A 29. CIKK ALAPJÁN LÉTREHOZOTT ADATVÉDELMI MUNKACSOPORT

17/HU

WP 248 rev.01

Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e

Az elfogadás időpontja: 2017. április 4.

A legutóbbi felülvizsgálat és elfogadás időpontja: 2017. október 4.

AZ EGYÉNEKNEK A SZEMÉLYES ADATOK FELDOLGOZÁSA TEKINTETÉBEN VALÓ VÉDELMÉVEL FOGLALKOZÓ MUNKACSOPORT

amelyet az 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvvel hoztak létre,

tekintettel az említett irányelv 29. és 30. cikkére,

tekintettel eljárási szabályzatára,

ELFOGADTA EZT AZ IRÁNYMUTATÁST:

Tartalomjegyzék

I. Bevezetés

Az (EU) 2016/679 rendeletet 2018. május 25-től kell alkalmazni.[1] Az (EU) 2016/680 irányelv[2] mellett az általános adatvédelmi rendelet 35. cikke is bevezeti az adatvédelmi hatásvizsgálat fogalmát[3].

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[4] 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)[5]. Az **adatvédelmi hatásvizsgálat tehát a rendelet betartásának elérésére és bizonyítására szolgáló eljárás**.

Az általános adatvédelmi rendelet 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 (a 35. cikk (1) és (3)–(4)

---

[1] Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

[2] 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 szóló, 2016. április 27-i (EU) 2016/680 irányelv 27. cikke is rögzíti, hogy a magánