezte meg az adatkezelő.[72]

---

68 European Union Agency for Fundamental Rights, 2018.
69 GDPR (39) preambulumbekezdés.
70 Article 29 Data Protection Working Party, 2018.
71 European Union Agency for Fundamental Rights, 2018.
72 L. GDPR 13. cikkét és 14. cikk (1)-(2) bekezdéseit.

Az adatokat az érintettől gyűjtik	Az adatokat nem az érintettől gyűjtik
adatkezelő és képviselőjének adatai	adatkezelő és képviselőjének adatai
adatvédelmi tisztviselő adatai	adatvédelmi tisztviselő adatai
adatkezelés célja	adatkezelés célja
adatkezelés jogalapja	adatkezelés jogalapja
személyes adatok címzettjei vagy a címzettek kategóriái	személyes adatok címzettjei vagy a címzettek kategóriái
adattárolás időtartama	adattárolás időtartama
érintetti jogok	érintetti jogok
jogorvoslati lehetőségek	jogorvoslati lehetőségek
automatizált döntéshozatal	automatizált döntéshozatal
adatszolgáltatás önkéntessége vagy kötelező jellege	–
–	személyes adatok kategóriái
–	adatok forrása

1. sz. táblázat: A tájékoztatás tartalma

A táblázatban felsorolt elemek csupán a tájékoztatás minimális tartalmát testesítik meg. Az adatkezelő ugyanis köteles az érintett rendelkezésére bocsátani minden olyan további információt, amely – a személyes adatok kezelésének konkrét körülményeinek és kontextusának figyelembe vételével – szükséges lehet.[73] Példaként említhető, hogy ha *„az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”*, az adatkezelő köteles tájékoztatni az érintetteket, annak érdekében, hogy megtehessék a szükséges óvintézkedéseket.[74]

A tájékoztatáshoz való jog általános korlátját jelenti – akár az érintettektől gyűjtik az adatokat, akár más adatkezelőtől – az az eset, amikor az adatalany már rendelkezik a vonatkozó információkkal. Az adatkezelő ez esetben – az elszámoltathatóság elvére tekintettel – köteles igazolni ezt a tényt.[75]

A közvetetten felvett személyes adatok esetében az általános kivételen túl el lehet tekinteni az információk rendelkezésre bocsátásától, ha az lehetetlen lenne. Abban az esetben viszont, ha azért nem tud az adatkezelő tájékoztatást nyújtani a személyes adatok eredetéről, mivel azok különböző forrásokból származnak, általános tájékoztatást kell adni az érintett részére.[76] Szintén kivételt jelent az, amikor a szóban forgó információk rendelkezésre bocsátása aránytalanul nagy erőfeszítést igényelne az adatkezelő részéről, különösen a közérdekű archiválás céljából, kutatási- vagy statisztikai célból végzett adatkezelések esetében. Nem érvényesül a tájékoztatási kötelezettség akkor sem, amikor az valószínűsíthetően lehetetlenné tenné, vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését, illetve ha az információknak szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia. Végezetül, el lehet tekinteni az információk rendelkezésre bocsátásától, amennyiben az adatok megszerzését vagy közlését az adatkezelőre vonatkozó olyan jogszabály írja elő.

[73] GPDR (60) preambulumbekezdés.
[74] GDPR (86) preambulumbekezdés.
[75] Article 29 Data Protection Working Party, 2018.
[76] GDPR (61) preambulumbekezdés.

5.1.2. A hozzáféréshez való jog

A hozzáféréshez való jog révén az érintett tájékoztatást kaphat a rá vonatkozóan kezelt adatokról. Ezt a jogát az adatalany – egyszerűen és észszerű időközönként – az adatkezelés jogszerűségének megállapítása és ellenőrzése érdekében gyakorolhatja.[77] A hozzáférés által az adatalany megismerheti az adatkezelés körülményeit, annak jogszerű vagy jogellenes voltát. E jog ezért *„szükséges annak lehetővé tételéhez, hogy az érintett [az adatvédelemmel kapcsolatos más] jogait gyakorolja”*.[78]

A hozzáféréshez való jog alapján érintett egyrészt visszajelzést kaphat az adatkezelőtől arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e. Amennyiben igen, úgy az adatkezelő köteles biztosítani az adatalany számára azt, hogy megismerje az alábbi adatokat:

- a személyes adatok kezelésének céljai,
- a kezelt adatok kategóriái,
- az adatok címzettjei vagy címzettek kategóriái,
- az adattárolás időtartama,
- az érintetti jogok és gyakorlásuk feltételei,
- az igénybe vehető jogorvoslati lehetőségek,
- az automatizált döntéshozatallal kapcsolatos információk,
- az adatok forrása (ha az adatokat nem az érintettől gyűjtötték).

A fentieken túlmenően az érintett rendelkezésére kell bocsátani minden olyan további információt, amely az adatkezelés szempontjából releváns lehet. Például a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása esetén, az érintett tájékoztatást kaphat az adatkezelő vagy adatfeldolgozó által nyújtott megfelelő garanciákról.[79] Továbbá az adatalany jogosult megismerni az egészségi állapotára vonatkozó konkrét személyes adatokat, illetve a vele kapcsolatban elvégzett kezeléseket és a beavatkozásokat tartalmazó egészségügyi dokumentációkat.[80]

A hozzáféréshez való jog nem pusztán az adatkezeléssel kapcsolatos tájékoztatást jelenti. Az adatkezelők ugyanis kötelesek tényleges hozzáférést biztosítani az adatalanyok részére a kezelt személyes adatokhoz, mégpedig oly módon, hogy az érintett rendelkezésére bocsátják az adatkezelés tárgyát képező személyes adatok másolatát. A másolat rendelkezésre bocsátásának lehetősége ugyanakkor nem érintheti hátrányosan mások jogait és szabadságait.[81]

5.1.3. Az adathordozhatósághoz való jog

A GDPR újdonságként, a hozzáféréshez való jog egyfajta kiegészítéseként szabályozta az adathordozhatóság lehetőségét. Ez alapján az adatalany jogosult megkapni a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat, ezeket az adatokat továbbíthatja egy másik adatkezelőnek, illetve kérheti a személyes adatok adatkezelők közötti közvetlen továbbítását is. Az adathordozhatósághoz való jog célja tehát az érintettek tudatos magatartásának elősegítése a saját személyes adataik vonatkozásában.[82]

E jog csak automatizált módon, gépi úton megvalósított adatkezelések esetén gyakorolható. Az adathordozhatóság továbbá kizárólag az érintett által az adatkezelő rendelkezésére bocsátott, rá vonatkozó adatokra terjed ki. Osztott személyes adatok tekintetben az adatok megszerzéséhez való jog nem

77 GDPR (63) preambulumbekezdés.
78 2009. május 7-i Rijkeboer ítlet, C-553/07, ECLI:EU:C:2009:293, 51. pont.
79 L. GDPR 15. cikk (2) bekezdés és 46. cikk.
80 GDPR (63) preambulumbekezdés.
81 GDPR 15. cikk (3) és (4) bekezdés.
82 Article 29 Data Protection Working Party, 2017b.

sértheti az egyéb érintettek e rendelet szerinti jogait.[83] Az adatkezelés, amelynek vonatkozásában e joggal az érintett élni kíván, kizárólag hozzájáruláson vagy szerződésen alapulhat. Ez a jog természeténél fogva nem érvényesíthető olyan adatkezelőkkel szemben, akik a személyes adatokat jogi kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása során kezelik.[84]

Az adathordozhatósághoz való jog gyakorlása során az adatkezelő köteles a személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban az érintett rendelkezésére bocsátani. E követelmény akkor teljesül, ha a dokumentum *„olyan fájlformátumú, amely lehetővé teszi a szoftveres alkalmazások számára, hogy a benne lévő egyedi adatokat könnyen azonosítsák, felismerjék és kinyerjék”*.[85] E formátumok lehetnek nyíltak vagy védettek, hivatalos szabványúak vagy ezektől eltérők. Ugyanakkor az adatok kinyerését korlátozó vagy ellehetetlenítő fájlformátumban kódolt dokumentumok nem tekintendők számítógéppel olvashatónak.

Emellett biztosítani kell egyfajta átjárhatóságot, interoperabilitást a formátum vonatkozásában. Általánosságban e fogalom az eltérő és különböző szervezetek együttműködési képességét jelenti *„a kölcsönösen hasznos és kölcsönösen megállapított közös célok érdekében, ideértve az információk és ismeretek megosztását a szervezetek között az általuk támogatott munkafolyamatokon keresztül, a saját [információs és kommunikációs technológia]-rendszereik* közötti adatcsere segítségével*”*.[86] E követelmény azonban nem teremt olyan kötelezettséget az adatkezelők számára, hogy egymással műszakilag kompatibilis adatkezelő rendszereket vezessenek be vagy tartsanak fenn.[87] Mindazonáltal ösztönözni kell őket arra, hogy interoperábilis formátumokat fejlesszenek ki.

Az adathordozhatóság nem érinti a törléshez való jog gyakorlását. Nem járhat ugyanakkor olyan személyes adatok törlésével, amelyeket az érintett valamely szerződés teljesítése céljából bocsátott rendelkezésre, amennyiben a szóban forgó személyes adatokra szükség van az adott szerződés teljesítéséhez. E jog gyakorlása továbbá nem érintheti hátrányosan mások jogait és szabadságait.

5.2. A pontosság elvét érvényre juttató jogok

A pontosság elve azt jelenti, hogy a kezelt személyes adatnak pontosnak és naprakésznek kell lennie.[88] Ez pedig egyrészt kötelezettséget teremt az adatkezelő oldalán arra, hogy a pontosság biztosítása érdekében meghozzanak minden észszerű intézkedést. Másrészt jogot biztosít az adatalanyok számára arra, hogy a pontatlan vagy nem naprakész adatok helyesbítését, törlését kérjék. E jogok testesítik meg hagyományosan az érintetti jogok jogorvoslati funkcióját.[89]

5.2.1. A helyesbítéshez való jog

A helyesbítéshez való jog alapján az érintett kérheti az adatkezelőtől a rá vonatkozó pontatlan személyes adatok helyesbítését, illetve a hiányos személyes adatok kiegészítését. E jog gyakorlása kiterjed-

[83] Az osztott személyes adatok azok, amelyek esetében az információk egynél több érintettre vonatkoznak.

[84] GDPR (68) preambulumbekezdés.

[85] A közszféra információinak további felhasználásáról szóló 2003/98/EK irányelv módosításáról szóló 2013/37/EU irányelv (21) preambulumbekezdés.

[86] Az európai közigazgatások közötti átjárhatósági eszközökről szóló 2009/922/EK határozat 2. cikk a) pont.

[87] GDPR (68) preambulumbekezdés.

[88] Vö. Infotv. 4 § (4) bekezdés.

[89] European Union Agency for Fundamental Rights, 2018.

het az egyszerű elírások, pontatlanságok (például név- vagy számelírás) korrekciójára. Egyszerűbb esetekben ezért az adatkezelők kötelesek indokolatlan késedelem nélkül eleget tenni a kérelemben foglaltaknak. Máskor viszont, amikor a helyesbítéssel érintett információk pontosítása, kiegészítése jelentős érdekeket érinthet, az adatkezelő a helyesbítés megalapozottságának igazolását kérheti az adatalanytól.[90] Ilyen lehet például egy hitelkérelem elbírálása során, valamint a hatósági erkölcsi bizonyítvány kiállítása érdekében kezelt adatok helyesbítése. Az igazolás megkövetelése ugyanakkor nem eredményezheti az adatalanyok jogai gyakorlásának észszerűtlen korlátozását. Az adatkezelő köteles minden olyan címzettet tájékoztatni a személyes adatok helyesbítéséről, akivel, illetve amelylyel a személyes adatot közölték.

5.2.2. A törléshez és elfeledtetéshez való jog

A törléshez való jog alapján az érintett kérheti az adatkezelőtől a személyes adatai kezelésének megszüntetését.[91] Ebben az esetben az adatkezelő köteles személyes adatot oly módon felismerhetetlenné tenni, hogy információ és az adatalany közötti kapcsolat helyreállítása többé már nem lehetséges. A törlést követően tehát az adatkezelő nem rendelkezhet azokkal a technikai feltételekkel, amelyek az információk érintettel való kapcsolatának helyreállításhoz szükségesek.[92] A törlést olyan módon kell elvégezni, hogy a kapcsolat helyreállítása később se legyen lehetséges.

E jog egyrészt akkor gyakorolható, amennyiben – figyelemmel a célhoz kötöttség, az adattakarékosság, illetve a korlátozott tárolhatóság elvére – a személyes adatok kezelésére már nincs szükség. Az adatalany továbbá akkor kérheti személyes adatai törlését, amennyiben:

- az adatkezelés jogellenes,
- a személyes adatok gyűjtésére közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában került sor,[93]
- az érintett visszavonja hozzájárulását,
- az érintett tiltakozik személyes adatai kezelése ellen,
- azt jogszabályi kötelezettség írja elő.

Az elfeledtetéshez való jog tulajdonképpen a törléshez való jog online környezetben történő kiterjesztése. Amennyiben ugyanis az érintett kéri valamely, az adatkezelő által korábban nyilvánosságra hozott személyes adatának törlését, az adatkezelő köteles – a rendelkezésre álló technológia és a végrehajtás költségeinek figyelembevételével – észszerű lépéseket tenni azért, hogy a törlés kezdeményezéséről az ilyen információkat átvevő adatkezelőket tájékoztassa. A tájékoztatás nyomán a címzettek vonatkozásában felmerülő törlési kötelezettség a személyes adatokra mutató linkek, a személyes adatok másolatának, illetve másodpéldányának törlésére is kiterjed.

A törléshez és az elfeledtetéshez való jog nem gyakorolható akkor, ha:

- a személyes adatokat a véleménynyilvánítás szabadságához fűződő jog és az információszabadság gyakorlása céljából kezelik;
- a személyes adatok további megőrzése valamely jogi kötelezettségnek való megfelelés, illetőleg közérdekből végzett feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása, érdekében szükséges;
- a személyes adatok kezelése jogi igények érvényesítése érdekében szükséges;

---

90 Uo.

91 GDPR (65) preambulumbekezdés.

92 L. Nemzeti Adatvédelmi és Információszabadság Hatóság, 2013.

93 Utóbbi esetkör azért jelentős, mivel a gyermekek még nincsenek teljesen tisztában az adatkezelés kockázataival, így akár gyerekként, akár felnőtt korban gyakorolhatják törléshez való jogukat az említett szolgáltatások keretében végzett adatkezelések vonatkozásában.

- a személyes adatok kezelése a népegészségügy területét érintő közérdek érvényesítése, közérdekű archiválás, tudományos és történelmi kutatási vagy statisztikai céljából végzett szükséges.

Az adatkezelő köteles minden olyan címzettet tájékoztatni a személyes adatok törléséről, akivel, illetve amellyel a személyes adatot közölték.

5.2.3. Az adatkezelés korlátozásához való jog

Az érintett kérheti az adatkezelőtől az adatkezelés korlátozását. Az adatkezelőnek ez esetben zárolnia kell a személyes adatokat, azaz ideiglenesen be kell szüntetnie az információkon végzett összes műveletet mindaddig, ameddig fennáll az azt megalapozó érdek. A zárolásra alkalmas módszer lehet személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezése, az adatokhoz való felhasználói hozzáférés megszüntetése, vagy az adatok ideiglenes eltávolítása.[94] Szemben tehát a törléssel, a korlátozása során az adatkezelő személyes adatok feletti kontrollja nem szűnik meg teljes mértékben.

Az adatalany egyrészt akkor élhet e jogával, ha vitatja a személyes adatok pontosságát. Ez esetben a zárolás arra az időtartamra vonatkozik, amely alatt az adatkezelő ellenőrizni tudja a személyes adatok pontosságát. Másrészt, jogellenes adatkezelés esetén, az érintett a törlés helyett kérheti a személyes adatok felhasználásának korlátozását is. Harmadrészt zárolni lehet a személyes adatokat abban az esetben is, ha azok kezelésére már nincs szükség, de az adatalany a jogi igényének érvényesítése érdekében ezt kéri. Végezetül zárolni kell az adatokat akkor is, ha az érintett tiltakozott az adatkezelés ellen. Ekkor az adatkezelés korlátozásának időtartama addig terjed, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben vagy sem.

Korlátozás esetén kizárólag az érintett hozzájárulása alapján, jogi igények előterjesztése vagy mások jogainak védelme érdekében, valamint fontos közérdekéből lehet a személyes adatokon újból műveleteket végezni.

Az adatkezelő köteles előzetesen tájékoztatni az érintettet az adatkezelés korlátozásának feloldásáról. Továbbá minden olyan címzettet tájékoztatni kell az adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték.[95]

5.3. A tiltakozáshoz való jog

Egyes jogszerű gazdasági érdekek vagy közérdek szükségessé teheti a személyes adatok kezelését, függetlenül az adatalanyok akaratától.[96] Ilyen esetekben a korrekciós mechanizmusok hiányában a személyes adatok védelme kiüresedhetne. Az érintett tiltakozáshoz való jogának célja éppen ezért egyensúlyt teremteni a személyes adatok védelméhez fűződő jog, valamint az adatkezelő vagy harmadik személyek jogszerű érdekei között.[97]

---

94 GDPR (67) preambulumbekezdés.

95 European Union Agency for Fundamental Rights, 2018.

96 2014. május 13-i Google ítélet, C-131/12, ECLI:EU:C:2014:317, 81. pont; 2017. március 9-i Manni ítélet, C-398/15, ECLI:EU:C:2017:197, 49-50. pontok.

97 European Union Agency for Fundamental Rights, 2018.

Főszabály szerint az adatalany bármely, a saját helyzetével kapcsolatos okból, időbeli megkötés nélkül tiltakozhat a személyes adatai kezelése ellen, amennyiben az adatkezelés közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges, illetve ha az jogszerű érdekmérlegelésen alapul.[98] Megilleti továbbá az érintettet a tiltakozáshoz való jog, amennyiben a személyes adatainak kezelésére kutatási vagy statisztikai célból került sor. Az adatkezelő ez esetben nem kezelheti tovább a személyes adatokat, azokat törölni köteles.

Az adatkezelő bizonyíthatja, hogy a saját érdeke elsőbbséget élvez az érintett érdekeivel, alapvető jogaival és szabadságaival szemben. Ilyen lehet például az, amikor az adatkezelést kényszerítő erejű jogos okok indokolják, vagy ha az adatok felhasználása jogi igények előterjesztéséhez kapcsolódik. Kutatási vagy statisztikai célú adatkezelés esetén pedig azt kell igazolni, hogy az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség. Amennyiben az adatkezelő érdekei elsőbbséget élveznek az érintett érdekeivel szemben, a tiltakozáshoz való jog nem érvényesíthető. A közvetlen üzletszerzés érdekében végzett adatkezelés, például hírlevelek küldése esetén az érintett tiltakozási joga nem esik korlátozás alá. Az adatalany tehát bármikor, díjmentesen jogosult a személyes adatainak – eredeti vagy további – kezelése ellen tiltakozni. Az adatkezelő a továbbiakban e célból nem kezelheti a személyes adatokat.

5.4. Automatizált döntéshozatal egyedi ügyekben

A modern világban számos esetben fordul elő az, hogy emberi beavatkozás nélkül, kizárólag technológiai eszközök alkalmazása révén születnek döntések. Példaként említhető az online hitelkérelem elbírálás, az online munkaerő-toborzás, a csalások és az adócsalás nyomon követése és megelőzése, valamint a profilalkotás is. E döntések jelentős befolyással lehetnek az egyének életére, társadalmi helyzetére, munkavállalására.[99] Főszabály szerint ezért az adatalany jogosult arra, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amely a rá vonatkozó egyes személyes jellemzők kiértékelésén alapul, és amely rá nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti.

E jog nem érvényesül akkor, ha az adatkezelés szerződéses jogalapon vagy az érintett kifejezett hozzájárulásán alapult. Másrészt, korlátozottan érvényesül e jog, amennyiben a döntés meghozatalát olyan jogszabály teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít. A kivételek azonban csak abban az esetben alkalmazhatók, amennyiben az adatkezelés nem érint különleges adatokat. Ilyen esetekben – a hozzájáruláson alapuló adatkezelést leszámítva – az érintett jogosult:

- emberi beavatkozást kérni az adatkezelőtől,
- kifejezni álláspontját,
- kifogást benyújtani a döntéssel szemben.[100]

Az adatkezelő köteles az első kapcsolatfelvétel során kifejezetten felhívni az érintett figyelmét a tiltakozáshoz való jogra, a vonatkozó tájékoztatást pedig egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

98 Article 29 Data Protection Working Party, 2014.
99 GDPR (71) preambulumbekezdés.
100 Article 29 Data Protection Working Party, 2017a.

5.5. Az érintetti jogok korlátozásának általános követelményei

Az információs önrendelkezési joghoz hasonlóan az éritetti jogok sem abszolút, korlátozhatatlan jogosultságok. Az uniós vagy nemzeti jogalkotó jogosult jogalkotási intézkedést hozni az egyes jogok korlátozása érdekében. Ennek feltétele, hogy a korlátozás tiszteletben tartsa az alapvető jogok és szabadságok lényeges tartalmát, valamint hogy az szükséges és arányos legyen egy demokratikus társadalomban az alábbi legitim cél vagy célok védelme érdekében:

- nemzetbiztonság,
- honvédelem,
- közbiztonság,
- bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését,
- az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot,
- a bírói függetlenség és a bírósági eljárások védelme,
- a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása,
- a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység,
- az érintett védelme,
- mások jogainak és szabadságainak védelme,
- polgári jogi követelések érvényesítése.

Az érintetti jogok korlátozását előíró jogszabálynak részletes rendelkezéseket kell tartalmaznia az alábbiak vonatkozásában:

- az adatkezelés céljai vagy kategóriái,
- a kezelt személyes adatok kategóriái,
- a bevezetett korlátozások hatálya,
- a visszaélést, illetve a jogosulatlan hozzáférés vagy továbbítás megakadályozását célzó garanciák,
- az adatkezelő,
- az adattárolás időtartama,
- az alkalmazandó garanciák.

A jogalkotó továbbá köteles felmérni a korlátozás révén az érintettek jogait és szabadságait érintő kockázatokat. Az érintett pedig jogosult tájékoztatást kapni a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját.

5.6. Az adatkezelők további kötelezettségei az érintetti jogok érvényesítése vonatkozásában

Az adatkezelők kötelesek az érintetti jogok gyakorlását elősegítő intézkedéseket hozni, amelyek azt szolgálják, hogy az említett jogosultságok megfelelő módon érvényesüljenek a gyakorlatban. Ebben két intézkedési kör emelendő ki. Egyrészt ide tartoznak az érintett részére nyújtott tájékoztatás, illetve a vele való kommunikációval kapcsolatos előírások. Másrészt pedig az olyan intézkedések meghozatala, amelyek az érintetti joggyakorlást könnyítik meg.

5.6.1. Átlátható tájékoztatás és kommunikáció

Az adatkezelés átláthatóságának elvéből az is következik, hogy az érintettek részére nyújtott minden tájékoztatás – legyen szó a tájékoztatáshoz vagy a hozzáféréshez való jogról, vagy az érintetti jogok gyakorlása iránti kérelemmel kapcsolatos adatkezelői döntésekről – tömör, könnyen hozzáférhető és könnyen érthető legyen.[101] Az információkat főszabály szerint írásban kell megadni. A tájékoztatás emellett nyújtható elektronikus formátumban, például nyilvánosságnak szánt valamely honlapon keresztül is.[102] Kivételes esetben pedig, amennyiben azt az adatalany kéri, szóbeli tájékoztatás is adható.

A tájékoztatást világos és közérthető nyelven kell megfogalmazni. Ennek megfelelően az adatkezelő köteles felmérni azt az érintetti kört, amely vonatkozásában személyes adatokat kíván kezelni, és az adatalanyokhoz igazítottan kell az információkat kialakítani.[103] E kötelezettség különösen a gyermekek, illetőleg más hátrányos helyzetű csoportok – például fogyatékkal élők – vonatkozásában jelent többlet követelményeket. Esetükben az adatkezelőnek minden kommunikációt olyan világos és közérthető nyelven kell megfogalmaznia, amelyet az érintett könnyen megért.

A transzparencia elve továbbá lehetővé teszi, hogy az adatkezeléssel kapcsolatos tájékoztatást szükség esetén az adatkezelők vizuálisan is megjelenítsék.[104] Az információkat adott esetben olyan szabványosított ikonokkal is ki lehet egészíteni, amelyek azok közérthetőséget erősítik. Az ikonok által megjelenítendő információk és a szabványosított ikonok biztosítására vonatkozó eljárások meghatározása az Európai Bizottság hatáskörébe tartozó jogalkotási feladat.

5.6.2. A joggyakorlást elősegítő speciális intézkedések

Az adatkezelő köteles mindent megtenni annak érdekében, hogy elősegítse az adatalany jogainak gyakorlását. Ennek keretében lehetősége van arra, hogy a kérelmek elektronikus benyújtását lehetővé tevő eszközöket alkalmazzon, különös tekintettel az automatizált módszerekkel történő, elektronikus adatkezelésekre.[105] Az érintett személyes adataihoz való hozzáférése továbbá biztosítható egy biztonságos rendszerhez történő távoli hozzáférés útján is.[106] Információs társadalommal összefüggő szolgáltatások esetén pedig a tiltakozáshoz való jog gyakorolható műszaki előírásokon alapuló automatizált eszközökkel is.[107]

Főszabály szerint az adatkezelők az érintetti jogok gyakorlása iránti kérelmek nyomán hozott intézkedésről, vagy az intézkedés elmaradásának okairól és a jogorvoslati lehetőségekről indokolatlan késedelem nélkül, legfeljebb azonban a kérelem beérkezésétől számított egy hónapon belül tájékoztatják az érintettet. Ha az adatkezelő eleget kíván tenni az érintett kérelmében foglaltaknak, a határidő további két hónappal meghosszabbítható, ha a kérelem összetettsége vagy a kérelmek száma ez indokolja. Ebben az esetben a kérelem kézhezvételétől számított egy hónapon belül tájékoztatni kell az adatalanyt a késedelem okairól.

Speciális rendelkezés, hogy ha a személyes adatokat nem az érintettől, hanem más forrásból gyűjtötték, az ügy körülményeit figyelembe véve, észszerű határidőben, de legkésőbb egy hónapon belül kell tájékoztatást nyújtani az adatalany részére.[108] Továbbá a tájékozgatást kapcsolattartási célú

[101] Article 29 Data Protection Working Party, 2018.
[102] GDPR (58) preambulumbekezdés.
[103] Article 29 Data Protection Working Party, 2018.
[104] GDPR (58) preambulumbekezdés.
[105] GDPR (59) preambulumbekezdés.
[106] GDPR (63) preambulumbekezdés.
[107] GDPR 21. cikk (5) bekezdés.
[108] GDPR (61) preambulumbekezdés.

adatkezelés esetén legalább az érintettel való első kapcsolatfelvétel alkalmával, adattovábbítás esetén pedig legkésőbb a személyes adatok első alkalommal való közlésekor kell megadni.

Az érintettek jogainak gyakorlását megkönnyítő intézkedések közé tartozik az, hogy – főszabály szerint – az adatkezelő köteles a tájékoztatást és az intézkedést díjmentesen biztosítani a részükre. E szabály alól kivétel csak az egyértelműen megalapozatlan vagy túlzó kérelem, valamint ha az adatalany a hozzáféréshez való jog gyakorlása keretében további másolatokat igényel. Ilyen esetekben az adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat állapíthat meg.[109]

Végezetül az adatkezelő jogosult minden észszerű intézkedést megtenni a személyazonosság megállapítására, ha kérelmet benyújtó természetes személy kilétével kapcsolatban kétségei merülnek fel. Így például kérheti az adatalanytól a személyazonosság megerősítéséhez szükséges információk nyújtását, különösen az online szolgáltatásokkal és az online azonosítókkal összefüggésben. A személyes adatokat ugyanakkor tilos megőrizni kizárólag abból a célból, hogy a lehetséges kérelmeket az adatkezelő meg tudja válaszolni.[110]

5.7. ellenőrző kérdések

Mi szerint változhat a tájékoztatás tartalma?

Melyek a pontosság elvét érvényre juttató jogosultságok?

Mikor nem érvényesíthető a tiltakozáshoz való jog?

Milyen jogalap(ok) alapján kezelt személyes adatok tekintetében gyakorolható az adathordozhatósághoz való jog?

A hozzáféréshez való jog esetében mit jelent a tényleges hozzáférés biztosítása az érintett részére?

[109] Vö. GDPR 12. cikk (5) bekezdés és 15. cikk (3) bekezdés.

[110] GDPR (64) preambulumbekezdés.

6. MAGATARTÁSI KÓDEX

A GDPR az adatvédelemnek egy olyan megfelelőségi keretrendszerét hozza létre, amelynek középpontjában az elszámoltathatóság alapelve és az érintettek alapvető jogai vannak. Ennek érdekében számos olyan eszközt hoz létre, amely a megfelelést segíti. Ezen eszközök egy része meghatározott esetekben kötelezően alkalmazandó (például az adatvédelmi tisztviselő kijelölése, illetve adatvédelmi hatásvizsgálat elkészítése), míg egy része az adatkezelő vagy adatfeldolgozó által önkéntesen alkalmazható.[111]

A GDPR 40. cikke alapján a tagállamok, felügyeleti hatóságok, a Testület és a Bizottság ösztönzik olyan magatartási kódexek kidolgozását, amelyek – a különböző adatkezelő ágazatok egyedi jellemzőinek, valamint mikro-, kis- és középvállalkozások sajátos igényeinek figyelembevételével – segítik a rendelet alkalmazását. Az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek tehát magatartási kódexeket dolgozhatnak ki, hogy pontosítsák a GDPR alkalmazását. A GDPR tartalmaz egy példálózó felsorolást[112] arra vonatkozóan, hogy mely kérdések vonatkozásában pontosíthatja egy magatartási kódex a GDPR alkalmazását.

A magatartási kódex útján tehát egy szektor, vagy adatkezelők kategóriáit képviselő szervezet létrehozhat egy szabályrendszert arra vonatkozóan, hogy az ezt önkéntesen vállaló adatkezelőknek milyen módon kell a tevékenységüket folytatni adatvédelmi szempontból. A magatartási kódex azáltal válik hatékonnyá, hogy abban részletesen meghatározzák azt, hogy egy adott szakmába vagy szektorba tartozó adatkezelők vagy adatfeldolgozók saját tevékenységüket milyen módon végezhetik a lehető legmegfelelőbben, jogszerűen és etikusan.

6.1. Magatartási kódex jóváhagyása

Amennyiben egy egyesület vagy egyéb szervezet magatartási kódexet kíván kidolgozni, vagy meglévő kódexet kíván módosítani vagy kibővíteni, a tervezetet benyújtja az illetékes felügyeleti hatóságnak.[113] Az illetékes felügyeleti hatóság véleményt bocsát ki arról, hogy a tervezet összhangban van-e a GDPR-ral, és amennyiben úgy ítéli meg, hogy a tervezet elegendő és megfelelő garanciát nyújt, úgy jóváhagyja azt.[114]

Előfordulhat, hogy a kódex több tagállamot is érintő adatkezelési tevékenységekre vonatkozik. Ebben az esetben az illetékes hatóság a jóváhagyást megelőzően a GDPR szerinti egységességi mechanizmus keretében a tervezetet benyújtja a Testületnek,[115] amely a GDPR 64. cikk (1) bekezdés b) pontja alapján véleményt bocsát ki. Amennyiben a Testület véleménye megerősíti, hogy a tervezet összhangban van a GDPR-ral, azt benyújtja a Bizottságnak, amely végrehajtási aktusok útján ha-

[111] European Data Protection Board Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

[112] GDPR 40. cikk (2) bekezdés a)-k) pontjai.

[113] GDPR 40. cikk (5) bekezdés.

[114] GDPR 40. cikk (5) bekezdés.

[115] GDPR 40. cikk (7) bekezdés.

tározhat úgy, hogy a hozzá benyújtott, jóváhagyott magatartási kódex az Unió területén általános érvénnyel rendelkezik.

Az átláthatóság biztosítása értekében a felügyeleti hatóság a jóváhagyott magatartási kódexet nyilvántartásba veszi és közzéteszi.[116] Amennyiben egy kódex a Bizottság döntése alapján általános érvényű, akkor a nyilvánosságáról is a Bizottságnak kell gondoskodnia.[117] Emellett a Testület valamennyi jóváhagyott magatartási kódexet egy nyilvántartásban állítja össze, és megfelelő módon nyilvánosan elérhetővé teszi őket.[118]

6.2. Jóváhagyott magatartási kódexnek való megfelelés ellenőrzése

A magatartási kódex egyik legfontosabb eleme, hogy olyan mechanizmusokat határoz meg, melyek lehetővé teszik, hogy az erre akkreditált szervezet ellenőrizze, hogy a kódex alkalmazását vállaló adatkezelők vagy adatfeldolgozók megfelelnek-e a kódex rendelkezéseinek.[119] Ez biztosítja azt, hogy ellenőrizhető legyen, hogy azon adatkezelők vagy adatfeldolgozók, akik a kódex alkalmazását vállalják, valóban betartják-e az abban foglaltakat.

A magatartási kódexnek való megfelelés ellenőrzését olyan szervezet végezheti, amely a kódex tárgya tekintetében megfelelő szakértelemmel rendelkezik, és amelyet az illetékes felügyeleti hatóság erre akkreditál.[120] A GDPR 41. cikk (2) bekezdése alapján egy magatartási kódexnek való megfelelés ellenőrzésére abban az esetben lehet akkreditálni egy szervezetet, amennyiben az:

- az illetékes felügyeleti hatóság számára kielégítő bizonyítékot szolgáltatott arra nézve, hogy független, és a kódex tárgyában szakértelemmel bír;
- létrehozott olyan eljárásokat, amelyek révén meg tudja állapítani, hogy az érintett adatkezelők és adatfeldolgozók alkalmasak-e a kódex alkalmazására, ellenőrizni tudja, hogy az érintett adatkezelők és adatfeldolgozók betartják-e a kódex rendelkezéseit, és rendszeres időközönként felül tudja vizsgálni a kódex működését;
- létrehozott olyan eljárásokat és struktúrákat, amelyek révén kezelni tudja a kódex megsértésével vagy a kódex adatkezelő vagy adatfeldolgozó általi alkalmazásával kapcsolatos panaszokat, és ezeket az eljárásokat és struktúrákat az érintettek és a nyilvánosság számára átláthatóvá teszi; és
- az illetékes felügyeleti hatóság számára kielégítő bizonyítékot szolgáltat arra nézve, hogy feladataival kapcsolatban nem áll fenn összeférhetetlenség.

A GDPR alapján a felügyeleti hatóságnak közzé kell tennie honlapján az ellenőrző szervezet akkreditációjával kapcsolatos szempontokat, amelynek tervezetét az egységességi mechanizmus keretében meg kell küldeni a Testület részére is.[121]

A fentebb felsorolt feltételeknek, illetve a felügyeleti hatóság által közzétett szempontoknak megfelelő szervezet feladata tehát az, hogy kikényszerítse azt, hogy a magatartási kódex alkalmazását vállaló tagok valóban betartsák az abban előírtakat, ezzel biztosítva az eszköz hatékonyságát és hasznosságát a megfelelés igazolása terén.

[116] GDPR 40. cikk (6) bekezdés.
[117] GDPR 40. cikk (10) bekezdés.
[118] GDPR 40. cikk (11) bekezdés.
[119] GDPR 40. cikk (4) bekezdés.
[120] GDPR 41. cikk (1) bekezdés.
[121] GDPR 41. cikk (3) bekezdés; GDPR 57. cikk (1) bekezdés p) pont.

7. AKKREDITÁCIÓ ÉS TANÚSÍTÁS

A GDPR alapján az átláthatóság és a GDPR-nak való megfelelés elősegítése érdekében a felügyeleti hatóságoknak ösztönözniük kell olyan tanúsítási mechanizmusok, adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek a GDPR előírásainak.[122]

A GDPR pontosítja azokat a specifikus kötelezettségeket, amelyeknek való megfelelést az adatkezelők vagy adatfeldolgozók tanúsítással igazolhatják, ezek:

- a megfelelő technikai és szervezési intézkedések végrehajtására vonatkozó kötelezettség biztosítása és ennek igazolása;[123]
- a megfelelő garanciák biztosításának bizonyítása.[124]

A tanúsítás önmagában nem bizonyítja a megfelelést, azonban felhasználható a megfelelés bizonyításának részeként. Ennek érdekében kiemelten fontos, hogy a tanúsítás átlátható eljáráson keresztül legyen elérhető az adatkezelők és az adatfeldolgozók számára. Ebből következik az is, hogy a tanúsítvány kibocsátására vonatkozó döntés során ki kell térni a szempontok alkalmazásával kapcsolatos indokokra, bizonyítékokra, illetve a tanúsítási eljárás során gyűjtött következtetésekre, véleményekre, vagy tényekből levont következtetésekre is.[125]

A tanúsítás ezáltal lehetővé teszi az érintettek számára is, hogy gyorsan értékelni tudják az adott termék vagy szolgáltatás adatvédelmi szintjét. A tanúsítási mechanizmus tehát elősegíti az érintettek számára az átláthatóságot, illetve az adatkezelők számára a GDPR-nak való megfelelés igazolását.

A GDPR 57. cikk (1) bekezdése alapján a felügyeleti hatóságok egyik feladata az adatvédelmi tanúsítási mechanizmusok ösztönzése. A GDPR tehát nem teszi kötelezővé a felügyeleti hatóságok számára azt, hogy tanúsítási szervezetként járjanak el, azonban általánosságban feltételezi az ehhez szükséges szakértelem meglétét. Tanúsítványt a GDPR alapján a felügyeleti hatóság, vagy az erre akkreditált tanúsító szervezet bocsáthat ki.[126] Ez alapján tehát többféle megoldás elképzelhető a felügyeleti hatóság tanúsítással összefüggő feladataival kapcsolatban:

- a hatóság a saját tanúsítási rendszere alapján állít ki tanúsítványt;
- a hatóság saját tanúsítási rendszere alapján állít ki tanúsítványt, de a megfelelőségértékelés egy részét vagy egészét más szervezetekre delegálja;
- a hatóság megalkotja saját tanúsítási rendszerét, amely alapján más tanúsító szervezetek állítják ki a tanúsítványt;
- a hatóság ösztönözi a piaci szereplőket arra, hogy tanúsítási rendszereket dolgozzanak ki, amelyekre vonatkozóan a tanúsítási szempontokat a hatóság jóváhagyja.

---

122 GDPR 42. cikk (1) bekezdés.

123 GDPR 24. cikk (1) és (3) bekezdései, 25. cikk, és 32. cikk (1) és (3) bekezdései.

124 GDPR 28. cikk (5) bekezdés.

125 European Data Protection Board Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

126 GDPR 42. cikk (5) bekezdés.

7.1. Tanúsító szervezetek akkreditációja

A GDPR 43. cikk (1) bekezdése alapján a tagállamoknak nemzeti jogukban kell rendezniük, hogy az alább felvázolt három megoldás közül egy adott tagállamban milyen módon zajlik a tanúsítási szervezetek akkreditációja:

- az akkreditációt a felügyeleti hatóság végzi az általa kidolgozott követelményrendszer alapján;
- az akkreditációt a 765/2008/EK parlamenti és tanácsi rendelettel összhangban megnevezett nemzeti akkreditáló testület végzi az EN-ISO/IEC 17065/2012 szabvánnyal, illetve a felügyeleti hatóságok által megállapított kiegészítő követelményekkel összhangban;
- az akkreditációt mind a felügyeleti hatóság, mind az akkreditáló testület végzi.

7.2. Tanúsítási szempontok jóváhagyása

A GDPR a tanúsítási szempontok jóváhagyását a felügyeleti hatóságok feladatai között említi, azonban a szempontok kidolgozását nem. Elvileg azonban lehetséges az, hogy az illetékes felügyeleti hatóság jóváhagyja a saját maga által kidolgozott szempontokat, de erre nincs kötelezettsége a hatóságoknak. A tanúsításnak azonban minden esetben jóváhagyott szempontokon kell alapulnia.[127]

A tanúsító szervezet feladata az, hogy tanúsítványokat állítson ki, vizsgáljon felül és újítson meg a tanúsítási mechanizmusok és a jóváhagyott tanúsítási szempontok alapján. Ehhez az szükséges, hogy a tanúsítási szervezet vagy egyéb tanúsítási rendszer tulajdonos eljárásokat dolgozzon ki, így különösen az ellenőrzésre, felülvizsgálatra, panaszkezelésre és a visszavonásra vonatkozóan, illetve megállapítson tanúsítási szempontokat, amelyek alapján a tanúsítvány kiállítható. A tanúsítási szervezet akkreditációjának feltétele a tanúsítási mechanizmus, illetve a tanúsítási szempontrendszer megléte, illetve annak a felügyeleti hatóság, vagy a Testület általi jóváhagyása.[128]

Egy tanúsító szervezet csak egy adott tagállamban bocsáthat ki tanúsítványt, az adott hatóság által jóváhagyott szempontok alapján. Más megközelítésből, a tanúsítási szempontokat az abban a tagállamban illetékes felügyeleti hatóságnak kell jóváhagynia, amelyben az adott szervezet a tanúsítvány kibocsátását tervezi. A másik lehetőség az, hogy egy adott szervezet a Testület által jóváhagyott szempontok alapján bocsát ki tanúsítványt, melynek eredményeként európai adatvédelmi bélyegző állítható ki.[129]

A GDPR 43. cikk (1) bekezdése alapján a tanúsító szervezetek kötelesek tájékoztatni az illetékes felügyeleti hatóságot arról, ha egy tanúsítványt kívánnak kiállítani, illetve megújítani, amely lehetővé teszi, hogy a hatóság gyakorolja korrekciós hatásköreit. Emellett a GDPR 43. cikk (5) bekezdése azt is megköveteli, hogy a tanúsító szervezet közölje az illetékes felügyeleti hatósággal a kért tanúsítvány megadásának vagy visszavonásának okait. A kapott információk alapján az illetékes felügyeleti hatóságok gyakorolhatják azon hatáskörüket, hogy elvégezzék a kiadott tanúsítványok felülvizsgálatát, illetve hogy utasítsák a tanúsító szervezetet, hogy a tanúsítványt ne adja ki, vagy vonja vissza.

---

127 GDPR 42. cikk (5) bekezdés.

128 European Data Protection Board Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

129 European Data Protection Board Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679.

8. A SZEMÉLYES ADATOK HARMADIK ORSZÁGBA TÖRTÉNŐ TOVÁBBÍTÁSA

A GDPR 44. cikk alapján olyan személyes adatok továbbítására, amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni, csak abban az esetben kerülhet sor, a GDPR egyéb rendelkezéseinek betartása mellett, ha az adatkezelő és az adatfeldolgozó teljesíti az V. fejezetben rögzített feltételeket.

A GDPR (101) preambulumbekezdése emlékeztet rá, hogy a nemzetközi kereskedelem és együttműködés bővítéséhez szükség van személyes adatok Európai Unión kívülre történő továbbítására, amely során – tekintettel az ezzel kapcsolatos egyedi kihívásokra és problémákra – azon adatkezelő vagy adatfeldolgozó, aki személyes adatok kíván továbbítani harmadik országba, köteles teljesíteni a GDPR V. fejezetében támasztott feltételeket.

A GDPR V. fejezete tehát olyan szabályokat alkot, amelyeknek a legfőbb célja az, hogy a személyes adatok GDPR által garantált védelmi szintje ne sérüljön, amikor azokat harmadik országokba vagy nemzetközi szervezet részére továbbítják. Ennek érdekében ez a fejezet számos eszközt jelöl meg és hoz létre, amelyeknek az a célja, hogy a személyes adatok a továbbítást követően is megfelelő szintű védelemben részesüljenek.

A megfelelő garanciák vagy azáltal vannak biztosítva, hogy az adott harmadik ország az Európai Bizottság megalapozott véleménye alapján megfelelő szintű védelmet biztosít a személyes adatok vonatkozásában (45. cikk), vagy azáltal, hogy az adatokat továbbító adatkezelő vagy adatfeldolgozó megteremti valamilyen eszközzel a megfelelő garanciákat (46. cikk). Csupán a GDPR 49. cikke szerinti kivételes esetekben kerülhet sor úgy személyes adatok harmadik országba történő továbbítására, hogy sem a megfelelő szintű védelem, sem a megfelelő garanciák nincsenek biztosítva.

A GDPR a harmadik országba történő adattovábbításra vonatkozóan megállapít egy alapelvet (az adattovábbításra vonatkozó általános elv), és ezt követően megállapítja azokat a további feltételeket, amelyeknek teljesítése mellett sor kerülhet személyes adatoknak az Európai Unión kívülre történő továbbítására.

Az adattovábbítás általános elvének lényege az, hogy személyes adatok harmadik országbeli adatkezelőknek, adatfeldolgozóknak történő továbbítása esetén nem sérülhet a természetes személyeknek az Unióban biztosított védelem szintje. A rendelet kiemeli emellett azt is, hogy ennek a védelemnek nem csak a harmadik ország irányába történő, hanem az onnan további vagy újbóli továbbítására is ki kell terjednie.

A Testület elődjének tekintendő 29-es Munkacsoport régóta hangsúlyozza a többszintű megközelítés fontosságát az adattovábbítás eszközeinek alkalmazása során. Ez alapján az adatkezelőnek első sorban meg kell vizsgálnia, hogy az adott harmadik ország megfelelő védelmi szintet biztosít-e, amely alapján a személyes adatok a továbbítást követően is részesülnek az európaihoz hasonló szintű védelemben. Amennyiben az adott ország nem biztosít ilyen védelmet, akkor az adatkezelőnek vagy adatfeldolgozónak kell megpróbálnia a megfelelő garanciákat megteremtenie. Így az adatkezelőknek mindenekelőtt arra kell törekedniük, hogy a 45. és 46. cikk szerinti megfelelő védelem, vagy garanciák biztosítva vannak, és csak akkor kellene alkalmaznia a GDPR 49. cikkében található különös helyzetekben biztosított eltéréseket, ha arra nincs lehetőség.[130]

---

[130] European Data Protection Board Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

8.1. Az adat továbbítása megfelelőségi határozat alapján

Az első tényező tehát, amit meg kell vizsgálni a továbbítást tervező adatkezelőnek vagy adatfeldolgozónak az, hogy az adott célország megfelelő szintű védelmet biztosít-e. A GDPR 45. cikk (1) bekezdése alapján, azt, hogy egy harmadik ország, vagy annak valamely területe, ágazata, vagy egy nemzetközi szervezet megfelelő védelmi szintet biztosít, a Bizottság állapíthatja meg. Ennek során a Bizottság különösen a GDPR 45. cikk (2) bekezdésében foglalt tényezőket kell, hogy figyelembe vegye, így például a jogállamiság, az emberi jogok és alapvető szabadságok tiszteletben tartását, a vonatkozó általános és ágazati jogszabályokat, vagy, hogy az adott országban létezik-e független és hatékony felügyeleti hatóság, amely az adatvédelmi szabályok betartásának biztosításáért felel.

A GDPR viszonylag részletes szabályokat állapít meg a megfelelőségi határozatok elfogadásával kapcsolatban, amelyben arra is kitér, hogy mely körülményeket kell figyelembe venni és elemezni. A GDPR 45. cikk (9) bekezdése arról is rendelkezik, hogy a korábban elfogadott ilyen megfelelőségi határozatok – mint például a Bizottság által az Egyesült Államokkal kapcsolatban elfogadott, a Privacy Shield keretrendszer által biztosított védelem megfeleléséről szóló döntés[131] – hatályban maradnak.

8.2. Megfelelő garanciák alapján történő adattovábbítás

Amennyiben a harmadik ország vonatkozásában, amelybe a személyes adatok továbbítását tervezi az adatkezelő vagy adatfeldolgozó, nem fogadott el a Bizottság megfelelőségi határozatot, az adattovábbításra akkor kerülhet sor, ha ez az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújt, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.[132]

Az alábbi táblázat összefoglalóan tartalmazza a megfelelő garanciák megteremtésére szolgáló, GDPR V. fejezete szerinti eszközöket, aszerint, hogy melyek azok, amelyek a felügyeleti hatóság külön engedélye nélkül alkalmazhatóak, és melyek azok, amelyek csak engedéllyel.

Felügyeleti hatóság külön engedélye nélkül	**Felügyeleti hatóság engedélyével**
Közfeladatot ellátó szervek közötti kötelező erejű, kikényszeríthető jogi eszköz	Adatkezelő vagy adatfeldolgozó és a harmadik országbeli adatkezelő, adatfeldolgozó vagy a címzett közötti szerződéses rendelkezések
Bizottság vagy felügyeleti hatóságok által elfogadott általános adatvédelmi kikötések	Közhatalmi vagy egyéb, közfeladatot ellátó szervek között létrejött, közigazgatási megállapodásba beillesztendő rendelkezések
Jóváhagyott kötelező erejű vállalati szabályok (BCR)	
Jóváhagyott magatartási kódex	
Jóváhagyott tanúsítási mechanizmus	

[131] A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről.

[132] GDPR 46. cikk (1) bekezdés.

A fentiekből látható, hogy két olyan eszköz van, amelynek alkalmazásakor szükséges az adattovábbításhoz az illetékes felügyeleti hatóság engedélye. Azonban azt is ki kell emelni, hogy az első oszlopban található eszközök egy része esetén is feltétele az engedély nélküli alkalmazásnak a konkrét eszköz illetékes felügyeleti hatóság általi jóváhagyása. Így tehát BCR, magatartási kódex és tanúsítás útján is csak akkor lehet a megfelelő garanciákat biztosítani a konkrét adattovábbításhoz, amennyiben magát az eszközt korábban az illetékes felügyeleti hatóság jóváhagyta.

Az ilyen engedélyezés, jóváhagyás során az illetékes felügyeleti hatóság azt vizsgálja meg, hogy az adott rendelkezések, szerződés, kötelező erejű vállalati szabályok, magatartási kódex és tanúsítási mechanizmus alkalmas-e arra, hogy megfelelő garanciákat nyújtson az érintettek számára a harmadik országba történő adattovábbítás esetére, valamint arra, hogy az érintettek számára érvényesíthető jogokat és hatékony jogorvoslati lehetőségeket biztosítson.

8.2.1. Általános adatvédelmi kikötések

A megfelelő garanciákat nyújtó eszközök közül talán a leggyakrabban használt az általános adatvédelmi kikötések, vagy korábbi elterjedt elnevezéssel modellszerződések. A GDPR alapján a Bizottság elfogadhat olyan általános adatvédelmi kikötéseket, amelyeknek megkötésével az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújthat arra az esetre, ha harmadik országbeli adatkezelő vagy adatfeldolgozónak kíván személyes adatokat továbbítani.

Ilyen eszköz alkalmazására már a korábbi adatvédelmi irányelv[133] is adott lehetőséget, mely alapján a Bizottság elfogadott három határozatot,[134] melyek ilyen kikötéseket, általános szerződési feltételeket tartalmaznak. A GDPR úgy rendelkezik, hogy ezek a korábbi bizottsági határozatok mindaddig hatályban maradnak, amíg azokat szükség esetén a GDPR alapján elfogadott határozat nem módosítja, váltja fel, vagy helyezi hatályon kívül.[135]

Általános adatvédelmi kikötéseket a felügyeleti hatóságok is elfogadhatnak, melyek abban az esetben jelentenek megfelelő garanciákat, ha azokat a Bizottság is jóváhagyta.[136]

8.2.2. Kötelező erejű vállalati szabályok (Binding Corporate Rules vagy BCR)

A BCR egy olyan eszköz, amely arra szolgál, hogy személyes adatoknak egy adott vállalatcsoport Európai Unióban letelepedett tagjai által, ugyanazon vállalatcsoport harmadik országban található tagjai részére történő továbbítása esetén megfelelő garanciákat nyújtson. A BCR tehát egy vállalatcsoport által létrehozott, kötelező szabályozásoknak olyan összessége, amelyet annak érdekében alkottak meg, hogy a csoport tagjai közötti adattovábbítás során semmilyen esetben ne csökkenjen a védelmi szint (akkor sem, ha a fogadó szervezet harmadik országban található), illetve, hogy az így létrehozott garanciák kikényszeríthetők legyen mind a csoport tagjaitól, mind az érintettek részé-

[133] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról 26. cikk (4) bekezdése.

[134] A Bizottság 2001/497/EK (2001. június 15.) határozata a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről; A Bizottság 2004/915/EK (2004. december 27.) határozata a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről; A Bizottság 2010/87/EU (2010. február 5.) határozata a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről.

[135] GDPR 46. cikk (5) bekezdése.

[136] GDPR 46. cikk (2) bekezdés d) pont.

ről. A BCR-nak tehát minden olyan alapvető elvet és érvényesíthető jogot magukban kell foglalnia, amelyek megfelelő garanciát nyújtanak a személyes adatoknak vagy azok bizonyos kategóriáinak a továbbítására vonatkozóan.[137]

A megfelelő garanciákat nyújtó eszközök közül egyébként kiemelten, részletesen tartalmaz a GDPR rendelkezéseket a BCR-ról.[138] Ezt az eszközt a 29-es Munkacsoport dolgozta ki az adatvédelmi irányelv 26. cikk (2) bekezdése alapján, és a GDPR hatályba lépését megelőzően ennek a globális jellegű eszköznek az egységességét az így elfogadott munkadokumentumok, és a tagállami felügyeleti hatóságok közötti együttműködés biztosította. A GDPR, a munkadokumentumokban foglaltakat lényegében átvéve, definiálja a BCR-t, és részletes, pontos felsorolást nyújt arról, hogy melyek annak kötelező tartalmi elemei. Emellett rendelkezik arról is, hogy a BCR jóváhagyása során alkalmazni kell a GDPR által létrehozott egységességi mechanizmust,[139] ezzel biztosítva azt, hogy a Testület, az egész Európai Unióra irányadó véleménye által a BCR az illetékes felügyeleti hatóságok külön engedélye nélkül alkalmas eszköz legyen a megfelelő garanciák nyújtására, harmadik országba történő adattovábbítás esetén.

8.2.3. Magatartási kódex és tanúsítás

Harmadik országba történő adattovábbítás esetén megfelelő garanciákat jelenthet a GDPR által létrehozott két új eszköz is: a magatartási kódex és a tanúsítás. Mindkét eszköz esetén feltétel, hogy az adott eszköz a GPDR előírásainak megfelelően jóváhagyásra kerüljön. Külön feltételt jelent továbbá, hogy ezek az eszközök csak abban az esetben alkalmasak arra, hogy a harmadik országban letelepedett adatkezelő vagy adatfeldolgozó bizonyítsa, hogy megfelelő garanciákat biztosít, amennyiben, amennyiben szerződéses vagy egyéb, jogilag kötelező erejű és kikényszeríthető kötelezettségvállalást tesz arra, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogaira vonatkozókat is.[140] Ez a gyakorlatban azt jelenti, hogy mind a magatartási kódex, mind a tanúsítás azzal a feltétellel alkalmazható a harmadik országba történő adattovábbítás eszközeként, ha a harmadik országbeli adatkezelő vagy adatfeldolgozó ezekben foglalt vállalásai kötelezőek és kikényszeríthetők.

8.3. Különös helyzetekben biztosított eltérések

A GDPR 49. cikke felsorolja azokat a helyzeteket, amelyek esetén az adattovábbításra sor kerülhet akkor is, ha a továbbítás célországára vonatkozóan nincs elfogadott megfelelőségi határozat, illetve az adatkezelő vagy adatfeldolgozó nem biztosít megfelelő garanciákat.

A már korábban említett többszintű megközelítés által a Testület tulajdonképpen úgy értelmezi a GDPR V. fejezetének cikkeit, mint amelyek sorrendiséget állítanak fel a továbbítás különböző eszközei között. Az adatkezelőknek és adatfeldolgozóknak mindenekelőtt arra kell törekedniük, hogy a 45. és 46. cikk szerinti megfelelő védelem, vagy garanciák biztosítva legyenek, és csak akkor alkalmazhatják a GDPR 49. cikkében található különös helyzetekben biztosított eltéréseket, ha erre nincs lehetőség.[141]

---

137 GDPR (110) preambulumbekezdés.
138 GDPR 47. cikk.
139 GDPR 47. cikk (1) bekezdés.
140 GDPR 40. cikk (3) bekezdés és 40. cikk (2) bekezdés.
141 European Data Protection Board Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.

A GDPR 49. cikke alapján tehát, megfelelőségi határozat, illetve megfelelő garanciák hiányában csak az alábbi feltételek legalább egyikének teljesülése esetén kerülhet sor személyes adatok harmadik országba történő továbbítására:

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő esetleges kockázatokról;
- az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges;
- az adattovábbítás az adatkezelő és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges;
- az adattovábbítás fontos közérdekből szükséges;
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges;
- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására;
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja, és amely vagy általában a nyilvánosság, vagy az ezzel kapcsolatos jogos érdekét igazoló bármely személy számára betekintés céljából hozzáférhető, de csak ha az uniós vagy tagállami jog által a betekintésre megállapított feltételek az adott különleges esetben teljesülnek.

A 49. cikk által felsorolt helyzetek tehát kivételek azon főszabály alól, hogy személyes adatok harmadik országba történő továbbítására csak akkor van lehetőség, ha a megfelelő védelmi szint biztosított az adott országban, vagy ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújt. Ez alapján, illetve tekintettel a 49. cikk címének megfogalmazására is (különös helyzetekben biztosított), a 49. cikkben található eltéréseket szűken kell értelmezni, annak érdekében, hogy a kivétel ne váljon szabállyá.

A fentieken kívül a GDPR 49. cikk (1) bekezdés utolsó albekezdése tartalmaz még egy speciális helyzetet, amelynek fennállása esetén sor kerülhet személyes adatok harmadik országba történő továbbítására. Az ilyen, érdekmérlegelési teszt elvégzését is megkövetelő, szűken alkalmazható, kivételes adattovábbításnak azonban szigorú és konjunktív feltételei vannak, melyek magukba foglalják azt is, hogy arról mind az érintettet, mind az illetékes felügyeleti hatóságot tájékoztatni kell.

8.3.1. Ellenőrző kérdések a 6., 7., 8. fejezethez

Mire szolgál a magatartási kódex?
Ki bocsáthat ki a GDPR szerinti tanúsítványt?
Mi indokolja a harmadik országba történő adattovábbítás speciális szabályozását?
Mi a harmadik országba történő adattovábbítás alapelve és főbb eszközei?
Mi a lényege a megfelelő garanciák alapján történő adattovábbításnak?

9. A GDPR SZABÁLYAINAK ÉRVÉNYESÍTÉSÉRE IRÁNYULÓ FELÜGYELETI ELJÁRÁSOK TÍPUSAI ÉS JELLEMZŐI

9.1. Bevezető

A NAIH feladata a személyes adatok védelméhez való jog érvényesülésének ellenőrzése és elősegítése, 2018. május 25. napjától a GDPR 57. cikk (1) bekezdés a) pontja alapján nyomon követi és kikényszeríti GDPR alkalmazását.

A NAIH hatásköre nem terjed ki:

- a személyes adatok olyan kezelésére, amelyet a bíróságok igazságszolgáltatási feladatkörükben eljárva végeznek;[142]
- a természetes személyek kizárólag személyes vagy otthoni tevékenység keretében végzett adatkezelésére, ha az semmilyen szakmai vagy üzleti tevékenységgel nem hozható összefüggésbe. Személyes vagy otthoni tevékenységnek minősül például a levelezés, a címtárolás valamint az említett személyes és otthoni tevékenységek keretében végzett, közösségi hálózatokon történő kapcsolattartás és online tevékenységek;[143] továbbá
- az olyan adatkezelésre, amely jogi személyekre vonatkozik (különösen a jogi személy nevére, formájára, valamint a jogi személy elérhetőségére vonatkozó adatok kezelésér);[144]
- az anonim adatokkal végzett statisztikai és kutatási célú adatkezelés.[145]

A GDPR szabályainak érvényesítésére irányuló eljárások típusai:[146]

- vizsgálati eljárás, mely indulhat bejelentés alapján vagy hivatalból;
- adatvédelmi hatósági eljárás, mely indulhat az érintett kérelmére vagy hivatalból;
- adatkezelési engedélyezési eljárás, mely kérelemre indul.

9.2. Az adatvédelmi vizsgálati eljárás

9.2.1. Az eljárás főbb szabályai

A NAIH vizsgálati eljárása nem minősül közigazgatási hatósági eljárásnak, az eljárásra a GDPR-ban meghatározott eltérésekkel az Infotv. rendelkezéseit kell alkalmazni. A NAIH vizsgálati eljárása ingyenes, a vizsgálat költségét a NAIH előlegezi és viseli.

---

142 GDPR 2. cikk (2) bekezdés d) pont.
143 GDPR 2 cikk (2) bekezdés c) pont.
144 GDPR (14) Preambulumbekezdés.
145 GDPR (26) Preambulumbekezdés.
146 Infotv. 38. § (3) bekezdés.

Adatvédelmi vizsgálati eljárást bejelentéssel – a sérelmet szenvedett természetes személy kivételével[147] – bárki kezdeményezhet arra való hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye áll fenn.

Ha a bejelentő kéri, a panaszolt adatkezelő és/vagy az adatfeldolgozó előtt a bejelentő kilétét a NAIH akkor sem fedheti fel, ha ennek hiányában a vizsgálat nem folytatható le. Erről a jogkövetkezményről a NAIH tájékoztatja a bejelentőt.

A NAIH a bejelentést érdemi vizsgálat nélkül elutasíthatja,[148] ha:

- a bejelentésben megjelölt jogsérelem csekély jelentőségű,
- a bejelentés névtelen,
- a bejelentés ismétlődő jellegű, túlzó,
- a bejelentés megalapozatlan.

A NAIH a bejelentést érdemi vizsgálat nélkül elutasítja,[149] ha:

- az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született,
- a bejelentő a NAIH tájékoztatását követően, a jogkövetkezmény ismeretében is fenntartja azt a kérését, hogy a panaszolt adatkezelő és/vagy az adatfeldolgozó előtt a kilétét a hatóság ne fedje fel,
- a bejelentés tárgyában a NAIH hatósági ellenőrzést végez vagy hatósági eljárást folytat.

Ha a bejelentést az alapvető jogok biztosa tette, a NAIH a bejelentést érdemi vizsgálat nélkül csak abban az esetben utasíthatja el, ha az adott ügyben bírósági eljárás van folyamatban, vagy az ügyben korábban jogerős bírósági határozat született.

A NAIH a vizsgálatot megszünteti,[150] ha:

- a kérelem érdemi elutasításának lett volna helye, az elutasítási ok azonban a vizsgálat megindítását követően jutott a NAIH tudomására,
- a vizsgálat folytatására okot adó körülmény már nem áll fenn.

Adatvédelmi vizsgálati eljárás hivatalból is indítható akkor, ha a NAIH felé más szerv jelzi vagy a NAIH maga észleli, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn és hatósági eljárás megindítása az Infotv. szerint nem kötelező.

A NAIH a hivatalból indított vizsgálatot megszünteti, ha a vizsgálat folytatására okot adó körülmény már nem áll fenn.

A vizsgálati eljárás ügyintézési határideje a bejelentés beérkezésétől, illetve a hivatalból történő megindításától számított két hónap. Az Infotv. szabályai szerint az ügyintézési határidőt megszakítja:[151]

- a tényállás tisztásához szükséges adatok közlésére irányuló felhívástól az annak teljesítéséig terjedő idő;
- a vizsgálattal összefüggő irat fordításához szükséges idő; valamint
- a NAIH működését legalább egy teljes napra akadályozó körülmény, ellehetetlenítő üzemzavar vagy más elháríthatatlan esemény időtartama.

147 Az érintett kérelmére ugyanis az 1.3. pontban ismertetettek szerint adatvédelmi hatósági eljárás indul.
148 GDPR 57. cikk (4) bekezdés és Infotv. 53. § (2) bekezdés.
149 Infotv. 53. § (3) bekezdés.
150 Infotv. 53. § (5) bekezdés.
151 Infotv. 55. § (1a) bekezdés.

9.2.2. A tényállás tisztázásának eszközei a vizsgálati eljárása során

A NAIH:[152]

a) a vizsgált adatkezelő kezelésében levő, a vizsgált üggyel összefüggésbe hozható összes iratba betekinthet, illetve azokról másolatot kérhet;
b) a vizsgált üggyel összefüggésbe hozható adatkezelést megismerheti, az adatkezelés helyszínéül szolgáló helyiségbe beléphet;
c) a vizsgált adatkezelőtől, illetve az adatkezelő bármely munkatársától írásbeli és szóbeli felvilágosítást kérhet;
d) a vizsgált üggyel összefüggésbe hozható bármely szervezettől vagy személytől írásbeli felvilágosítást, illetve a vizsgált üggyel összefüggésbe hozható iratról másolatot kérhet; valamint
e) az adatkezelő hatóság felügyeleti szervének vezetőjét vizsgálat lefolytatására kérheti fel.

A c) és d) pont szerinti felvilágosítást az arra felhívott személy megtagadhatja,[153] ha:

- az a személy, akit a NAIH vizsgálatának alapját képező bejelentés érint, a Polgári Törvénykönyv szerinti hozzátartozója vagy volt házastársa;
- a felvilágosítás során magát vagy a Polgári Törvénykönyv szerinti hozzátartozóját, illetve volt házastársát bűncselekmény elkövetésével vádolná, az azzal kapcsolatos kérdésben.

9.2.3. A vizsgálat eredményeként hozható döntések

Amennyiben a NAIH a bejelentés érdemi vizsgálatának eredményeként megállapítja, hogy:

a) a GDPR-ban meghatározott jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye áll fenn:
aa) Az adatkezelőt vagy az adatfeldolgozót a jogsérelem orvoslására, illetve annak közvetlen veszélye megszüntetésére szólítja fel. Ha a felszólítás nem vezetett eredményre ajánlást tehet az adatkezelő vagy az adatfeldolgozó felügyeleti szervének,
ab) ha a jogsérelem, illetve annak közvetlen veszélye jogi szabályozásra vagy annak hiányára, illetve hiányosságára vezethető vissza, ajánlást tehet jogszabály módosításra, hatályon kívül helyezésre vagy jogalkotásra,
ac) a vizsgálatot lezárja, és adatvédelmi hatósági eljárást indít;

b) jogsérelem nem következett be, illetve annak közvetlen veszélye nem áll fenn, a vizsgálatot lezárja.[154]

A vizsgálat eredményéről, a vizsgálat lezárásának indokáról, esetleges intézkedéséről, illetve hatósági eljárás megindításáról a Hatóság a bejelentőt értesíti.

A NAIH vizsgálati eljárása során hozott döntések és a bejelentő értesítésének közigazgatási perben történő felülvizsgálatát törvény nem teszi lehetővé.

A NAIH a bejelentés alapján folytatott vizsgálatról jelentést készíthet, ha az ügyben adatvédelmi hatósági eljárás megindítására vagy bírósági eljárás kezdeményezésére nem kerül sor.

[152] Infotv. 54. § (1) bekezdés.
[153] Infotv. 54. § (3) bekezdés.
[154] Infotv. 56.-58 §.

9.3. Az adatvédelmi hatósági eljárás

Az eljárásra a GDPR-ban és az Infotv.-ben meghatározott eltérésekkel, az Ákr. rendelkezéseit kell alkalmazni.

A személyes adatok védelméhez való jog érvényesülése érdekében a NAIH az érintett erre irányuló kérelmére adatvédelmi hatósági eljárást indít, és hivatalból adatvédelmi hatósági eljárást indíthat.[155]

Az ügyintézési határidő 150 nap.[156] A NAIH az eljárást a GDPR-ban meghatározott együttműködési eljárás és egységességi mechanizmus alkalmazásának időtartamára felfüggeszti, azzal, hogy a NAIH a felfüggesztés időtartama alatt is elvégzi az együttműködési eljárásban és az egységességi mechanizmusban szükséges eljárási cselekményeket.

Az érintettnek jogában áll megbízni egy, a személyes adatok védelmével foglalkozó nonprofit szervet, szervezetet vagy egyesületet, hogy a nevében eljárva nyújtson be kérelmet az adatvédelmi hatóságnál, vagy gyakorolja a bírósági jogorvoslathoz való jogot.

9.3.1. Az eljárás megindítása

A kérelemnek tartalmaznia kell:[157]

- kérelmező és képviselője azonosításához szükséges adatokat és elérhetőségét,
- a feltételezett jogsértés megjelölését,
- a feltételezett jogsértést megvalósító konkrét magatartás vagy állapot leírását,
- a feltételezett jogsértést megvalósító adatkezelő, illetve adatfeldolgozó azonosításához szükséges, a kérelmező rendelkezésére álló adatokat,
- a feltételezett jogsértéssel kapcsolatos állításokat alátámasztó tényeket és azok bizonyítékait, továbbá
- a megjelölt jogsértés orvoslása iránti döntésre vonatkozó határozott kérelmet.

A NAIH hivatalból adatvédelmi hatósági eljárást indít,[158] ha:

- vizsgálata alapján megállapítja, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn, és a vizsgálati eljárásban kibocsátott felszólítás vagy ajánlás alapján a jogsérelem orvoslására, illetve a jogsérelem közvetlen veszélyének megszüntetésére a NAIH által meghatározott határidőben nem került sor,
- vizsgálata alapján megállapítja, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye áll fenn és a GDPR rendelkezései alapján bírság kiszabásának van helye.

Ha a hivatalból indított adatvédelmi hatósági eljárást a NAIH bejelentésen alapuló vizsgálata előzte meg, és a bejelentőt az eljárásba ügyfélként nem vonta be, a Hatóság értesíti az adatvédelmi hatósági eljárás megindításáról, illetve befejezéséről. Az eljárásban sommás eljárásnak és függő hatályú döntés meghozatalának sincs helye. A NAIH a kérelemre induló eljárást is teljes eljárásban folytatja le.

[155] Infotv. 60. § (1) bekezdés.
[156] Infot. 60/A. § (1) bekezdés.
[157] Infotv. 60. § (5) bekezdés.
[158] Infotv. 60. § (3) bekezdés.

9.3.2. Illetékességi kérdések

Kérelemre induló eljárás esetén az érintett kérelmének beérkezését követően, hivatalból induló eljárás esetén az első eljárási cselekmény megtétele előtt a NAIH-nak

- azonosítania kell a (bepanaszolt) adatkezelőt és/vagy adatfeldolgozót,
- meg kell vizsgálnia, hogy helyi ügyről vagy határokon átnyúló adatkezelésről van-e szó,
- meg kell állapítania, hogy ha nem a NAIH, akkor szerinte melyik másik uniós tagállam adatvédelmi hatósága a fő felügyeleti hatóság.[159]

A fő felügyeleti hatóságra az együttműködésre és az egységességi mechanizmusra vonatkozó szabályokat nem lehet alkalmazni abban az esetben, ha az adatkezelést közhatalmi szervek vagy közérdekből eljáró magánfél szervezetek végzik. Ilyen esetben kizárólag az a felügyeleti hatóság lehet illetékes az e rendelettel összhangban rá ruházott hatáskörök gyakorlására, amely annak a tagállamnak a felügyeleti hatósága, ahol az adott közhatalmi szerv vagy magánfél szerv székhelye található.[160]

Határon átnyúló adatkezelést[161] érintő eljárás, ha nem a NAIH a fő felügyeleti hatóság.

A GDPR a fő tevékenységi helyhez/tevékenységi központhoz[162] rendeli általában az eljáró hatóság illetékességét.[163]

A tevékenységi központ megállapításához előbb meg kell határozni az adatkezelő Unión belüli központi ügyvitelének helyét, ha van ilyen. A GDPR-ból következő megközelítés szerint az Unión belüli központi ügyvitel helyén születnek a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntések, és az ilyen döntések végrehajtatására is ez a hely rendelkezik hatáskörrel.

Példa: Egy bank székhelye Frankfurtban található, az összes banki adatkezelési tevékenységét onnan szervezik, biztosítási üzletága viszont Budapesten működik.

Ha az összes biztosítási célú adatkezelési tevékenységre vonatkozó döntések meghozatala és az e döntések végrehajtása az Európai Unió egész területét tekintve a budapesti tevékenységi hely hatáskörébe tartozik, akkor az általános adatvédelmi rendelet 4. cikkének 16. pontjában foglaltak szerint a fő hatóság a személyes adatok határokon átnyúló, biztosítási célú kezelését illetően a NAIH a felügyeleti hatóság, a személyes adatok banki célú kezelését illetően pedig a német hatóság (a hesseni tartományi felügyeleti hatóság) lesz, függetlenül attól, hol találhatóak az ügyfelek.

Amennyiben a szervezet több tevékenységi hellyel is rendelkezik az Európai Unióban, az alapelv szerint a tevékenységi központ a szervezet központi ügyvitelének helye. Ha azonban az adatkezelés céljaira és eszközeire vonatkozó döntéseket másik tevékenységi helyen hozzák, amely egyúttal hatáskörrel rendelkezik az említett döntések végrehajtatására, akkor ezt a tevékenységi helyet kell tevékenységi központnak tekinteni. Az adatkezelők feladata egyértelműen megjelölni, hol hozzák a személyesadat-kezelési tevékenységek céljaira és eszközeire vonatkozó döntéseket.

Egy példával élve, *ha a vállalkozás egy vagy több, határokon átnyúló adatkezelési tevékenységet végez, és a határokon átnyúló mindennemű adatkezeléssel kapcsolatos döntéseket az Unión belüli központi ügyvitel helyén hozzák, akkor az összes, határokon átnyúló adatkezelési tevékenység tekintetében egyetlen fő felügyeleti hatóság jár majd el. Ez a vállalkozás központi ügyvitelének helye szerinti ország felügyeleti hatósága lesz.*

A fő felügyeleti hatóság mellett többi más tagállam felügyeleti hatósága is érintett[164] lehet az eljárásban vagy azért, mert hozzá is panasz érkezett az adott ügyben, vagy az adott ország területén

---

159 A 29-es Adatvédelmi Munkacsoport iránymutatást bocsátott ki (244. számú iránymutatás) az adatkezelő vagy az adatfeldolgozó fő felügyeleti hatóságának meghatározásához.

160 GDPR 55. cikk (2) bekezdés.

161 GDPR 4. cikk 23. pont.

162 GDPR 4. cikk 16. pont.

163 GDPR 56. cikk (1) bekezdés.

164 GDPR 4. cikk 22. pont.

is megtalálható tevékenységi hely okán, vagy az országban tartózkodó adatalanyok jelentős mértékű érintettsége miatt.

Amennyiben a NAIH kérelemre vagy hivatalból induló eljárás esetén azt állapítja meg, hogy az ügy határon átnyúló adatkezelést érint, az eljárást felfüggeszti és írásban tájékoztatja az ügyben szerinte illetékes fő felügyeleti hatóságot. A fő felügyeleti hatóság a tájékoztatását követő három héten belül dönt arról, hogy eljár-e az ügyben.[165] Ha a fő felügyeleti hatóság úgy határoz, hogy eljár az ügyben, az eljárást, a tényállás tisztázást a saját tagállamának eljárási szabályai szerint folytatja le. A hozzá érkezett kérelemre tekintettel a fő felügyeleti hatóság eljárásában a NAIH érintett hatóságként vesz részt.

A fő felügyeleti hatóság és a NAIH, valamint az ügyben esetlegesen érintett más felügyeleti hatóságok a GDPR-ban szabályozott együttműködési eljárás keretében állapodnak meg a döntésről, amely az adatkezelőre és az adatfeldolgozóra nézve kötelező. Az adatkezelővel és az adatfeldolgozóval a fő felügyeleti hatóság közli a döntést.[166]

Ilyen esetben a NAIH a nála indult, felfüggesztett eljárást megszünteti, és a fő felügyeleti hatóság döntését postázza a kérelmező részére. Ezzel egyidejűleg tájékoztatja a Kérelmezőt arról, hogy a döntéssel szemben a fő felügyeleti hatóság szerinti tagállam bíróságához fordulhat jogorvoslatért.

Amennyiben az érintett által a NAIH-nál benyújtott kérelem az együttműködési eljárás során részben vagy egészben elutasításra kerül, a döntést a NAIH-nak kell írásba foglalnia, mivel az elutasításról mindig az a felügyeleti hatóság dönt, amelyhez a kérelmet benyújtották. A kérelmező az elutasító határozatnak a közigazgatási perben történő felülvizsgálatát a Fővárosi Törvényszékhez címzett, de a NAIH-hoz elektronikus úton benyújtott keresetlevélben kérheti.

Hazai/helyi ügyek azok, melyek esetében az adatkezelőnek a tevékenységi központja vagy az Európai Unión belüli kizárólagos tevékenységi helye Magyarországon van. Továbbá azok az ügyek melyek esetében az adatkezelőnek a tevékenységi központja nem Magyarországon van, de az adatkezelési művelet kizárólag Magyarországra irányul, illetve kizárólag Magyarországon tartózkodó polgárokat jelentős mértékben érint és a fő felügyeleti hatóság döntése alapján a NAIH jár el.[167]

Ha a megkeresett fő felügyeleti hatóság úgy határoz, hogy nem jár el az ügyben, a felfüggesztő végzés visszavonását követően az eljárást teljes eljárásban a NAIH folytatja le. A GDPR-ban szabályozott együttműködési eljárás és egységességi mechanizmus alkalmazásával született – az adatkezelőre és/vagy az adatfeldolgozóra vonatkozó kötelező döntést és az érintetti kérelem részben vagy egészben történő elutasításról szóló – döntést a NAIH hozza. A határozat a közigazgatási perben történő felülvizsgálatát a Fővárosi Törvényszékhez címzett, de a NAIH-hoz elektronikus úton benyújtott keresetlevélben kérhetik.

9.3.3. Egyéb eljárásjogi kérdések azokban az ügyekben, melyekben az adatvédelmi hatósági eljárást a NAIH folytatja le

A NAIH eljárásaiban sommás eljárásnak és függő hatályú döntés meghozatalának sincs helye. A NAIH a kérelemre induló eljárást teljes eljárásban folytatja le.

Az adatvédelmi hatósági eljárásban a kérelmezőt költségmentesség illeti meg, a NAIH előlegezi az olyan eljárási költséget, amelynek előlegezése a kérelmezőt terhelné.

A kérelemre indult eljárásokban a kérelmező által megjelölt ellenérdekű felet vagy feleket, azaz az adatkezelőt és/vagy az adatfeldolgozót a NAIH az eljárásba ügyfélként vonja be és erről a tényről az ügyféli jogállás megállapításáról hozott végzéssel tájékoztatja. Egyidejűleg a tényállás tisztázása érdekében végzésben kérdéseket intéz az adatkezelőhöz/adatfeldolgozóhoz.

---

165 GDPR 56. cikk (3) bekezdés.

166 GDPR 60. cikk.

167 GDPR 56. cikk (1)-(2) bekezdés.

Az ügyféli jogállás megállapításáról szóló végzés ellen önálló jogorvoslatnak van helye. Amennyiben az adatkezelő és/vagy az adatfeldolgozó az ügyféli jogállását vitatja és emiatt közigazgatási perben a végzés felülvizsgálatát kezdeményezi, az eljárás megszakad. Az adatkezelő és/vagy az adatfeldolgozó ügyféli jogállása ugyanis olyan előkérdés, melynek jogerős elbírálásáig a tényállás tisztázására nincs lehetőség.

Ha a döntéshozatalhoz nem elegendőek a rendelkezésre álló adatok, a NAIH bizonyítási eljárást folytat le.

A GDPR szerint azt, hogy az adatkezelés a személyes adatok kezelésére vonatkozó, jogszabályban vagy a GDPR-ban meghatározott előírásoknak megfelel, az adatkezelő, illetve az adatfeldolgozó köteles bizonyítani.[168]

A GDPR alapján az eljárása során:

- a NAIH utasíthatja az adatkezelőt és az adatfeldolgozót, illetve adott esetben az adatkezelő vagy az adatfeldolgozó képviselőjét, hogy számára a feladatai elvégzéséhez szükséges tájékoztatást megadja;[169]
- a NAIH hozzáférést kap az adatkezelőtől vagy az adatfeldolgozótól a feladatainak teljesítéséhez szükséges minden személyes adathoz és minden információhoz;[170]
- a NAIH felhívására az adatkezelő vagy az adatfeldolgozó, valamint – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselője rendelkezésére bocsátja az adatkezeléseiről vezetett nyilvántartását;[171]
- az adatkezelő és az adatfeldolgozó, valamint – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselője feladatai végrehajtása során a NAIH-al – annak megkeresése alapján – együttműködik;[172]

Ha a Hatóság az adatvédelmi hatósági eljárást a kérelem benyújtását követő kilencven napon belül nem szüntette meg vagy az ügy érdemében nem döntött, a kérelmezőt értesíti az értesítés időpontjáig megtett eljárási cselekményekről.[173]

Amennyiben a NAIH nem jár el a kérelem alapján, vagy három hónapon belül nem tájékoztatja a kérelmezőt az eljárása eredményéről, az érintett az adatvédelmi hatósággal szemben bírósági jogorvoslatra jogosult.[174]

Amennyiben az adatvédelmi hatósági eljárás során a NAIH jogsértést állapít meg vagy a kérelmet részben vagy egészben elutasítja, az eljárást határozattal zárja le. Amennyiben a hivatalból indított eljárás jogsértést nem tár fel, a NAIH az eljárást végzéssel szünteti meg. E döntések a közlésük napján véglegessé válnak, ellenük közigazgatási úton fellebbezésnek helye nincs, bírósági felülvizsgálatuk a – a közléstől számított harminc napon belül – Fővárosi Törvényszékhez címzett, de a NAIH-hoz elektronikus úton benyújtandó keresetlevéllel kezdeményezhető.

9.3.4. A szankcionálás szabályai

Intézkedésként[175] a Hatóság:

- figyelmeztetést adhat ki, amennyiben az adatkezelési tevékenysége[k] valószínűsíthetően sértik [a] GDPR rendelkezéseit;

168 GDPR 5.cikk (2) bekezdés.
169 GDPR 58. cikk (1) a) pontja.
170 GDPR 58. cikk (1) bekezdés e) pontja.
171 GDPR 30. cikk (4) bekezdés.
172 GDPR) 31. cikke.
173 GDPR 77. cikk (2) bekezdés.
174 GDPR 78. cikk (2) bekezdés.
175 GDPR 58. cikk (2) bekezdés.

- elmarasztalhatja az adatkezelőt a GDPR rendelkezéseinek megsértéséért;
- utasíthatja az érintett jogainak gyakorlására vonatkozó kérelem teljesítésére, továbbá ezzel összefüggésben elrendelheti az érintett személyes adatainak helyesbítését, törlését;
- kötelezheti az adatkezelőt arra is, hogy alakítsa át adatkezelési gyakorlatát a GDPR szabályainak megfelelően, valamint átmenetileg, vagy véglegesen korlátozhatja, illetve meg is tilthatja az adatkezelést;
- elrendelheti továbbá személyes adatok harmadik országba továbbításának a felfüggesztését is.

Szankcióként intézkedés alkalmazása mellett vagy helyett bírság kiszabására is sor kerülhet. Bírság helyett megrovás alkalmazására is lehetőség van, például abban az esetben, ha az adatkezelő természetes személy, és a valószínűsíthetően kiszabásra kerülő bírság számára aránytalan terhet jelentene. Kiindulásképpen a felügyeleti hatóságnak értékelnie kell, hogy a szóban forgó eset körülményeinek mérlegelése alapján szükség van-e bírság kiszabására. Amennyiben a bírság kiszabását szükségesnek ítéli, a felügyeleti hatóságnak azt is mérlegelnie kell, hogy a kiszabásra kerülő bírság egy természetes személy számára aránytalan terhet jelentene-e.[176]

A GDPR megköveteli minden egyes eset egyedi értékelését. A bírság kiszabásának szükségessége, valamint mértékének megállapítása során figyelembe kell venni:[177]

- a jogsértés jellegét, súlyosságát, időtartamát, az adatkezelés jellegét, körét, célját, az érintettek számát és az elszenvedett kár mértékét,
- a jogsértés szándékos vagy gondatlan jellegét,
- az adatkezelőnek vagy az adatfeldolgozónak az érintettek által elszenvedett kár enyhítése érdekében tett intézkedéseit,
- az adatkezelő vagy adatfeldolgozó felelősségének mértékét (különös tekintettel az általuk alkalmazott adatbiztonsági, valamint beépített és alapértelmezett adatvédelmet),
- korábban elkövetett jogsértéseket, korábbi, ugyanabban a tárgyban elrendelt intézkedések végrehajtását,
- a NAIH-al a jogsértés megszüntetése érdekében történő együttműködés mértékét,
- a jogsértéssel érintett személyes adatok kategóriáit,
- megfelelt-e a jóváhagyott magatartási kódexnek,
- valamint az eset körülményei szempontjából releváns egyéb súlyosbító vagy enyhítő körülményeket.

A bírság maximális összege 10.000.000 euró, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg lehet, amennyiben a jogsértés például gyermekek információs társadalommal összefüggő adatkezelését, a beépített és alapértelmezett jogvédelem követelményét érinti, illetve amennyiben adatfeldolgozás, az adatkezelési tevékenységek nyilvántartása, adatbiztonság, adatvédelmi incidensek, az adatvédelmi hatásvizsgálat követelményeinek a megsértése körében történik.[178]

A bírság kiszabható legmagasabb összege 20.000.000 euró, illetve vállalkozások esetén az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg, az alábbi jogsértési kategóriák esetében: az adatkezelés elvei, ideértve a hozzájárulás feltételeit is, az érintettek jogai, személyes adatok harmadik országba való továbbítása, speciális tagállami szabályok megsértése, valamint abban az esetben, ha az a NAIH előző pontban bemutatott intézkedéseinek be nem tartása, illetve a NAIH eljárása során az adatkezelés vizsgálata körében a hozzáférés biztosításának elmulasztása miatt volt szükséges. [179]

A bírság kiszabható legmagasabb összege 20.000.000 euró, illetve vállalkozások esetén az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg akkor is, ha a megálla-

[176] GDPR (148) és (150) preambulumbekezdés.
[177] GDPR 83. cikk (2) bekezdés.
[178] GDPR 83. cikk (4) bekezdés.
[179] GDPR 83. cikk (5) bekezdés.

pített jogsértések orvoslása érdekében a felügyeleti hatóság már adott ki korábban utasítást, ezen utasítást azonban az adatkezelő vagy adatfeldolgozó nem tartotta be.[180] Tehát ez valójában végrehajtási bírság, mely alkalmazható akkor is, ha a korábban csak figyelmeztetésben részesített adatkezelő vagy az adatfeldolgozó nem hajtotta végre a hatóság döntésében szereplő utasításokat.

A bírság mértéke százezertől 20.000.000 forintig terjedhet, ha az adatvédelmi hatósági eljárásban hozott határozatban kiszabott bírság megfizetésére kötelezett költségvetési szerv.[181]

A NAIH eljárásában figyelmeztetés és óvadék alkalmazása kizárt, ha a NAIH a mérlegelésére vonatkozó előírások alapján bírság kiszabásának szükségességét állapítja meg.[182]

A NAIH elrendelheti határozatának – az adatkezelő, illetve az adatfeldolgozó azonosító adatainak közzétételével történő – nyilvánosságra hozatalát,[183] ha:

- a határozat személyek széles körét érinti,
- azt közfeladatot ellátó szerv tevékenységével összefüggésben hozta, vagy
- a bekövetkezett jogsérelem súlya a nyilvánosságra hozatalt indokolja.

A határozat megtámadására nyitva álló keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott adatkezeléssel érintett adatok nem törölhetők, illetve nem semmisíthetők meg.[184]

A NAIH döntésének végrehajtását a döntésben foglalt, meghatározott cselekmény elvégzésére, meghatározott magatartásra, tűrésre vagy abbahagyásra irányuló kötelezés vonatkozásában a NAIH foganatosítja.[185]

A NAIH döntésében megállapított fizetési kötelezettség mérséklésének a kötelezett kérelmére nincs helye. A kötelezett kérheti a fizetési kötelezettség, valamint a meghatározott cselekmény elvégzésére, meghatározott magatartásra, tűrésre vagy abbahagyásra irányuló kötelezés teljesítésére halasztás vagy részletekben történő teljesítés (a továbbiakban együtt: teljesítési kedvezmény) engedélyezését. A kérelemben a kötelezett igazolja, hogy rajta kívül álló ok lehetetlenné teszi a határidőben való teljesítést vagy az számára aránytalan nehézséget jelentene.[186]

Ha a teljesítési kedvezmény iránti kérelmet a kötelezett a NAIH döntése végrehajtásának elrendelését követően terjeszti elő, a NAIH teljesítési kedvezményt csak akkor engedélyezhet, ha a kötelezettség határidőben való teljesítését a kötelezetten kívül álló ok tette lehetetlenné.[187]

9.4. A NAIH engedélyezési hatáskörei a GDPR alapján

Az adatvédelmi engedélyezési eljárás a GDPR alapján a felügyeleti hatóságokra ruházott és a NAIH által gyakorolt engedélyezési, jóváhagyási típusú feladat- és hatáskör gyakorlásának közös eljárásrendjét biztosítja. Az eljárásra a GDPR-ban és az Infotv.-ben meghatározott eltérésekkel, az általános Ákr. rendelkezéseit kell alkalmazni. Az adatkezelési engedélyezési eljárásban nincs helye sommás eljárásnak.[188]

Az adatkezelési engedélyezési eljárásért miniszteri rendeletben meghatározott mértékű igazgatási szolgáltatási díjat kell fizetni.

[180] GDPR 83. cikk (6) bekezdés.
[181] Infotv. 61. § (5) bekezdés.
[182] GDPR 83. cikk (7) bekezdés és Infotv. 61. § (5) bekezdés.
[183] Infotv. 61. § (2) bekezdés.
[184] Infotv. 61. § (7) bekezdés.
[185] Infotv. 61. § (8) bekezdés.
[186] Infotv. 61. § (9) bekezdés.
[187] Infotv. 61. § (10) bekezdés.
[188] Infotv. 64/C. § (4) bekezdés.

9.4.1. Az adatkezelési engedélyezési eljárás kérelemre induló eljárás.

A NAIH kérelemre a GDPR:

a) 40. cikkében meghatározott magatartási kódexek tervezetének, kiegészítésének vagy módosításának jóváhagyása,
b) 41. cikkében meghatározott ellenőrzési tevékenység engedélyezése,
c) 42. cikk (5) bekezdésében meghatározott tanúsítási szempontok jóváhagyása,
d) 46. cikk (3) bekezdés a) pontjában meghatározott szerződéses rendelkezések engedélyezése,
e) 46. cikk (3) bekezdés b) pontjában meghatározott rendelkezések engedélyezése,
f) 47. cikkében meghatározott kötelező erejű vállalati szabályok jóváhagyása

iránti adatkezelési engedélyezési eljárást folytat le.[189]

Az engedélyezés iránti kérelemnek tartalmaznia kell:

- kérelmező és képviselője azonosításához szükséges adatokat és elérhetőségét, továbbá
- az a) pontban meghatározott esetben a magatartási kódex, illetve annak kiegészítése vagy módosítása tervezetét,
- a b) pontban meghatározott esetben az általános adatvédelmi rendelet 41. cikk (2) bekezdésében, valamint a NAIH által közzétett engedélyezési követelményekben meghatározott feltételek fennállásának igazolására szolgáló adatokat,
- a c) pontban meghatározott esetben kérelem tartalmazza a tanúsítási mechanizmus általános leírását és a tanúsítási szempontok tervezetét,
- a d) pontban meghatározott esetben a szerződéses rendelkezések tervezetét,
- az e) pontban meghatározott esetben a rendelkezések tervezetét,
- az f) pontban meghatározott esetben a kötelező erejű vállalati szabályok kötelező jellegének igazolására szolgáló adatokat és a kötelező erejű vállalati szabályok tervezetét.[190]

Az adatkezelési engedélyezési eljárásban az a)-c) és f) pontjában meghatározott kérelmek esetén a NAIH a jóváhagyás, illetve az engedély megadhatósága érdekében szükség szerinti alkalommal a kérelem és az annak tárgyát képező tervezetek módosítása vagy kiegészítése vonatkozásában nyilatkozattételre hívhatja fel a kérelmezőt.

Az adatkezelési engedélyezési eljárásban az ügyintézési határidő:

- az a)-c) és f) pontban meghatározott kérelmek esetén 180 nap,
- a d) és e) pontban meghatározott kérelmek esetén 90 nap.

A NAIH az adatkezelési engedélyezési eljárást a GDPR-ban meghatározott együttműködési eljárás és egységességi mechanizmus alkalmazásának időtartamára felfüggeszti, azzal, hogy a NAIH a felfüggesztés időtartama alatt is elvégzi az együttműködési eljárásban és az egységességi mechanizmusban szükséges eljárási cselekményeket.

9.4.2. Döntések

Az adatkezelési engedélyezési eljárásban hozott határozatában a NAIH:

a) a GDPR:
aa) 40. cikkében meghatározott magatartási kódexek tervezetét, kiegészítését vagy módosítását jóváhagyja,
ab) 41. cikkében meghatározott ellenőrzési tevékenységet engedélyezi,

[189] Infotv. 64/A. §.
[190] Infotv. 64/A. § (2) bekezdés.

ac) 42. cikk (5) bekezdésében meghatározott tanúsítási szempontokat jóváhagyja,
ad) 46. cikk (3) bekezdés a) pontjában meghatározott szerződéses rendelkezések alkalmazását engedélyezi,
ae) 46. cikk (3) bekezdés b) pontjában meghatározott rendelkezések alkalmazását engedélyezi,
af) 47. cikkében meghatározott kötelezető erejű vállalati szabályokat jóváhagyja; vagy

b) a kérelmet elutasítja.[191]

A NAIH határozata vagy az eljárást megszüntető végzése a közlése napján véglegessé válik, ellene közigazgatási úton fellebbezésnek helye nincs. A határozat bírósági felülvizsgálata – a közléstől számított harminc napon belül – a Fővárosi Törvényszékhez címzett, de a NAIH-hoz elektronikus úton benyújtandó keresetlevéllel kezdeményezhető.

9.5. Adatvédelmi Incidens bejelentése

Az adatkezelő minden adatvédelmi incidensről nyilvántartást vezet[192]. Azokat az adatvédelmi incidenseket, amelyek valószínűsíthetően kockázattal járnak a természetes személyek jogaira és szabadságaira nézve, bejelenti a NAIH-nak.[193] Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.[194] Az adatkezelőnek az adatvédelmi incidenst haladéktalanul, de legfeljebb az adatvédelmi incidensről való tudomásszerzését követő hetvenkét órán belül be kell jelentenie a NAIH-nak. Az adatvédelmi incidenst nem kell bejelenteni, ha valószínűsíthető, hogy az nem jár kockázattal az érintettek jogainak érvényesülésére.

Ha az adatkezelő a bejelentési kötelezettséget akadályoztatása miatt határidőben nem teljesíti, azt az akadály megszűnését követően haladéktalanul teljesítenie kell, és a bejelentéshez mellékelnie kell a késedelem okait feltáró nyilatkozatát is.

Ha az adatvédelmi incidens az adatfeldolgozó tevékenységével összefüggésben merült fel, vagy azt egyébként az adatfeldolgozó észleli, arról – az adatvédelmi incidensről való tudomásszerzését követően – haladéktalanul tájékoztatnia kell az adatkezelőt.

Az adatvédelmi incidens bejelentésének kötelező tartalmi elemei:

- az adatvédelmi incidens jellegének, beleértve – ha lehetséges – az érintettek körének és hozzávetőleges számának, valamint az incidenssel érintett adatok körének és hozzávetőleges mennyiségének ismertetése;
- az adatvédelmi tisztviselő vagy a további tájékoztatás nyújtására kijelölt más kapcsolattartó nevét és elérhetőségi adatait;
- az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetését; illetve
- az adatkezelő által az adatvédelmi incidens kezelésére tett vagy tervezett – az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb – intézkedések leírását.

Ha a bejelentendő valamely információ a bejelentés időpontjában nem áll az adatkezelő rendelkezésére, azzal az adatkezelő a bejelentést annak benyújtását követően utólag – az információ rendelkezésre állásáról való tudomásszerzését követően haladéktalanul – ki kell egészítenie.

---

191 Infotv. 64/D. §.
192 GDPR 33. cikk (5) bekezdése.
193 GDPR 33. cikk (1) bekezdés.
194 GDPR 33. cikk (1) bekezdés.

Az adatvédelmi incidens bejelentési kötelezettség – a minősített adatot tartalmazó bejelentés kivételével – a NAIH által e célra biztosított elektronikus felületen teljesíti az adatkezelő. Nemzetbiztonsági célú adatkezelés esetén az adatkezelőt terhelő bejelentési kötelezettség teljesítése nemzetbiztonsági érdekbe ütközne, azt e nemzetbiztonsági érdek megszűnését követően kell teljesíteni.

Az incidensjelentés nem minősül az Ákr. szerint kérelemnek és az incidens jelentéssel kapcsolatos eljárás nem indítható kérelemre. Az incidens jelentés hivatalbóli tudomásszerzésnek minősül a hatóság hatáskörébe tartozó ügyre vonatkozóan.

Az eljárási határidő a valószínűsíthetően kockázattal járó incidensek hatósági ellenőrzésére 60 nap.

Abban az esetben, ha az adatkezelő elmulasztja teljesíteni bejelentési, vagy tájékoztatási kötelezettségét, a NAIH-ot megilleti a választás lehetősége a rendelkezésére álló korrekciós hatáskörei gyakorlása közül, amibe beletartozik a körülményeknek megfelelő közigazgatási bírság kivetése, továbbá a GDPR 58. cikk (2) bekezdése szerinti korrekciós hatáskörében megtehető egyéb intézkedés alkalmazása vagy annak mellőzése.

Közigazgatási bírság alkalmazása esetén a kiszabható legmagasabb bírság 10.000.000 euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg.

9.6. Ellenőrző kérdések

Mely adatkezelésekre nem terjed ki a NAIH hatásköre?

Milyen döntések hozhatóak a vizsgálati eljárás eredményeként?

A GDPR alapján melyek a hazai/helyi ügyek ismérvei?

Sorolja fel, hogy a bírság kiszabásának szükségessége, valamint mértékének megállapítása során a milyen szempontokat kell figyelembe venni!

A NAIH kérelemre milyen engedélyezési eljárásokat folytat le a GDPR alapján?

10. ELSZÁMOLTATHATÓSÁG

A GDPR megalkotása során kiemelt szempont volt, hogy az adatkezelőknek eszközöket biztosítson az adatvédelemnek a szervezeten belüli gyakorlati előmozdításához. Ennek sikeres alkalmazásához, illetve kikényszeríthetőségéhez szükséges volt egy általános szabályozás bevezetésére, amely az adatkezelőtől az adatvédelmi tudatosságot megköveteli, a GDPR ennek megfelelően alapelvi rangra emelte az elszámoltathatóság elvét.

Ezzel az adatkezelőnek az adatkezelés megtervezésétől kezdve az adatkezelés megkezdésén át egészen a kezelt személyes adatok törléséig valamennyi adatkezelési műveletet úgy kell megvalósítani, hogy az adatkezelő bármelyik pillanatban bizonyítani tudja hogyan felelt meg az adatvédelmi előírásoknak.

A GDPR 5. cikk (2) bekezdése értelmében az adatkezelő felelős az adatvédelmi alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására (elszámoltathatóság). A Rendelet 24. cikke tovább részletezi az elszámoltathatóság kötelezettségét az adatkezelő feladatainál. Ennek megfelelően az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja, és szükség esetén naprakésszé teszi. Ha az adatkezelési tevékenység vonatkozásában arányos, ennek részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.

Az elszámoltathatóság elve lényegében azt jelenti, hogy az adatkezelőknek mind a szervezeti kultúrájukat, mind valamennyi tevékenységüket az adatvédelemi megfontolásokra tekintettel kell kialakítaniuk, végezniük. Az adatkezelőknek minden egyes lépésüknél el kell gondolkodniuk, hogy az adatvédelmi előírásokat miként vették figyelembe.

Természetesen ezen az általános attitűdön túl a GDPR számos elvi és gyakorlati eszközzel is megpróbálja segíteni az elszámoltathatóság elvének érvényesülését. Ennek megfelelően az elszámoltathatóság követelményének teljesítését segíti elő többek között:

- a beépített és alapértelmezett adatvédelem (25. cikk);
- az adatkezelési tevékenységek nyilvántartása (30. cikk);
- az adatvédelmi hatásvizsgálat (35. cikk);
- az adatvédelmi tisztviselő (37-39. cikk);
- a magatartási kódexek (40-41. cikk) és tanúsítás (42-43. cikk);
- illetve a kötelező erejű vállalati szabályok (47. cikk) stb.

Fontos emellett kiemelni, hogy az elszámoltathatóságnak nem csak a GDPR-ban szereplő eszközökkel lehet megfelelni. Számos olyan adatvédelmet elősegítő technika (Privacy Enhancing Tecnologies) létezik, amely nincs nevesítve a GDPR-ban, de segít az adatkezelőknek az adatvédelmi megfelelés kialakításában és igazolásában.

Ebben a kötetben a terjedelmi megfontolások miatt külön nem szólunk az adatvédelmi tisztviselő jogintézményéről.[195]

---

[195] Az adatvédelmi tisztviselőről lásd Guidelines on Data Protection Officers (‚DPOs') (wp243rev.01). Lásd: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (utolsó letöltés: 2018. szeptember 10.)

11. AZ ADATVÉDELMI HATÁSVIZSGÁLAT

11.1. Az adatvédelmi hatásvizsgálat előzményei és fogalma

Az adatvédelmi hatásvizsgálat lényege az adatkezelés előzetes kontrollja a kockázatok feltárása és a kockázatok mérséklésére teendő intézkedések értékelése révén.

A GDPR 35. cikkében szabályozott adatvédelmi hatásvizsgálat jogintézményének azonban a rendeleti szabályozásnál régebbre nyúló gyökerei vannak. A GDPR szabályozásának bemutatása előtt röviden bemutatjuk a jogintézmény kialakulását.

11.1.1. Az adatvédelmi hatásvizsgálat előképe: a privacy hatásvizsgálat

Az adatvédelmi hatásvizsgálat előképének tekinthető a jogirodalomban a privacy-hatásvizsgálat (Privacy Impact Assessment, PIA) kifejezése. A GDPR-ban azonban nem ez, hanem az adatvédelmi hatásvizsgálat, angol nyelvű szóhasználatával a Data Protection Impact Assessment (DPIA) kifejezés szerepel. Az elnevezésbeli különbség egyebek között az általános személyiségvédelem amerikai és európai fejlődési modelljei közötti eltérésben gyökerezik. Míg az Egyesült Államokban a személyiségi jogi védelem a magánszférához való jog (right to privacy) keretein belül teljesedett ki, addig Európában a szűkebb értelemben vett személyes adatok védelme vált a hatásvizsgálat meghatározó elemévé.[196]

A privacy-hatásvizsgálat gyökerei jellemzően az angolszász-jogrendszerekben (például az Egyesült Államokban, Ausztráliában, Új-Zélandon, Kanadában, az Egyesült Királyságban) találhatók; kialakulásuk az 1990-es évek derekára tehető.[197] A GDPR-ban szabályozott adatvédelmi hatásvizsgálat ettől eltérően viszont újabb jogintézmény, ezért azzal kapcsolatban szűkösebb mértékben áll rendelkezésre releváns szakirodalom. Az alábbiakban ezért a PIA intézménye alapján kíséreljük meg bemutatni a két hatásvizsgálati módszertan alapvető elemeit és fogalommeghatározásait.

A privacy-hatásvizsgálatnak nincs nemzetközileg elfogadott egységes definíciója. Az egyes angolszász definíciók ugyan eltérnek egymástól, azonban azok lényegi fogalmi elemeit figyelembe véve a privacy-hatávizsgálatot úgy lehet meghatározni, mint egy módszert, amely „[…] felméri egy projekt, policy, program, szolgáltatás vagy más kezdeményezés magánszférára gyakorolt hatásait abban az esetben, amennyiben személyes adatok kezelésére kerül sor, valamint az érintettekkel egyeztetve a negatív hatások elkerülése vagy csökkentése érdekében ajánlásokat fogalmaz meg."[198]

A terminológiai különbségek mellett a privacy-hatásvizsgálathoz kapcsolódóan nem létezik egységes módszertan sem. Ez elsősorban az egyes országok jogi és kulturális különbségeire vezethető vissza. A privacy-hatásvizsgálat jogforrásainak szintjei között is tapasztalhatóak eltérések – míg egyes országok (például Kanada, Új-Zéland, Egyesült Államok) hard law-eszközökkel szabályozzák, máshol a soft law-eszközök a meghatározóak.[199]

---

196 Balogh et. al., 2014.
197 Wright – De Hert, 2012
198 Wright – De Hert, 2012.
199 Balogh et. al., 2014.

Ugyanakkor nemcsak a tengerentúli országok adatvédelmi hatóságai, hanem azokkal párhuzamosan európai, így az angol és a francia adatvédelmi hatóságok is már évekkel ezelőtt kidolgozták és azóta is alkalmazzák saját PIA gyakorlatukat.

Az angol és a francia hatásvizsgálatok már jóval a GDPR-ban szabályozott adatvédelmi hatásvizsgálat előtt részletesen szabályozásra kerültek. Mind az angol Information Commissioner's Office (a továbbiakban: ICO), mind pedig a francia Commission Nationale de l'Informatique et des Libertés (a továbbiakban: CNIL) által kidolgozott vizsgálati eljárás egy checklist, azaz ellenőrző lista alapú eljárás.

A checklist-alapú vizsgálati eljárás vitathatatlan előnye, hogy azok nagyban megkönnyítik az egyes adatkezelők számára a hatásvizsgálat lefolytatását, azonban ezzel egyidejűleg magában hordozza azt a veszélyt is, hogy így egy általános, nem a konkrét projektre szabott vizsgálati eljárás kerül lefolytatásra, azaz a vizsgálat nem a konkrét esetben felmerülő kockázatokra fókuszál.[200] Az alábbiakban a francia CNIL által kidolgozott módszertan az alábbi szakaszokra osztható:[201]

1. Elsőként meg kell határozni a kezelt személyes adatok körét, ideértve az érintettek kategóriáját, az adatkezelés célját, valamint annak szükségességét és arányosságát.
2. Ezt követően meg kell vizsgálni, hogy a személyes adatok védelme érdekében milyen ellenőrzési mechanizmusok kerülnek beépítésre, azok valóban alkalmasak-e betölteni szerepüket.
3. Ezt követően a kockázatok felmérése, azonosítása szükséges. Ennek keretében át kell tekinteni, hogy az azonosított kockázatok bekövetkezte, illetve az azok elhárítására alkalmazott eszközök milyen hatással járhatnak az érintettek jogaira.
4. Ezt követően az egyes hatások, eredmények valószínűségének rangsorát kell felállítani.
5. Az adatvédelmi hatásvizsgálat zárásaként pedig mérlegelni kell a hatásvizsgálati eljárás eredményességét, és szükség esetén ismételten el kell végezni azt.

A CNIL módszertan azt is megjegyzi, hogy az elkészült hatásvizsgálati eredményt, a részletes kockázatelemzést, illetve annak megállapításait az adatvédelmi hatóság erre irányuló kérésére át kell adni. A CNIL a GDPR adatvédelmi hatásvizsgálati követelményei alapján a fentieken túl nyilvánosságra hozta hatásvizsgálati szoftverét is, amely interaktív online eszközként segíti az adatkezelőket a hatásvizsgálatok elvégzésében.[202]

11.2. Az adatvédelmi hatásvizsgálat előnyei

A fent leírtak alapján a hatásvizsgálati eljárás módszertani lényege egyrészről egy projekt, vagy más egyéb szolgáltatás, esemény stb. magánszférára gyakorolt hatásainak felmérése, amennyiben az személyes adatok kezelését is magában foglalja, másrészről annak célja az adatkezelés során esetlegesen felmerülő negatív hatások elkerülése vagy csökkentése.[203]

A hatásvizsgálat nem csupán egy eszköz, hanem egy olyan eljárás, amelyet az adatkezelést integráló projekt legelején, annak megkezdését megelőzően célszerű elvégezni, elvégeztetni. A korai előkészületi szakaszban elvégzett hatásvizsgálat a tervezett projekt eredményességét is biztosíthatja. A hatásvizsgálati eljárást a projekt során, illetve annak befejezése után is célszerű bizonyos időközönként megismételni. Sőt, jó hatásvizsgálati gyakorlatnak tekinthető, ha magába a hatásvizsgálati eljárásba külső szereplők is bevonásra kerülnek, hiszen így az adatkezelők számára független ajánlások is segíthetnek a kockázatok kezelésében, csökkentésében.[204]

[200] Veres, 2017.
[201] CNIL, 2015.
[202] A CNIL adatvédelmi hatásvizsgálati szoftvere az alábbi hivatkozáson keresztül érhető el: https://www.cnil.fr/en/PIA-privacy-impact-assessment-en (utolsó letöltés: 2018. szeptember 10.)
[203] Veres, 2017.
[204] Wright – De Hert, 2012.

11.3. Az adatvédelmi hatásvizsgálat szabályozása a GDPR-ban

11.3.1. Az adatvédelmi hatásvizsgálat lefolytatásának szükségessége

Az Európai Unió működéséről szóló szerződés 288. cikke alapján a rendelet egy olyan jogalkotási aktus, amely az EU területén közvetlenül és teljes egészében alkalmazandó. A GDPR 99. cikk (2) bekezdése alapján azt 2018. május 25. napjától kell alkalmazni, mely teljes egészében kötelező és közvetlenül alkalmazandó az EU valamennyi tagállamában. Az adatvédelmi hatásvizsgálatnak a GDPR-ban lévő sajátosságait az alábbiakban tekintjük át.

A GDPR (75) – (77) preambulum bekezdései alapján az adatvédelmi hatásvizsgálat lényege a természetes személyek jogait és szabadságait érintő kockázatok feltárása és a kockázatok mérséklése érdekében a megfelelő intézkedések kidolgozása és átültetése.

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával. Az adatvédelmi hatásvizsgálatok az elszámoltathatóság szempontjából is jelentőséggel bírnak, ugyanis nemcsak az általános adatvédelmi rendelet előírásainak teljesítését könnyítik meg az adatkezelők számára, de a rendelet betartása érdekében hozott megfelelő intézkedések végrehajtásának bizonyítását is (lásd a 24. cikket). Az adatvédelmi hatásvizsgálat tehát a rendelet betartásának elérésére és bizonyítására szolgáló eljárás.[205]

A GDPR értelmében az adatvédelmi hatásvizsgálatra vonatkozó előírások be nem tartása esetén az illetékes felügyeleti hatóság bírságot szabhat ki. Amennyiben az adatkezelést kötelező adatvédelmi hatásvizsgálatnak alávetni, annak elmulasztása, helytelen elvégzése, vagy szükség esetén az illetékes felügyeleti hatósággal való egyeztetés elmulasztása közigazgatási bírsággal sújtható, amelynek összege legfeljebb tízmillió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-a. A kettő közül a magasabb összeget kell kiszabni.[206]

Az általános adatvédelmi rendeletben kifejezésre juttatott kockázatalapú megközelítéssel összhangban nem mindegyik adatkezelési művelet esetében kötelező adatvédelmi hatásvizsgálatot végezni. Csak akkor van szükség adatvédelmi hatásvizsgálatra, ha az adatkezelés *„valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”.* Ahogy a hivatkozott rendelkezésből is következik a kockázat azonosítása kulcskérdés, azaz hogy a GDPR alkalmazásában mit tekintünk kockázatnak. E tekintetben a GDPR preambulum bekezdései, valamint a 35. cikkben foglaltak adnak iránymutatást.

A GDPR (75) preambulum bekezdése rögzíti, hogy a természetes személyek jogait és szabadságait érintő kockázatok származhatnak a személyes adatok kezeléséből, amelyek eredménye lehet fizikai, vagyoni, nem vagyoni kár, hátrányos megkülönböztetés, személyazonosság lopás, vagy személyazonossággal való visszaélés, szakmai titoktartási kötelezettség által védett személyes adat bizalmas jellegének sérülése, az álnevesítés engedély nélküli feloldása, gazdasági vagy szociális hátrány. E körbe sorolandó az is, ha az érintettek nem gyakorolhatják jogaikat, vagy nem rendelkezhetnek saját személyes adataik felett, vagy olyan személyes adatok (a személyes adatok különleges kategóriái) kezelése történik, amely faji vagy etnikai származásra vagy politikai véleményre, vallási, illetve világnézeti meggyőződésre, szakszervezeti tagságra utalnak. Ugyancsak ide tartozik, ha az adatkezelés genetikai adatokra, egészségügyi adatokra, a szexuális életre, a büntetőjogi felelősség megállapítására vonatkozik. Végül, ha személyes jellemzők értékelésére, így a munkahelyi teljesítmény, gazdasági helyzet, egészségi állapot, személyes preferenciák, érdeklődési körök, megbízhatóság vagy viselke-

[205] WP29, 2017.
[206] WP29, 2017.

dés, tartózkodási hely vagy mozgás elemzésére és előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából.

A hatásvizsgálat előkészítésének következő kérdése, hogy miként elemezze az adatkezelő a konkrét esetben a kockázat súlyosságát, illetve valószínűségét. A rendelet maga ad néhány fogódzót erre az esetre: az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell megállapítani, hogy a kockázat valószínűsíthetően magas-e. Erre utalhat például új technológia alkalmazása is. Ezt követően a GDPR preambuluma olyan objektív értékelésre utal, amelynek részletei a normaszövegben már nem találhatók meg. Itt nyilvánvaló szerepe lesz az olyan iránymutatásoknak, amelyek az adatvédelmi hatóságoktól, illetve az Európai Adatvédelmi Testülettől (Testület) várhatók.[207]

A kockázatok azonosítását követően a kockázatok mérséklésére irányuló intézkedések számbavétele az adatkezelő feladata. Itt a rendelet ismét csak utal bizonyos támpontokra, így bevált gyakorlatokra, amelyek például jóváhagyott magatartási kódexekben lelhetők fel, továbbá a tanúsítási eljárásokra, a Testület iránymutatásaira, valamint az adatvédelmi tisztviselő által házon belül nyújtott iránymutatásokra. A rendelet a kockázatok mérséklésére irányuló intézkedések között több helyen is említi az adatok álnevesítését, mint lehetséges intézkedést. A jogbiztonság terén nem csupán az azonosított magas kockázatokra, és ezek mérséklésére vonatkozó iránymutatások fognak fontos szerepet játszani, hanem azok a dokumentumok is, amelyek a valószínűsíthetően magas kockázattal nem járó adatkezelési műveleteket mutatják be. A Testület például meghatározhatja, hogy melyek ezek, és azt is, hogy mely intézkedések elegendők a kockázatok mérséklésére.[208]

A GDPR (90)-(91) bekezdései rögzítik, hogy a hatásvizsgálat magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, valamint a rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat. Ez különösen vonatkozik egyrészt azokra a nagymértékű adatkezelési műveletekre, amelyek jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelését célozzák, és amelyek az érintettek jelentős számára hatással lehet, és amelyek például az adatok érzékenysége folytán valószínűsíthetően magas kockázattal járnak. Másrészt azokra az adatkezelési műveletekre, amelyeknél nagy arányban a technológia elismert állásának megfelelő új technológiát alkalmaznak. Ezen felül olyan más adatkezelési műveletekre is vonatkozik, amelyek magas kockázattal járnak az érintettek jogaira és szabadságaira nézve, abból a szempontból, ha az említett műveletek megnehezítik az érintettek számára, hogy a jogaikat gyakorolják.

Adatvédelmi hatásvizsgálatot kell végezni továbbá, amikor az a személyes adatkezelés célja, hogy konkrét természetes személyekkel kapcsolatban döntést lehessen hozni azt követően, hogy elvégzik a természetes személyek személyes jellemzőinek szisztematikus és kiterjedt értékelését az adatokon alapuló profilalkotás alapján. Ez vonatkozik a személyes adatok különleges kategóriáira, a biometrikus adatokra, a büntetőjogi felelősség megállapítására és a bűncselekményekre vagy a kapcsolódó biztonsági intézkedésekre vonatkozó adatok kezelését követően. Az adatvédelmi hatásvizsgálatok elvégzése a nyilvános helyek nagymértékű megfigyelése esetében szintén követelmény, különösen, ha ezt elektronikus optikai eszközök alkalmazásával hajtják végre. Ezen felül olyan egyéb műveletek esetében is, amelyeknél az illetékes felügyeleti hatóság úgy ítéli meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, különösen mivel megakadályozza, hogy az érintettek a jogaikat gyakorolják, vagy szolgáltatásokat vegyenek igénybe, vagy szerződést érvényesítsenek, vagy mivel az említett műveletekre szisztematikusan és nagy számban kerül sor.

A GDPR fenti preambulumbekezdései explicite kimondják egyfajta értelmezésként azonban, hogy a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szak-

[207] Az új adatvédelmi rendelet szerint az EGT adatvédelmi hatóságait az Európai Bizottság tanácsadó szerveként működő, az irányelv 29. cikke alapján létrehozott Munkacsoportot felváltja a Bizottságtól független, nem csupán tanácsadó, hanem döntéshozatali jogosultságokkal is felruházott Európai Adatvédelmi Testület.

[208] Szabó, 2016.

orvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik. Ilyen esetekben az adatvédelmi hatásvizsgálatot nem kell kötelezővé tenni.

A GDPR továbbá azt is kimondja a (92) preambulumbekezdésben, hogy bizonyos körülmények között észszerűnek és gazdaságosnak bizonyulhat az adatvédelmi hatásvizsgálat nem egyetlen projekt tekintetében történő lefolytatása, például ha közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek közös alkalmazást vagy adatkezelési felületet kívánnak létrehozni. Szintén ilyen körülmény lehet, ha több adatkezelő közös alkalmazást vagy adatkezelési környezetet kíván bevezetni valamely ágazat vagy szegmens, vagy valamely széles körben végzett horizontális tevékenység tekintetében.

A GDPR 35. cikk (3) bekezdése egy példálózó felsorolást tartalmaz, melyben külön nevesítésre kerülnek azok az esetek, ahol az adatvédelmi hatásvizsgálatot mindenképpen el kell végezni. Ezek a következők:

- a természetes személyekre vonatkozó egyes jellemzők módszeres és kiterjedt értékelése, amely automatizált adatkezelésen alapul, ideértve a profilalkotást is, és amely a természetes személy tekintetében jelentős jogi vagy hasonló következményekkel jár;
- ha a személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó személyes adatok nagy számban történő kezelése történik; vagy
- ha nyilvános helyek nagymértékű, módszeres megfigyelése történik.

A GDPR alapján tehát az adatkezelőnek kettős kötelezettsége keletkezik. Egyrészről meg kell vizsgálniuk, hogy egyáltalán jár-e kockázattal az adatkezelés, másrészről hogy szükséges-e az adatvédelmi hatásvizsgálat elvégzése.

A GDPR fent hivatkozott preambulum bekezdései és a 35. cikk (3) bekezdése tehát olyan konkrét eseteket sorol fel, ahol az adatkezelőnek nincs mérlegelési lehetősége, az adatvédelmi hatásvizsgálatot le kell folytatni.

A GDPR 35. cikk (11) bekezdése rögzíti azt is, hogy az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén köteles ismételten lefolytatni az ellenőrzést annak értékelése céljából, hogy a konkrét adatkezelés az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

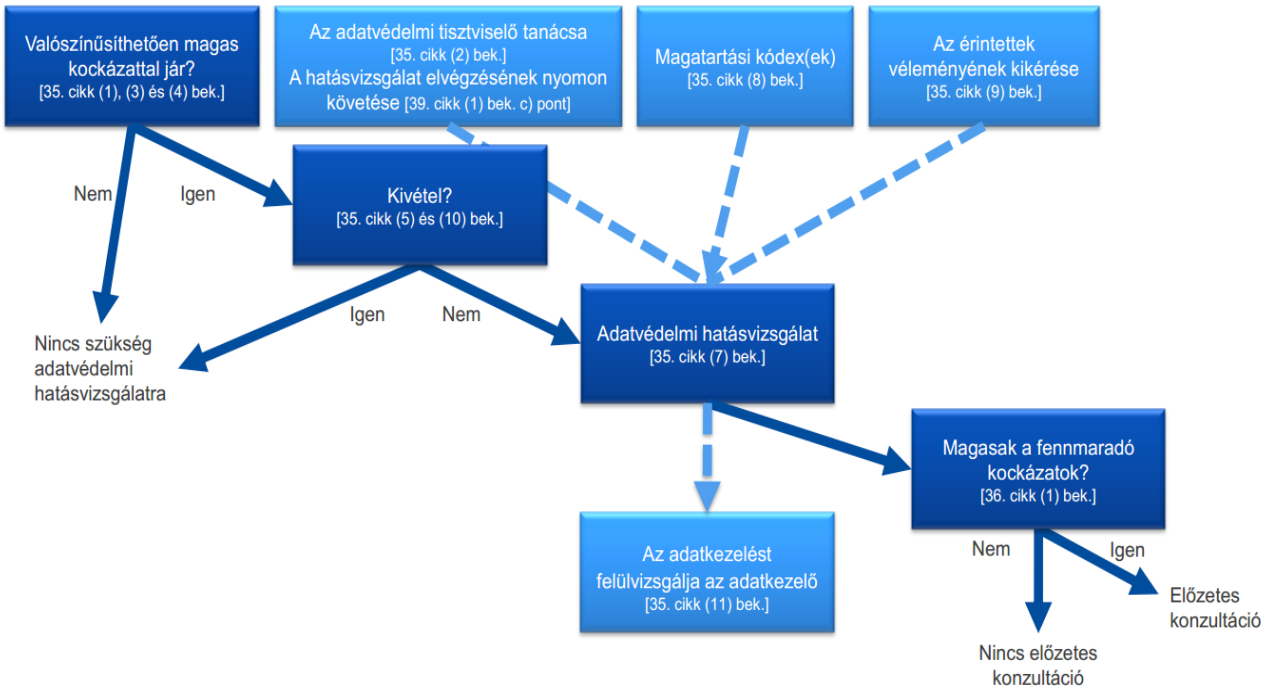
A GDPR a fentieken túl csak két iránymutatást nyújt az elvégzett adatvédelmi hatásvizsgálatok felülvizsgálata kapcsán: egyrészt szükség szerint kell elvégezni, másrészt legalább akkor, amikor a kockázat változik. Ez számos körülmény miatt bekövetkezhet, például megnő az érintettek száma, vagy bármilyen olyan új körülmény adódik, ami a kockázatokról szóló felsorolásban szereplő körülmények jelentős változásával járnak.[209]

A GDPR 35. cikk (10) bekezdése némi könnyebbséget jelenthet az adatkezelőknek a tekintetben, hogy abban az esetben, ha korábban egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot, akkor nem szükséges külön egy újabb adatvédelmi hatásvizsgálatot végezni.

Fontos kivételszabály a hatásvizsgálat lefolytatása alól, hogy abban az esetben, ha az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének c) és e) pontja szerint (az adatkezelés jogi kötelezettség teljesítése céljából, valamint közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásához szükséges) uniós vagy tagállami jog írja elő, akkor nem szükséges az adatvédelmi hatásvizsgálatot elvégezni. Ennek feltétele, hogy a jogalap elfogadása során, tehát a jogalkotási folyamatba építve egy általános hatásvizsgálat keretében már adatvédelmi vizsgálatot is végeztek. A tagállamok még ebben az esetben is rendelkezhetnek úgy, hogy az adatvédelmi hatásvizsgálatot az egyes adatkezelések megkezdése előtt el kell végezni.

Az alábbi ábra azt szemlélteti, hogy mely esetekben szükséges lefolytatni a GDPR alapján az adatvédelmi hatásvizsgálatot, illetve, hogy mely esetekben szükséges annak során konzultálni a tagállami felügyeleti hatósággal.[210]

[209] Szabó, 2016.
[210] WP29, 2017.



A felügyeleti hatósággal való előzetes konzultációról lásd bővebben a fejezet 4. pontjában írtakat.

11.3.2. Az adatvédelmi hatásvizsgálat kötelező lefolytatását előíró hatósági jegyzék

A GDPR gyakorlati alkalmazása során néhány esetben az adatkezelőknek komoly kihívás lehet a hatásvizsgálat szükségességének eldöntése. Ezt figyelembe véve az EU jogalkotó a GDPR 35. cikk (4) bekezdésében feladatként határozza meg a tagállami adatvédelmi hatóságok számára egy olyan jegyzék összeállítását, amely azon adatkezelési típusokat tartalmazza, amelyekre vonatkozóan mindenképpen el kell végezni az adatvédelmi hatásvizsgálatot.

A hatásvizsgálat hatékony alkalmazásának előfeltétele, hogy a hatóságok összehangolják tevékenységüket ezen a téren, ezért a rendelet előírja, hogy a jegyzékek elfogadását megelőzően az egységességi mechanizmus keretében egyeztessenek egymással.[211]

Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság hozza nyilvánosságra a honlapján azon adatkezelési típusok jegyzékét, amelyek esetén kötelező a hatásvizsgálati lefolytatása.

Megjegyzendő, hogy az előzetes adatvédelmi hatásvizsgálat elvégzésének követelménye adott esetben jelentős terhet jelent az adatkezelő szervezet számára. Ennek alapján a hatóságok csupán azokat az adatkezeléseket vonják ilyen kötelezettség alá a nyilvános jegyzékben, amelyek valóban olyan kockázatokat hordoznak, amelyek mérséklése nagy körültekintést és felkészültséget igényel.[212]

A GDPR 35. cikk (5) bekezdése pedig egy olyan jegyzék összeállítására biztosít lehetőséget, amely azon adatkezelési műveletek típusait tartalmazza, amelyre vonatkozóan nem kell adatvédelmi hatásvizsgálatot elvégezni. Ez utóbbi azonban csak lehetőség az adatvédelmi hatóságok számára.

[211] Szabó, 2016.
[212] Szabó, 2016.

11.3.3. Az adatvédelmi hatásvizsgálat lefolytatásával kapcsolatos követelmények

A GDPR 35. cikk (7) bekezdése tartalmazza, azokat a minimum követelményeket, amelyeket minden hatásvizsgálat lefolytatásakor figyelembe kell venni.

Első lépésként a tervezett adatkezelési műveleteket módszeresen le kell írni külön figyelmet fordítva az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket. Amennyiben az adatkezelés természete, forrásai vagy a kockázatok mértéke indokolja, adott esetben a GDPR 35. cikk (9) bekezdésében foglaltak szerint már ekkor célszerű lehet az adatkezelésben érintett személyeket bevonni a vizsgálatba.

Másodszor az adatkezelő az így begyűjtött információ birtokában már mérlegelni tudja az adatkezelés, illetve az egyes adatkezelési műveletek – az adatkezelési célra, valamint az érintettek jogait és szabadságait érintő kockázatokra figyelemmel – szükségességét, arányosságát.[213]

Végezetül az adatkezelőnek be kell mutatni a hatásvizsgálat során azokat a kockázatok kezelését célzó intézkedéseket, amelyek a személyes adatok védelmét hivatottak megfelelő módon biztosítani.[214]

Az adatkezelő ennek az utóbbi követelménynek akár úgy is eleget tehet, ha egy konkrét példán keresztül ismerteti például az a GDPR 33. és 34. cikkei szerinti adatvédelmi incidens bekövetkezte esetén alkalmazott folyamatot, azaz hogyan, milyen módon, mely esetekben értesíti az adatvédelmi hatóságot, illetve az érintett személyeket.[215]

Továbbá a GDPR 35. cikk (8) bekezdése nevesíti, hogy az adatkezelők, illetve adatfeldolgozók által végzett adatkezelési műveletek hatásainak értékelése figyelembe kell venni a GDPR 40. cikke szerinti magatartási kódexekben és a GDPR 42. cikke szerinti tanúsítási mechanizmusokba foglaltakat.

A GDPR nem szabályozza az adatvédelmi hatásvizsgálati dokumentáció, illetve a vizsgálati eredmények nyilvánosságának kérdését. A rendelet 36. cikk (1) bekezdése csak annyit rögzít, hogy amennyiben az adatvédelmi hatásvizsgálat alá vont adatkezelés valószínűsíthetően magas kockázattal jár, úgy az adatkezelő konzultálni köteles az adatvédelmi hatósággal. Valamint, a GDPR 36. cikk (3) bekezdés e) pontja értelmében az adatkezelő tájékoztatni köteles az adatvédelmi hatóságot a lefolytatott adatvédelmi hatásvizsgálatról (lásd bővebben: jelen fejezet 4. pontját).

11.3.4. A GDPR-ban szabályozott adatvédelmi hatásvizsgálat szakaszai

A vonatkozó szakirodalom a hatásvizsgálati eljárás alábbi három főbb szakaszát különbözteti meg:[216]

1. előkészületi szakasz;
2. hatásvizsgálati elemzés;
3. a személyes adatok védelmét szolgáló biztonsági intézkedések alkalmazása.

Az első, vagyis az *előkészületi szakasz* során az adatkezelőnek elsőként azt kell megállapítania, hogy egyáltalán szükséges-e lefolytatni az adatvédelmi hatásvizsgálatot. Ennek eldöntéséhez a már fentebb említett GDPR 35. cikk (1) bekezdésében foglaltak az irányadók, azaz, ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Abban az esetben, ha az adatvédelmi hatásvizsgálatot le kell folytatni, akkor először annak célját, valamint a vizsgálat terjedelmét kell megállapítani. E körben ugyancsak fontos, hogy az a személy,

213 GDPR 35. cikk (7) bekezdés b) – c) pontok.
214 GDPR 35. cikk (7) bekezdés d) pont.
215 Veres, 2017.
216 Bieker et. al., 2016.

amely/aki a hatásvizsgálati eljárás lefolytatására kerül kijelölésre, az megfelelő szakértelemmel és forrással rendelkezzen annak lefolytatásához.

A hatásvizsgálatot lefolytató személy kijelölése, a hatásvizsgálati célkitűzések és a terjedelmi határok kijelölését követően fel kell állítani azt az adatvédelmi hatásvizsgálati modellt, azaz azt a vizsgálati tervet, amely alapján lefolytatására kerül a vizsgálat. Ennek lefektetéséhez ajánlott az európai jogalkotó által közzétett DPIA mintákat is figyelembe venni, hiszen így az adatkezelő adott esetben könnyebben alá tudja támasztani a konkrét adatkezelés adatvédelmi szabályoknak való megfelelését.[217]

A vizsgálat céljainak meghatározásához mindenképp szükséges, hogy az adatkezelő tisztában legyen a teljes adatkezeléssel. E körben az adatkezelőnek részletesen ismertetnie kell annak jellegét, hatókörét, körülményeit és céljait, ideértve az egyes adatkezelési műveletek terjedelmét, a személyes adatok tárolásának módját, megőrzési idejét stb. Ahogy azt a GDPR 35. cikke is tartalmazza e körben nem elegendő az adatkezelés egy-egy műveletét leírni, a hatásvizsgálatnak valamennyi adatkezelési műveletre ki kell terjednie, az adatkezelőnek ismertetnie kell mindazon technikai és szervezeti intézkedést, folyamatot, amelyet a személyes adatok védelme érdekében alkalmazni kíván. Ennek során figyelemmel kell lenni a rendeletben lefektetett adatvédelmi elvekre is, így különösen a jogszerűség, tisztességes eljárás és átláthatóság elvére, az adattakarékosság elvére, a célhoz kötöttség elvére.

A második szakasz, azaz a *hatásvizsgálati elemzés* egy olyan módszer szerinti elemzés végrehajtását kívánja meg, amely az egyes adatvédelmi célkitűzésekre figyelemmel alkalmas az egyes kockázatok kezelésére használt intézkedés és biztonsági mechanizmusok megfogalmazására. E körben hangsúlyozandó, hogy az általános kockázatelemzéshez képest a hatásvizsgálat során nem csak a szervezeten kívüli harmadik személyeket, potenciális támadókat kell számba venni, hanem a szervezeten belüli azon elemeket is, amelyek az érintettek jogaira és szabadságaira nézve jelentenek kockázatot (például: munkavállalók, felhasználói, hozzáférési jogosultsággal rendelkező személyek stb.).[218]

A kockázatelemzés során azt is vizsgálni kell az egyes kockázatok bekövetkeztére mekkora esély van, illetve, hogy a tervezett biztonsági intézkedések valóban hatékonyan tudják kezelni a kockázatokat. A fentiek elemzésekor mindvégig figyelemmel kell lenni a GDPR 37. cikk (7) bekezdés b) – c) pontjaiban írt szükségesség-arányosság elvére is.

A harmadik szakasz, azaz a *személyes adatok védelmét szolgáló biztonsági intézkedések alkalmazásának szakasza* során el kell készíteni az úgynevezett kockázatkezelési tervet. A GDPR 35. cikk (7) bekezdés d) pontja szerint e tervnek ki kell terjednie a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a GDPR-ral való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

A fentieknek megfelelően a kockázatkezelési tervnek részletesen tartalmazni kell:

(i) azon intézkedéseket, illetve mechanizmusokat, amelyek az érintettek jogaira és szabadságaira kockázatot jelentő elemeket megszüntetni vagy csökkenteni képesek;
(ii) a biztonsági intézkedéseket, illetve mechanizmusokat alkalmazó személy, illetve az a személy, akivel szükség estén konzultálni lehet;
(iii) az az időpont, amikorra a biztonsági intézkedéseket és mechanizmusokat átültetik az ahhoz kapcsolódóan elérhető források megjelölésével;
(iv) a biztonsági intézkedések és mechanizmusok eredményeinek elemzéséhez szükséges szempontok; és
(v) az a személy, aki jogosult a biztonsági intézkedések, mechanizmusok elemzésére, értékelésére.[219]

[217] Veres, 2017.
[218] Veres, 2017.
[219] Veres, 2017.

Annak érdekében, hogy a DPIA kívánt céljai megvalósuljanak, elengedhetetlen egy a fenti elemzések eredményeit összefoglaló dokumentáció elkészítése, illetve annak hozzáférhetővé tétele. E körben az adatkezelőknek célszerű lehet egy rövidebb összefoglalót is összeállítaniuk az elkészült dokumentáció alapján, amelyet az adatvédelmi hatóság erre irányuló kérésére, illetve a nyilvánosság számára is hozzáférhetővé lehet tenni. Ezzel az adatkezelők ugyancsak képesek lesznek az adatvédelmi szabályoknak való megfelelésüket alátámasztani.[220]

A GDPR is előírja a fentieken túl az elvégzett adatvédelmi hatásvizsgálat meghatározott esetekben történő (újbóli) ellenőrzését. A GDPR 35. cikk (11) bekezdése rögzíti, hogy az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e. Ilyen kockázat lehet az adatkezelő szervezetében bekövetkezett változás, vagy általában egy újabb adatbiztonsági kockázat (például: számítógépes vírus) megjelenése, de akár a jogi szabályozásban bekövetkezett változás is szükségessé teheti az ellenőrzés lefolytatását, és szükség szerint új biztonsági intézkedés, mechanizmus beépítését és alkalmazását.[221]

Összefoglalva a GDPR-ban szabályozott adatvédelmi hatásvizsgálat egyfajta korai „jelzőrendszernek" is tekinthető, amely lehetővé teszi az adatkezelő számára, hogy az adatkezelése során felmerülő a természetes személyek jogait és szabadságait érintő kockázatokat, illetve azok hatásait előre felmérje, s így megfelelő adatvédelmi, adatbiztonsági intézkedéseket dolgozzon ki azok kezelésére. Ez pedig a várakozások szerint egy hatékonyabb döntési folyamatot is lehetővé fog tenni, amely így alkalmas lehet az adatkezelő és az érintettek, illetve az adatkezelő és az adatvédelmi hatóság közötti bizalom erősítésére is. A bizalom erősítése mellett ugyancsak érdemes megjegyezni, hogy egy standardizált formában lefolytatott adatvédelmi hatásvizsgálat az adatkezelő és az adatvédelmi hatóságok számára is lehetővé teszi az adatkezelés könnyebb átláthatóságát, amely az adatkezelés gyenge pontjainak, illetve az esetleges szabálytalanságok, jogsértések azonosítását is könnyebbé teheti.[222]

11.4. A 29-es Adatvédelmi Munkacsoport iránymutatásában a kötelező hatásvizsgálattal kapcsolatban kiemelt esetek

A GDPR-ban foglalt adatvédelmi hatásvizsgálattal kapcsolatos rendelkezések értelmezése körében a 29-es cikk szerint Adatvédelmi Munkacsoport (a továbbiakban WP29 Munkacsoport) közzétett egy iránymutatást, amely általánosságban foglalkozik az adatvédelmi hatásvizsgálattal, illetve annak megállapításához nyújt segítséget az adatkezelőknek és adatfeldolgozóknak, hogy az általuk végzett adatkezelési vagy adatfeldolgozási művelet valószínűsíthetően magas kockázattal jár-e (a továbbiakban: WP 248 Iránymutatás).

A Munkacsoport az iránymutatásban az adatkezelők számára az eredendően magas kockázatuk miatt kötelező adatvédelmi hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének meghatározása érdekében a következő kilenc szempontot ismertette:[223]:

- Értékelési vagy pontozási rendszer használata, ideértve a profilozást és az előrejelzést is: Ilyen lehet, ha az adatkezelő különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján pontozza, profilozza az érintetteket. Erre példaként említhető a pénzügyi vállalkozás,

220 Veres, 2017.
221 Veres, 2017.
222 Veres, 2017.
223 WP29, 2017.

amely hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázist használ ügyfelei szűrésére, vagy a biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje, és előre jelezze a betegségek kockázatát és az egészségügyi kockázatokat.

- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: Olyan adatkezelés, amelynek célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala. Az adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti. A körben további felvilágosítást nyújt az Adatvédelmi Munkacsoport profilalkotásról szóló iránymutatása is.[224]
- Módszeres megfigyelés: Az érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés (jellemzően közterületeken vagy nyilvános helyeken történő megfigyelés például: bevásárlóközpont, nyilvános könyvtár).
- Különleges adatok vagy fokozottan személyes jellegű adatok kezelése: Ide sorolhatóak a GDPR 9. cikke szerinti különleges adatok, a 10. cikkben meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok. A GDPR e rendelkezésein túlmenően bizonyos más adatkategóriák is tekinthetőek úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat. Ilyenek például az olyan személyes adatok, amelyek kezelése kihat valamely alapvető jog gyakorlására, vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére. E tekintetben lényeges lehet, hogy az érintett vagy valamely harmadik személy már nyilvánosan hozzáférhetővé tette-e az adatokat. A személyes adatok nyilvános hozzáférhetősége az értékelés során egyik tényezőként figyelembe vehető, ha az adatok bizonyos célú további felhasználására lehet számítani.
- Nagy számban kezelt adatok: Az Adatvédelmi Munkacsoport ajánlása szerint ennek megállapításakor az alábbi tényezőket kell figyelembe venni: az érintettek száma konkrét számadatként vagy a lakosság arányában; a kezelt adatok mennyisége vagy adatfajták köre; az adatkezelési tevékenység időtartama vagy állandó jellege; az adatkezelési tevékenység földrajzi kiterjedése.
- Adatkészletek egymással való megfeleltetése vagy összevonása: Például kettő vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon.
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok: Például gyermekek, munkavállalók, idősek, mentális betegségben szenvedők adatai.
- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: Az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében; továbbá bizonyos, a „dolgok internetét" használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését. Az ilyen technológiák használatához újfajta adatgyűjtési és felhasználási formák kapcsolódhatnak, amelyek magas kockázattal járhatnak az egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek.
- Azok az esetek, amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek (Rendelet 22. cikk és (91) preambulumbekezdés): Erre példa, ha egy bank hitelreferencia-adatbázis alapján szűri ügyfeleit annak érdekében, hogy eldöntse, kínál-e nekik hitelt.

[224] A profilalkotásról szóló iránymutatás teljes angol nyelvű szövege az alábbi linken keresztül érhető el: http://naih.hu/files/Guidelines-on-Automated-individual-decision-making-and-profiling.pdf (utolsó letöltés: 2018. szeptember 10.).

A hatásvizsgálat folyamatosan ismétlődő jellegét a Munkacsoport kihangsúlyozta, így az adatkezelőknek a gyakorlatban valószínűleg a vizsgálat mindegyik szakaszát többször el kell végezniük a hatásvizsgálat lezárulta előtt. Azt követően is javasolt minden évben az ismétlése – az adatkezelések meghatározása, az intézkedések és kockázatok meghatározása körében például – és minden egyes jelentősebb változás bekövetkezésekor is indokolt a hatásvizsgálat felülvizsgálata.

A 248-as számú Iránymutatás 2. számú mellékletében az Uniós adatvédelmi hatóságok közös szempontrendszert dolgoztak ki annak érdekében, hogy az adatkezelők választani tudjanak a különböző adatvédelmi hatásvizsgálati módszertanok között. Az Adatvédelmi Munkacsoport álláspontja szerint az adatkezelő választja ki a módszertant, a kiválasztott módszereknek azonban meg kell felelnie az Iránymutatás 2. mellékletében megadott szempontoknak. Az adatvédelmi Munkacsoport ágazat specifikus adatvédelmi hatásvizsgálati keretek kidolgozását szorgalmazza, a keretek ezáltal az egyedi ágazati ismeretekre épülhetnek, így az adatvédelmi hatásvizsgálatok az adott jellegű adatkezelési művelet sajátosságaira összpontosíthatnak. Ennek keretében az adatvédelmi hatásvizsgálatok az adott gazdasági ágazatban, illetve bizonyos technológiák használatakor vagy meghatározott jellegű adatkezelési műveletek végrehajtásakor felmerülő kérdésekkel foglalkozhatnak.

A fentiekből adódóan a magasabb szintű megfelelés érdekében olyan módszertan kiválasztása javasolt, amelyet az adott adatvédelmi hatóság már összhangba hozott a rendelet rendelkezéseivel. Ilyen például a francia adatvédelmi hatóság (CNIL) módszertana, amely alkalmazását tovább erősíti az a tény, hogy a CNIL közzétett egy nyílt forráskódú szoftvert, amellyel az adatkezelők könnyen elkészíthetik a módszertannak megfelelő adatvédelmi hatásvizsgálatot. Az adatkezelőnek sem bejelentési, sem nyilvántartásba vételi kötelezettsége nincs. Saját döntése alapján nyilvánosságra hozhatja a hatásvizsgálat eredményét, akár egy összefoglaló formájában is, üzleti titkainak, adatbiztonságának feltárása nélkül.

Az iránymutatás kiemeli, hogy amely adatkezelőnél van kijelölt adatvédelmi tisztviselő, ott fontos szerepe van a hatásvizsgálat elvégzésében és a tanácsát is ki kell kérni.

11.5. Előzetes konzultáció a felügyeleti hatósággal

A GDPR bizonyos esetekben az adatvédelmi hatásvizsgálat lefolytatásával kapcsolatban kötelezően előírja az előzetes konzultációt az adott tagállam adatvédelmi hatóságával.

A GDPR (94) preambulumbekezdése alapján, ha az adatvédelmi hatásvizsgálat azt jelzi, hogy a kockázat mérséklését célzó garanciák, biztonsági intézkedések és mechanizmusok hiányában az adatkezelés magas kockázattal járna a természetes személyek jogaira és szabadságaira nézve, és az adatkezelő véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell. Ezt az előírást a GDPR 36. cikk (1) bekezdése is megismétli.

Az adatvédelmi hatásvizsgálat eredményéről a fentiek alapján tehát előzetesen konzultálni kell a felügyeleti hatósággal, ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére (tehát a fennmaradó kockázatok továbbra is jelentősek). Az elfogadhatatlanul magas fennmaradó kockázatra példa, ha az érintettek olyan jelentős vagy akár visszafordíthatatlan következményekkel szembesülnek, amelyeket nem tudnak leküzdeni (például: adatokhoz való jogosulatlan hozzáférés, amely az érintettek életét fenyegető veszélyt vagy pénzügyi nehézséget eredményez).

Ha a felügyeleti hatóság véleménye szerint a tervezett adatkezelés megsértené a GDPR előírásait – különösen, ha az adatkezelő a kockázatot nem elégséges módon azonosította vagy csökkentette –, a

felügyeleti hatóság az adatkezelőnek (és adott esetben az adatfeldolgozónak) legkésőbb a konzultáció iránti megkeresés kézhezvételétől számított nyolc héten belül írásban tanácsot ad, továbbá gyakorolhatja a GDPR 58. cikkében említett hatásköreit. A nyolc hetes alaphatáridő – a tervezett adatkezelés összetettségétől függően – hat héttel meghosszabbítható. A felügyeleti hatóság a megkeresés kézhezvételétől számított egy hónapon belül tájékoztatja az adatkezelőt (vagy adott esetben az adatfeldolgozót) a meghosszabbításról és a késedelem okairól. Az említett időtartamok felfüggeszthetők arra az időtartamra, amíg a felügyeleti hatóság nem jut hozzá azokhoz az információkhoz, amelyeket adott esetben a konzultáció céljából kért.

Ha a felügyeleti hatóság az említett határidőn belül nem reagál, az nem érinti a felügyeleti hatóságnak az a rendeletben megállapított feladataival és hatásköreivel összhangban álló beavatkozási jogkörét, az adatkezelési műveletek megtiltására vonatkozó hatáskörét is beleértve.

Az adatkezelő a felügyeleti hatósággal folytatott előzetes konzultáció során a felügyeleti hatóságot az alábbiakról köteles tájékoztatni:

a.) adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;
b.) a tervezett adatkezelés céljairól és módjairól;
c.) az érintettek e rendelet értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;
d.) adott esetben, az adatvédelmi tisztviselő elérhetőségeiről;
e.) a 35. cikk szerinti adatvédelmi hatásvizsgálatról; valamint
f.) a felügyeleti hatóság által kért minden egyéb információról.

A GDPR az előzetes konzultációt egyébként kötelező teszi minden, a személyes adatok kezeléséhez kapcsolódó, a nemzeti parlament által elfogadandó jogalkotási intézkedésre – vagy ilyen jogalkotási intézkedésen alapuló szabályozási intézkedésre – irányuló javaslat előkészítése során. E főszabálytól eltérve a tagállami jog előírhatja, hogy az adatkezelők konzultáljanak a felügyeleti hatósággal, és szerezzék be a felügyeleti hatóság előzetes engedélyét akkor is, ha valamely közérdek alapján ellátandó feladat végrehajtásához kapcsolódóan kezelnek személyes adatokat, ideértve a személyes adatoknak a szociális védelemhez és a népegészségügyhöz kapcsolódó kezelését is.

A konzultációs eljárás során az adatkezelés tekintetében végzett adatvédelmi hatásvizsgálat eredményét, és különösen a természetes személyek jogait és szabadságait veszélyeztető kockázat mérséklésére szolgáló intézkedések tervezetét be lehet nyújtani a felügyeleti hatóságnak.

Az adatfeldolgozókra vonatkozó különös előírás továbbá a GDPR (95) preambulumbekezdése szerint, hogy – szükség esetén kérésre – segíteniük kell az adatkezelőt abban, hogy teljesüljenek az adatvédelmi hatásvizsgálatok elvégzéséből és a felügyeleti hatósággal folytatott előzetes konzultációból eredő kötelezettségek.

11.6. Ellenőrző kérdések

Mi tekinthető az adatvédelmi hatásvizsgálat előképének és hol (mely országokban) alakult az ki?

Mikor kötelező az adatkezelőnek lefolytatnia az adatvédelmi hatásvizsgálatot?

Mi a felügyeleti hatóság feladata a kötelezően lefolytatandó adatkezelésekkel kapcsolatban? Mit kell ezzel kapcsolatban nyilvánosságra hoznia?

Mi a GDPR-ban szabályozott adatvédelmi hatásvizsgálat három szakasza?

Mely esetekben kötelező konzultálni a felügyeleti hatósággal az adatkezelőnek az adatvédelmi hatásvizsgálat megkezdése előtt?

12. ADATVÉDELMI INCIDENS BEJELENTÉS

12.1. Bevezetés

A GDPR az európai adatvédelmi szabályozásba bevezette az adatvédelmi incidens bejelentésének rendszerét. A szabályozás definiálja az adatvédelmi incidens fogalmát, illetve bizonyos feltételek fennállása esetén az adatkezelő kötelezettségévé teszi annak bejelentését az illetékes felügyeleti hatóság számára, illetve az érintettek értesítését az adatvédelmi incidensről.

Adatvédelmi incidensekhez kapcsolódó adatkezelői kötelezettségek korábban is jelen voltak mind a hazai mind az uniós szabályozásban, illetve egyes uniós országokban már a GDPR-t megelőzően létezett általános és kötelező adatvédelmi incidens bejelentési kötelezettség (például Hollandia). Ugyanakkor egy ilyen széles körű és az adatkezelők valamennyi csoportját általánosan terhelő adatvédelmi incidens jelentés a legtöbb uniós tagállam, így Magyarország adatkezelői és adatfeldolgozói számára is újdonság.

Az információbiztonság területén az információbiztonsági incidensek azonosítása és kezelése, ideértve az ilyen incidensek nyilvántartását, jelentését, régóta használt sikeres gyakorlat. Ennek az eljárásrendnek az adatvédelmi rezsimbe történő beleillesztése számos jótékony hatással járhat. Azzal, hogy az incidensek egy részét a felügyeleti hatóság számára be kell jelenteni az adatkezelő akár az adott incidens kezeléséhez, akár a jövőre nézve hasznos segítséget kaphat az adatvédelmi hatóságtól, különösen az incidens adatvédelmi kockázati besorolásához, illetve annak eldöntéséhez, hogy az érintettet tájékoztatni kell-e az incidensről. Azzal, hogy az érintetteket bizonyos esetekben kell, más esetekben célszerű tájékoztatni, az incidens hatásainak csökkentésébe és kockázatainak a mérséklésébe az adatalany is tevőlegesen részt vehet.

Az adatvédelmi incidensek kezelésének a középpontjában az érintettek jogainak és szabadságainak, a magánszférájuknak és a személyes adataiknak a védelme áll. Ennek megfelelően az adatvédelmi incidensek bejelentésének a kötelezettségére is egy compliance eszközként, illetve egy elszámoltathatósági mechanizmusként érdemes tekinteni.

12.2. Az adatvédelmi incidensek bejelentéséhez kapcsolódó alapelvek és alapfogalmak

Az adatvédelmi incidens bejelentési kötelezettség a GDPR által az adatvédelmi szabályozásban központi helyre emelt koncepció az elszámoltathatóság elve és kockázat alapú megközelítéshez kapcsolódik.

Az elszámoltathatóság elve alapján az adatkezelő felelős a személyes adatok kezelésére vonatkozó alapelveknek történő megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a GDPR-ral összhangban történik. Ezeket az intézkedéseket az

adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. A személyes adatok kezelésére vonatkozó alapelvek egyike az integritás és bizalmas jelleg elve, amely alapján a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az említett fogalmi elemek jól ismert információbiztonsági megjelöléseket jelölnek. A személyes adatok elvesztéséről akkor beszélhetünk, ha a személyes adat továbbra is létezik, de az adatkezelő nem fér hozzá, nincs a birtokában. A személyes adat megsemmisítése azt jelenti, hogy a személyes adat már nem létezik, legalábbis nincs meg olyan formátumban, amelyben az adatkezelő számára bármilyen módon felhasználható lenne. A személyes adatok károsodásáról pedig akkor beszélhetünk, ha az eredeti adatállományt megváltoztatták, az nem teljes vagy kompromittálódott.

Az adatvédelmi incidensek során ezeknek a fogalmaknak az ismerete és elhatárolása jelentőséggel bír, hiszen az incidensek vizsgálatában, kockázati besorolásában szerepet játszanak. Például egy vírustámadás esetén, ha a vírus többször felülírva törölte a fájlt, akkor az adat megsemmisült, de ha titkosította, akkor az adat elveszett, ha a vírus a fájlt megváltoztatta, akkor a személyes adat károsodott.

A másik, fentebb már említett koncepció, amely a GDPR szabályozásában központi helyre került a kockázat alapú megközelítés. A GDPR egy adatvédelmi incidens kezelésénél azt várja el az adatkezelőtől, hogy megtegye a megfelelő technikai és szervezési intézkedéseket, amelyeket a GDPR az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével követeli meg. Ennek során az adatkezelőnek a tudomány és technológia állására, a végrehajtás kockázatára és a védelmet igénylő személyes adatok jellegével összefüggő költségekre is figyelemmel kell lennie.

Az adatvédelmi incidensekre történő felkészülés és reagálás során általános elvárás, hogy az adatkezelő megelőzni, azonosítani és kezelni tudja a felmerülő adatvédelmi incidenseket.

12.3. Az adatvédelmi incidens fogalma, besorolása és azonosítása

Természetesen, hogy az adatkezelő megfelelően tudja kezelni az esetlegesen felmerülő incidenseket, először is azonosítania kell tudnia azokat.

Adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

A fogalomból adódik, hogy a biztonság sérüléséből kell következnie az incidensnek, így nem adatvédelmi incidens, ha az adatkezelő normál működési körében, tudatosan kialakított és követett eljárásrend vezet a jogosulatlan hozzáféréshez vagy közléshez. Ugyancsak nem beszélhetünk adatvédelmi incidensről, ha a biztonság sérülése révén nem személyes adatot érint az incidens, hanem például egy know-how-hoz vagy egy személyes adatokat nem tartalmazó üzleti titokhoz jogosulatlanul férnek hozzá. Tehát nem minden adatvédelmi jogsértés adatvédelmi incidens, de minden adatvédelmi incidens adatvédelmi jogsértés. Illetve nem minden biztonsági incidens adatvédelmi incidens, de minden adatvédelmi incidens biztonsági incidens.

Az adatvédelmi incidens fogalmának nem szükséges eleme a rosszhiszemű, jogellenes magatartás, illetve az incidens következhet az adatkezelő vagy az adatkezelőn kívüli másik fél magatartásából is. Tehát nem csak hacker vagy vírustámadások nyomán alakulhat ki adatvédelmi incidens, hanem azzal is, ha az adatkezelő munkatársa véletlenül törli a személyes adatot.

Az információbiztonságban jól ismert fogalmakat használva az adatvédelmi incidenseket alapvetően három kategóriába sorolhatjuk. Egyrészről létezhet bizalmassági incidens, amely a személyes adatok véletlen vagy felhatalmazás nélküli közlését, illetve az ezekhez való hozzáférést jelenti. Másrészről sértetlenséggel kapcsolatos incidens, amely a személyes adatok véletlen vagy jogtalan megváltoztatását foglalja magába. Harmadrészről pedig megkülönböztethetünk hozzáférhetőséggel kapcsolatos incidens, amely a személyes adatok véletlen vagy jogtalan megsemmisítését vagy ezek elvesztését eredményezi. A körülményektől függően egy adatvédelmi incidens több kategóriába is besorolható, például egy zsarolóvírus, amely a személyes adatokat nem csak titkosítja, hanem le is másolja és elküldi egy távoli szerverre egyszerre bizalmassági és hozzáférhetőséggel kapcsolatos incidens.

A bizalmassággal és a sértetlenséggel kapcsolatos adatvédelmi incidensek megítélése többnyire egyértelmű, hiszen a hasonló információbiztonsági incidensekkel megegyezően ítélhető meg. Ugyanakkor a hozzáférhetőséggel kapcsolatos adatvédelmi incidensek bizonyos aspektusokban különböznek az ilyen besorolású információbiztonsági incidensektől. Természetesen amellett, hogy csak a személyes adatokhoz való hozzáférhetetlenségre vonatkoznak, másik fontos elem, hogy csak a biztonság, azaz a security sérüléséből (például ransomware támadás) adódhatnak, így az ilyen megítélésű safety incidensek (például árvíz okozta szolgáltatáskiesés) nem tartoznak ide. Továbbá az ilyen jellegű incidensek besorolásánál kiemelt fontosságú szempont az idő tényező. Ha az adatok végleges megsemmisítéséről vagy elvesztéséről beszélünk, akár azáltal, hogy nem rendelkezünk a titkosított adat feloldásához szükséges kulccsal, akkor minden esetben adatvédelmi incidens következett be. Ugyanakkor eldöntendő kérdés, hogy az adatok átmeneti elvesztése, törlése adatvédelmi incidensnek tekinthető-e. Ennek megítéléséhez a GDPR 32. cikkéből érdemes kiindulnunk, amely értelmében az adatkezelő és az adatfeldolgozó megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét; továbbá a fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani. Ebből következően az időszakos hozzáférhetőséggel kapcsolatos személyes adatokat érintő incidensek, tehát többnyire a rendelkezésre állást érintő események is a biztonság sérüléseinek, így adatvédelmi incidenseknek tekintendő. Ennek megfelelően arról nyilvántartást kell vezetni, ugyanakkor az eset körülményeiből adódóan a felügyeleti hatóság felé történő bejelentés vagy az érintettek értesítése nem mindig szükséges ezekben az esetekben. Ez utóbbi eldöntése a később részletezett kockázatelemzéstől függ, amelyben az adatkezelő felméri, milyen hatást gyakorol az incidens az érintettek jogaira és szabadságaira nézve. Például, ha emberi hibából törlődik egy magánegészségügyi intézmény betegadatokat tartalmazó adatbázisa és a papír alapú nyilvántartásról történő helyreállás heteket vesz igénybe, amely következtében több műtéti beavatkozást is el kell halasztani, akkor az incidens az érintettek jogaira jelentős hatást gyakorolt, kockázattal járt. De például, ha egy hírlevél küldő szolgáltatónál a rossz beállítások miatt törlődnek az éles adatbázisból az e-mail címek, amelyet néhány napot követően helyreállítanak, de ezalatt az érintettek nem kapják meg a direkt marketing üzeneteket, akkor az érintettek jogaira és szabadságaira az incidens nem gyakorolt szignifikáns hatást, nem járt kockázattal. Ugyanakkor, amint fentebb említettük, egy incidens egyszerre több kategóriába is sorolható, így ha az utóbbi példában a hírlevélküldő szolgáltatás az e-mail címekhez egy zsarolóvírus támadás miatt nem fér hozzá pár napig, de a zsaroló vírus nem csak titkosította (hozzáférhetőséggel kapcsolatos incidens), hanem lemásolta és egy távoli szerverre elküldte a címeket (bizalmassági incidens), akkor ez már kockázattal járhat az érintettek magánszférájára nézve.

Az adatvédelmi incidens és körülményeinek azonosítását követően az adatkezelő legfontosabb feladata azt eldönteni, hogy az adott incidens milyen kockázatot jelent az érintett természetes személyek jogaira és szabadságaira nézve. Egy incidens sokféle negatív hatással járhat az érintettek magánszférájára való tekintettel, ebből sorol fel példálózó jelleggel néhányat a GDPR (75) és (85)

preambulumbekezdése, amely szerint az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. A természetes személyek jogait és szabadságait érintő kockázatok jelenthetnek hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal való visszaélést, pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett.

A kockázatelemzést követően az adatkezelőt a GDPR 33-34. cikkei alapján három kötelezettség terheli. Egyrészről nyilvántartja az adatvédelmi incidenseket. Másrészről indokolatlan késedelem nélkül bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Harmadrészről, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az incidens azonosítását, hatásainak feltérképezését, nyilvántartás vezetését, a felügyeleti hatóság értesítését és az érintett tájékoztatását fontosságát külön kiemeli a GDPR (87) preambulum bekezdése, amely szerint meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani.

Ha az adatkezelő nem teljesíti a fent említett kötelezettségeit, akkor a felügyeleti hatóság gyakorolhatja a GDPR-ban meghatározott korrekciós hatásköreit, amely magába foglalja annak a lehetőségét is, hogy közigazgatási bírságot szab ki. A bírság mértéke legfeljebb 10 000 000 euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg; a kettő közül a magasabb összeget kell kiszabni.

12.4. Az adatvédelmi incidensről történő tudomásszerzés

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

A bejelentési kötelezettség tehát a tudomásszerzéstől és nem az incidens bekövetkezésétől jön létre. Tudomásszerzésnek az tekinthető, amikor az adatkezelő észszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet. Hangsúly azon van, hogy az adatkezelő azonnali vizsgálatot kezdeményezzen annak megállapítására, hogy történt-e adatvédelmi incidens, és ha igen, milyen intézkedések szükségesek. Ennek a megelőző vizsgálatnak a hossza és bonyolultsága az adott incidens körülményeitől függ. Egyes esetekben gyorsan meg lehet állapítani, hogy incidens történt. Például egy rossz

címzettnek kiküldött e-mail esetében, ha a címzett visszajelez, hogy az e-mailt mellépostázták, akkor azonnal ellenőrizhető az incidens ténye és körülményei. Más esetekben hosszabb vizsgálatra is szükség lehet. Például, ha egy újságíró keresi meg az adatkezelőt egy incidenssel kapcsolatosan, akkor egy rövid belső vizsgálatot le lehet folytatni, amely arra irányul, hogy az incidens valóban bekövetkezett-e. Ugyanígy kell eljárni, ha maga a hacker keresi meg az adatkezelőt, és kér váltságdíjat a személyes adatokért cserébe. Ha az incidenst maga az adatkezelő azonosítja, például egy programozási vagy beállítási hiba feltárásával, akkor is egy rövid belső vizsgálatban érdemes felderíteni, hogy az adott hiba okán adatvédelmi incidens is történt-e az információbiztonsági incidens mellett.

Az értesülésnek, illetve a belső vizsgálat megkezdésének időpontjában még nem kell úgy tekinteni, hogy az adatkezelőnek tudomása van az incidensről, ugyanakkor fontos azt kiemelni, hogy a belső vizsgálatot azonnal el kell kezdeni és 72 órán belül be kell fejezni, ha eddig az időpontig nem tudott az adatkezelő kellő bizonyosságot szerezni az incidensről, akkor érdemes vélelmezni az incidens bekövetkeztét és meg kell kezdeni az incidens bejelentését és kezelését.

12.5. Az adatvédelmi incidensek kezelése a belső szabályzatokban

A gyors és sikeres incidenskezelés egyik előfeltétele a megfelelő felkészültség. Nem elvárható sikeres reagálás az incidensre, ha azt megelőzően az adatkezelő nem tekintette át egy ilyen esemény forgatókönyveit és az erre adandó válasz lépéseit belső szabályzatban vagy belső eljárásrendben nem rögzítette. A belső szabályozásban érdemes előre meghatározni, milyen módszertan alapján, milyen szempontok figyelembevételével fog történni a kockázatok azonosítása. Az incidenst milyen infrastruktúrán és kik fogják vizsgálni, mikor kerül sor külső szakértők bevonására. Az incidens kezelés során hogyan történik a felső vezetés értesítése és bevonása az incidens kezelésébe, illetve az adatvédelmi tisztviselő hogyan válik az incidens kezelés központi koordinátorává. A belső szabályozás elsődleges célja, hogy az incidens kezelése gördülékenyen haladjon, a szabályzatok segítséget nyújthatnak az incidens kezelésében részt vevőknek, hogy megállapíthassák, milyen eljárásrendet kell követni, milyen lépéseket kell megtenni (például hogyan alakul a riadólánc), ki a felelős az adott eljárásért, ki és milyen intézkedésre jogosult. A felkészülés és a belső szabályozás egyik legfontosabb eleme az incidens kezelő csoport (incident response team) felállítása. A csoport tevékenységének és eljárásrendjének a szabályozása azért kiemelt jelentőségű, mert nem elvárható egy ad hoc, hirtelen felállított és felkészületlen csapattól, hogy sikeresen reagáljon egy incidensre. A csoportban érdemes incidens kezelésben érintett területek képviselőiből összeállítani, így helyet kaphatnak benne IT szakértők, jogászok, felső vezetők, HR munkatársak, ügyfélszolgálati munkatársak és az adatvédelmi tisztviselő. A csoportra vonatkozó belső szabályozásban definiálhatja az adatkezelő a csapat által elérendő célok meghatározását. Az adatkezelő képességeitől függően ez irányulhat csupán az incidens azonosítására, az incidens megfékezésére és jelentésére, az incidenshez kapcsolódó bizonyítékok dokumentálására, az incidenshez vezető okok feltárására és esetlegesen kijavítására, illetve akár a teljes incidens kivizsgálására. Ha a csoportban résztvevő munkatársakat előre meghatározta a belső eljárásrend, akkor az incidensek kezelésére felkészítő oktatás is könnyebben megszervezhető. A szabályozásban azonban érdemes ügyelni arra, hogy a csoport összetételének rugalmasnak kell maradnia, illetve dinamikusan skálázhatónak kell lennie, hogy a különböző súlyú és volumenű incidensekre reagálni tudjon. Természetesen az adatkezelő lehetőségeihez és az incidensek gyakoriságához mérten állandó jelleggel is üzemelhet incidens kezelő csoport.

Az incidens kezelések során a belső eljárásrend mellett a külső szereplőkkel történő kommunikációra is fel kell készülnie az adatkezelőnek. Az incidensek során ilyen kommunikációs elvárás az adatfeldolgozóval történő kommunikáció. A GDPR alapján – ahogyan ezt később látni fogjuk – az adatfeldolgozónak is kötelezettsége az incidens azonosítása és arról az adatkezelő értesítése, továbbá

az együttműködés az incidens kezelésében. További fontos kommunikáció a felügyeleti hatóság értesítése és az érintettek tájékoztatása.

12.6. Az adatfeldolgozó kötelezettségei az adatvédelmi incidens kezelésében

Bár az általános felelősség az adatvédelmi incidensek kezeléséért, bejelentéséért az adatkezelőt terheli, az esetek egy jelentős részében az adatfeldolgozónak is jelentős lehet a szerepe. Ez a GDPR szövegéből is következik, hiszen az adatfeldolgozásra irányuló szerződésben (vagy egyéb jogi aktusban) szabályozni kell, hogy az adatfeldolgozó hogyan segíti az adatkezelőt az adatvédelmi incidensekkel kapcsolatos kötelezettségeinek a teljesítésében; különös tekintettel a rendelkezésre álló információk átadásában. A GDPR 33. cikk (2) bekezdése ezt külön pontosítja, miszerint az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzést követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek. A GDPR pontos határidőt nem határoz meg, de a rendszertani elemzés alapján megállapítható, hogy az adatfeldolgozónak 72 órán belül kell az adatkezelőt értesítenie. Tekintettel arra, hogy az adatfeldolgozó az adatkezelő nevében kezeli a személyes adatokat, így az adatfeldolgozó tudomásszerzésével az adatkezelő is tudomást szerzett az incidensről és a 72 órás határidő számítása megkezdődik. Ennek megfelelően az adatfeldolgozónak olyan módon kell az adatkezelőt értesítenie, hogy az még teljesíteni tudja a 33-34. cikkből következő kötelezettségeit. Ha az adatfeldolgozó több adatkezelő számára is nyújt hasonló szolgáltatást és az incidens az adatfeldolgozó érdekkörében merült fel, akkor az adatfeldolgozónak valamennyi adatkezelőt külön-külön kell értesítenie. Az adatfeldolgozó az adatkezelő nevében is megteheti a legfontosabb kötelezettségeket (például bejelentheti az incidenst a felügyeleti hatóságnak, tájékoztathatja az érintetteket az incidensről), ha erre megfelelő felhatalmazással rendelkezik az adatkezelőtől. Megemlítendő ugyanakkor, hogy a GDPR alapján a jogi kötelezettség az adatkezelőt terheli, ennek megfelelően az adatfeldolgozó mulasztása az adatkezelőt fogja terhelni.

12.7. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Ebben a bejelentésben az adatkezelőnek vagy a nevében eljáró adatfeldolgozónak ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát. Közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit. Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket; továbbá az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az adatvédelmi incidens bejelentés célja, hogy a természetes személyeknek esetlegesen okozott fizikai, vagyoni vagy nem vagyoni károkat az adatvédelmi incidens megfelelő és kellő idejű kezelésével csökkentse. Ennek megfelelően megakadályozza a személyes adataik feletti rendelkezés

elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. A fenti bejelentésben említett, a GDPR-ban nem pontosan meghatározott fogalmakat, mint például az érintettek kategóriái, az incidenssel érintett adatok kategóriái stb., ennek fényében érdemes bejelenteni. Ezzel összekapcsolva a bejelentett adatokat az elvégzett kockázatelemzéssel, tehát az érintettek kategóriái lehetnek ügyfelek; az incidenssel érintett adatok kategóriái elérhetőségi, pénzügyi és bankszámla adatok; így ezek a bejelentett adatok egyértelműen hozzá kapcsolható olyan negatív kockázatokhoz, mint például személyazonossággal való visszaélés, pénzügyi veszteség stb.

A GDPR természetesen csak a minimálisan szolgáltatandó adatokat tartalmazza, az adatkezelő, ha rendelkezésére áll, több adatot is megadhat, hiszen ezzel az elszámoltathatóság kötelezettségének jobban megfelel. Emellett meg kell említeni, hogy természetesen az illetékes felügyeleti hatóság az incidens bejelentés alapján indított eljárása során további információkat kérhet az adatkezelőtől az incidenssel kapcsolatosan.

Magyarországon az illetékes felügyeleti hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság, amely az incidensek bejelentésére online és offline formanyomtatványt tart fenn. Ebben a Hatóság a fent említett adatokat bekéri, ha az adatkezelő megfelelően kitölti az adatlapot, akkor szolgáltatja a GDPR-ban előírt adatokat.

A hatósági formanyomtatvány kitöltése során az adatkezelő az alábbi információkat szolgáltathatja:

- bejelentő adatai;
- időpontok: az adatvédelmi incidens időpontja, az incidensről való tudomásszerzés időpontja;
- az incidens észlelésének módja;
- esetleges késedelmes tájékoztatás indokai;
- az adatvédelmi incidens jellege: például eszköz elvesztése vagy ellopása; informatikai rendszer feltörése; rosszindulatú számítógépes programok például zsarolóprogram;
- személyes adatok téves címzett részére történő elküldése stb.;
- az adatvédelmi incidenssel érintett személyes adatok (például azonosító adatok, pénzügyi adatok, különleges adatok);
- az adatvédelmi incidenssel érintett személyes adatok becsült száma; az érintettek kategóriái (például alkalmazottak, ügyfelek, kiskorúak stb.);
- az incidens előtt alkalmazott intézkedések;
- az incidens következményeinek a megjelölése (például bizalmas jelleg sérülése, integritás sérülése, rendelkezésre állás sérülése);
- az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények, valamint a valószínűsíthető következmények súlyossága;
- a megtett intézkedések, ideértve az érintettek tájékoztatását – annak időpontját, formáját, tartalmát, a tájékoztatott érintettek számát, esetlegesen a tájékoztatás hiányának indokait;
- az adatvédelmi incidens orvoslására tett intézkedések;
- egyéb bejelentések (például az EU felügyeleti hatóságok listája, amelyeket az adatvédelmi incidens érinthet).

Egy adatvédelmi incidens – különösen egy bonyolultabb kibertámadás esetén – kezelése és kivizsgálása során az adatkezelő általában nem rendelkezik valamennyi az incidensre vonatkozó adattal, így a bejelentésben sem tudja az összes adatot szolgáltatni. Ugyanakkor ez a tény nem akadályozhatja az adatkezelőt abban, hogy az incidenst – ha szükséges – 72 órán belül jelentse a felügyeleti hatóságnak. Ennek az ellentmondásnak a feloldására a GDPR önmagában is kínál lehetőséget, hiszen a GDPR 33. cikk (4) bekezdése értelmében, ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

Ennek megfelelően az adatkezelő az incidens további kivizsgálása során a tudomására jutott információkat később, folyamatosan megoszthatja a felügyeleti hatósággal.

A GDPR 33. cikk (1) bekezdése értelmében, ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. A szabályozás tehát megengedi az adatkezelő számára, hogy ha a bejelentésre rendelkezésre álló szűk határidőt elmulasztja, akkor kimentheti magát. A kimentési indokokról a szabályozás nem szól, de az incidens jelentés természetéből adódóan méltányolandó kimentő ok lehet, ha az adatkezelő azért nem tudta a bejelentést időben megtenni, mert az incidens megfékezésével, a kárenyhítéssel volt elfoglalva. Ha egy kibertámadás során például egy adatkezelő teljes infrastruktúrája használhatatlanná válik, akkor a GDPR-ból is kiolvasható elvárás, hogy az adatkezelőnek először a jogszerű működést kell helyreállítani, ennek keretében az érintetteket érő károkat kell enyhíteni és csak utána szükséges a felügyeleti hatóságot értesíteni.

A GDPR 33. cikk (1) bekezdése értelmében, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor az adatvédelmi incidenst nem kell bejelenteni a felügyeleti hatóságnak. Például, ha az adatkezelőtől a személyes adatok megfelelően erősen titkosított formában, álnevesítve kerültek ki és létezik biztonsági mentés, amelyből az adatok visszaállítható, akkor az incidens valószínűsíthetően nem hordoz kockázatot az érintett magánszférájára nézve.

12.8. Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és legalább közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit; ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket; ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintett számára nyújtott tájékoztatási kötelezettség feltétele magasabb, mint a felügyeleti hatóság számára történő bejelentés során, ugyanis az adatvédelmi incidensnek magas kockázattal kell járnia az érintett jogaira és szabadságaira nézve. Ugyanakkor, bár az esetek egy részében ugyan nem kell, de érdemes az érintettet az adatvédelmi incidensről tájékoztatni, hiszen ebben az esetben az érintett is bevonható az incidens kockázatainak a mérséklésébe, amely csökkenti az incidens általános kockázati értékét.

A tájékoztatást közvetlenül az érintettnek kell megküldeni, kivéve, ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A tájékoztatásnak egyedinek kell lennie, azaz csak az adatvédelmi incidenssel kapcsolatos információkat tartalmazhat, az nem vonható össze egyéb tájékoztatásokkal, nem történhet hírlevélben vagy frissítési információkkal együtt, hiszen ezekben az esetekben a tájékoztatás világosságához és közérthetőségéhez kétség férhet.

A tájékoztatás közérthetőségéhez hozzátartozik, amennyiben az elektronikus formában történik, akkor azt közismert formátumot használva kell megtenni, hogy az érintett is meg tudja nyitni a tájékoztatást. Továbbá, ha ez ismert, akkor a tájékoztatást az érintett anyanyelvén, vagy ennek hiányában az érintett által preferált nyelven kell megtenni.

A tájékoztatás során figyelemmel kell lenni arra, hogy az adatkezelő ne használja az incidensben esetleg érintett kommunikációs csatornákat addig, amíg annak biztonságáról meg nem bizonyosodott.

A tájékoztatást indokolatlan késedelem nélkül kell megtenni és a fent említett kötelező elemek mellett mindig érdemes az érintettet tájékoztatni arról, mit tehet az incidens hatásainak csökkentése érdekében. Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

a.) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket (mint például a titkosítás alkalmazásan), amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b.) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c.) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja valamelyik előbb említett feltétel teljesülését.

Fontos kiemelni, ha az adatkezelő, amellett döntött, hogy az érintetteket nem tájékoztatja az incidensről, vagy azért, mert az nem jár magas kockázattal, vagy azért, mert a fent említett feltételek valamelyike teljesül, akkor az adatkezelőnek az elszámoltathatóság alapelvéből következően ezt a döntését megfelelően dokumentálni és indokolni kell, illetve a felügyeleti hatóság kérésére az indokokat ismertetni szükséges.

12.9. A kockázatelemzés

A GDPR hármas kötelezettséget ró az adatkezelőkre az adatvédelmi incidensekkel kapcsolatosan. Egyrészről valamennyi adatvédelmi incidensről nyilvántartást kell vezetni. Másrészről azokat az incidenseket, amelyek valószínűsíthetően kockázattal járnak az érintettek jogaira és szabadságaira be kell jelenteni a felügyeleti hatóságnak. Harmadrészről pedig, ha az előbb említett kockázat szintje magas, akkor az érintetteket is tájékoztatni kell az incidensről.

Ebből következik, hogy az incidensről történő tudomásszerzést követően az adatkezelőnek nem csak az incidens kezelését kell megkezdeni, hanem az incidens okozta kockázatok besorolását. Ez két szempontból fontos, egyrészről a kockázat valószínűségének és súlyosságának a tudatában az adatkezelő hatékonyabban tudja kezelni, csökkenteni az incidens hatását; másrészről meg tudja állapítani, hogy bejelentési, illetve tájékoztatási kötelezettsége keletkezett-e.

Kockázatról akkor beszélhetünk, ha az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban

forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. A természetes személyek jogait és szabadságait érintő kockázatok jelenthetnek hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal való visszaélést, pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett.

A kockázatelemzésnek objektív ismérveken kell alapulnia, illetve figyelembe kell venni a kockázatnak az érintett magánszférájára gyakorolt hatásának valószínűségét és súlyosságát. A kockázatelemzés során az alábbi kritériumokat fontos mérlegelni:

- *Az incidens típusa:* Bizonyos esetekben az incidens kockázatainak súlyosságát növeli az incidens típusa, például, ha közvetlen egészségügyi beavatkozást nem érint, akkor az egészségügyi adatoknak jogosulatlan személyekkel történő megosztása súlyosabb kockázatokat jelent az érintett számára, mint az ilyen adatok véletlen törlése, főleg, ha az adatok az érintett segítségével egyébiránt visszaállítható.
- *A személyes adatok fajtája, érzékenysége és száma:* Természetesen az incidens kockázatelemzése során az egyik legfontosabb faktor az incidensben érintett személyes adatok érzékenységének a besorolása. Általánosságban kijelenthető, minél érzékenyebb adatokat érint az incidens annál kockázatosabb a besorolása, ugyanakkor fontos figyelembe venni, hogy nyilvános vagy könnyen megismerhető személyes adatokkal kombinálható-e az incidensben érintett adatkör, hiszen ez jelentősen növelheti az incidens súlyosságát. Ugyancsak fontos tényező a kockázat besorolásánál, ha az adatból vagy adatok kombinációjából személyiségprofil építhető vagy érzékeny következtetés vonható le. Például önmagában a vásárlók listájának a nyilvánosságra kerülése nem jelent kockázatot, de ha ez egy daganatos megbetegedések kezelésére szolgáló étrend-kiegészítő bolt vásárlóinak a listája, akkor az már magasabb kockázatot hordoz magában. Az incidensben érintett személyes adatok száma mint kockázatot befolyásoló tényező jelentősebb magyarázatot nem igényel. Fontos mindig esetről esetre vizsgálni a kockázatokat, de általánosságban kijelenthető, hogy minél több adatot és minél több fajtájú adatot érint az incidens, annál magasabb lehet a kockázati besorolása, hiszen annál pontosabb profil építhető az érintettről.
- *Az érintettek azonosíthatósága:* Egy fontos szempont a kockázat besorolás során, hogy az incidensben érintett személyes adatok felhasználásával mennyire egyszerű az érintettet azonosítani, illetve a személyes adatot mennyire könnyű párosítani egyéb adatokkal, amely folyamat az érintett azonosításához vezet. Ennek a faktornak a mérlegelése csak az incidens körülményeinek az ismeretében lehetséges, hiszen könnyen előfordulhat, hogy az incidensben érintett adatok felhasználásával minden egyéb erőfeszítés nélkül közvetlenül azonosítható az érintett, de az is megtörténhet, hogy az érintettek azonosítása csak komoly erőfeszítések árán lehetséges. A természetes személyek azonosítása direkt vagy indirekt módon is lehetséges, ennek megítélése során figyelembe kell venni, hogy az érintett adatokból milyen következtetések vonható le, illetve mennyire kapcsolható össze nyilvánosan megismerhető adatokkal. Titkosítás, illetve pszeudoanonimizálás használata jelentősen csökkentheti ennek a kockázatnak a valószínűségét.
- *Az incidensnek az érintettre gyakorolt negatív hatásainak a súlyossága:* Az incidensben érintett személyes adatok különböző fajtái jelentősen befolyásolhatják az incidensnek az érintettre gyakorolt hatását. Ha különleges adatok vagy kiszolgáltatott helyzetben lévő érintettekre vonatkozó adatok kerülnek nyilvánosságra az incidens során, akkor az mindenképpen jelentősebb hatást gyakorol az érintett jogaira és szabadságaira nézve, ezért az incidens kockázati besorolása magasabb. Ugyancsak növeli az incidens hatását, ha az incidens körülményeiből valószínűsíthető, hogy rosszindulatú külső támadás történt és a kikerült személyes adatokkal való visszaélés valószínűsége nagyon magas. Ugyanakkor a kockázat valószínűsége csökkenthető, ha az incidens során olyan harmadik személy ismerte meg a személyes adatokat,

amelynél az adatkezelő könnyen elérheti az incidens megfelelő kezeléséről. Például, ha emberi hiba miatt az adatkezelő egyik beszállítója ismeri meg a személyes adatokat, amely beszállítóval régóta szerződéses kapcsolatban van az adatkezelő és a szerződésben szabályozott módon a beszállítónak dokumentálnia kell az adatkezelőt ért incidens mérséklésére tett lépéseket (ti. dokumentált módon törli a jogellenesen megismert személyes adatokat). Ugyancsak kockázatnövelő tényező lehet, ha az incidensnek hosszútávú hatása lehet az érintettre.

- *Az incidens sérülékeny csoportot érint:* Kockázatnövelő tényező lehet, ha az incidens kiszolgáltatott személyeket (például gyermekek) érint.
- *Az érintettek magas száma:* Általánosságban kimondható, minél magasabb az adatvédelmi incidenssel érintettek száma, annál súlyosabb az incidens. Ugyanakkor ezt a kritériumot sem lehet mechanikusan alkalmazni, hiszen egy érintett esetén is lehet az incidens olyan súlyosságú, hogy az incidens kockázatbesorolása magas lesz. És sok érintett esetén is lehetnek olyan kockázatcsökkentő tényezők, amely alapján az incidens kockázatbesorolása alacsony marad.
- *Adatkezelők speciális kategóriája:* Ha az adatkezelő oldalán lehet olyan kritériumot találni, amely emelheti az incidens besorolását. Ez legtöbbször olyan esetben történhet meg, amikor magából az adatkezelőből lehet levonni bizonyos következtetéseket (például az adatkezelő rákdiagnosztikai központ).

A kockázatelemzés során tehát az adatkezelőnek a fenti kritériumokat érdemes mérlegelnie és azokat figyelembe véve azonosítani az érintett jogaira és szabadságaira veszélyt jelentő kockázatokat, majd ezeket a kockázatokat valószínűség és súlyosság szerint besorolnia.

12.10. Az incidens nyilvántartása és dokumentálása

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

A nyilvántartási kötelezettség valamennyi adatvédelmi incidensre kiterjed, függetlenül annak kockázataitól. Ez a kötelezettség elsősorban az elszámoltathatóság alapelvének az adatvédelmi incidensek kapcsán történő konkretizálása. A nyilvántartás formájára és módszerére a GDPR nem ad iránymutatást, az teljesen az adatkezelőtől függ. Nagyobb adatkezelők esetén, ahol az adatvédelmi incidensek száma is vélhetőleg magasabb, érdemes ezt a nyilvántartást összekapcsolni az adatkezelési műveletek nyilvántartásával. Az elszámoltathatóság elvéből következik, hogy a fent leírtak mellett a nyilvántartásban érdemes azt is rögzíteni, hogy az adatkezelő milyen indokok alapján döntött az adatvédelmi incidens bejelentéséről vagy annak mellőzéséről.

12.11. Az adatvédelmi tisztviselő szerepe

Ha az adatkezelő adatvédelmi tisztviselőt nevezett ki, akkor rá az incidens kezelésében jelentős szerep hárul. A GDPR alapjában véve kapcsolattartási és koordinációs szerepet szán neki a folyamatban, ugyanakkor egy általános szupervizori szerep megfelelőbb megközelítés.

12.12. Ellenőrző kérdések

Mi az adatvédelmi incidens fogalma?

Milyen szempontokat érdemes figyelembe venni az adatvédelmi incidensről történő értesülés időpontjának meghatározásánál?

Milyen adatkezelői kötelezettségek következnek a GDPR-ból az adatvédelmi incidensekkel kapcsolatosan?

Milyen kockázatokat befolyásoló tényezőket érdemes figyelembe venni az adatvédelmi incidensek kockázat besorolásakor?

Milyen megoldásokkal lehet felkészülni az adatvédelmi incidensek kezelésére?

13. JOGSZABÁLYTÁR

Magyarország Alaptörvénye

Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről [általános adatvédelmi rendelet, GDPR]

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

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [Infotv.]

Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény [Ákr.]

14. MELLÉKLETEK

Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban
Elérhetőség: http://naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf
(utolsó letöltés: 2018. szeptember 10.)

15. IRODALOMJEGYZÉK

Article 29 Data Protection Working Party (2007): Opinion 4/2007 on the concept of personal data. Elérhetőség: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf (utolsó letöltés: 2018. június 12.)

Article 29 Data Protection Working Party (2010): Opinion 1/2010 on the concepts of „controller" and „processor". Elérhetőség: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (utolsó letöltés: 2018. június 12.)

Article 29 Data Protection Working Party (2012): Opinion 3/2012 on developments in biometric technologies.

Elérhetőség: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (utolsó letöltés: 2018. június 12.)

Article 29 Data Protection Working Party (2013): Opinion 03/2013 on purpose limitation.

Elérhetőség: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (utolsó letöltés: 2018. június 12.)

Article 29 Data Protection Working Party (2017b): Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01. Elérhetőség: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (utolsó letöltés: 2018. június 10.)

Article 29 Data Protection Working Party (2017a): Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Elérhetőség: http://naih.hu/files/Guidelines-on-Automated-individual-decision-making-and-profiling.pdf (utolsó letöltés: 2018. június 10.)

Article 29 Data Protection Working Party (2017b): Guidelines on the right to data portability. Elérhetőség: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (utolsó letöltés: 2018. június 10.)

Article 29 Data Protection Working Party (2018): Guidelines on transparency under Regulation 2016/679. Elérhetőség: http://naih.hu/files/wp260rev.01_EN_Guidelines_on_Transparency.pdf (utolsó letöltés: 2018. június 10.)

Article 29 Data Protection Working Party (2018): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 2017. október 4. Elérhetőség: http://naih.hu/files/Iranymutatas-az-adatvedelmi-hatasvizsgalat-elvegzesehez.pdf (utolsó letöltés: 2018. június 18.)

Nemzeti Adatvédelmi és Információszabadság Hatóság (2013): Gyakorlati útmutató védett adatot nem tartalmazó kivonat készítéséhez. Elérhetőség: http://naih.hu/files/2014_02_03_anonimizalas_gyak_utm.pdf (utolsó letöltés: 2018. június 10.)

European Union Agency for Fundamental Rights (2018): Handbook on European Data Protection Law. Elérhetőség: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law (utolsó letöltés: 2018. június 10.)

David Wright – Paul De Hert: Privacy Impact Assessment, Springer Science and Business Media B.V., Springer Dordrecht Heidelberg London New York, 2012.

Balogh Zsolt György – Böröcz István – Kiss Attila – Polyák Gábor – Szőke Gergely László: Az adatvédelmi hatásvizsgálat módszertana, Médiakutató: Médiaelméleti Folyóirat XV. év. 4. szám. Elérhetőség: http://epa.oszk.hu/03000/03056/00057/pdf/EPA03056_mediakutato_2014_tel_077-092.pdf (utolsó letöltés: 2018. június 13.)

Szabó Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről I. Az adathordozhatóság és az adatvédelmi hatásvizsgálat, Pázmány Law Working Papers 2016/26. Elérhetőség: http://d18wh0wf8v71m4.cloudfront.net/docs/wp/2016/2016-26_Szabo.pdf (utolsó letöltés: 2018. június 13.)

Commission Nationale de l'Informatique et des Libertés (CNIL): Privacy Impact Assessment: Methodology (how to carry out a PIA), 2015. Elérhetőség: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (utolsó letöltés: 2018. június 13.)

Information Commissioner's Office (ICO): Conducting privacy impact assessments code of practice. ICO, 2014. Elérhetőség: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (utolsó letöltés: 2018. június 13.)

Veres Zsuzsanna: Az adatvédelmi hatásvizsgálat sajátosságai az európai adatvédelmi rendeletben, különös tekintettel az intelligens fogyasztásmérő rendszerek adatvédelmi hatásvizsgálatra. Szakdolgozat, 2017. ELTE ÁJK adatbiztonsági és adatvédelmi szakjogász képzés.

Felix Bieker – Michael Friedewald – Marit Hansen – Hannah Obersteller – Martin Rost: A process for data protection impact assessment under the European General Data Protection Regulation, Springer International Publishing Switzerland, APF, LNCS 9857, Karlsruhe, 2016. Elérhetőség: http://www.springer.com/cda/content/document/cda_downloaddocument/9783319447599-c2.pdf?SGWID=0-0-45-1587701-p180200777 (utolsó letöltés: 2018. június 13.)

Nemzeti Adatvédelmi és Információszabadság Hatóság éves beszámolói

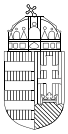
A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán
Címe:
1083 Budapest, Üllői út 82.
Kiadói szerkesztő:
Császár-Biró Anna
Tördelőszerkesztő:
Bödecs László

978-615-5870-71-2 (PDF)

A kiadvány
a KÖFOP-2.1.1-VEKOP-15-2016-00001
„A közszolgáltatás komplex kompetencia,
életpálya-program és oktatás technológiai
fejlesztése” című projekt keretében készült
el és jelent meg.



MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap

BEFEKTETÉS A JÖVŐBE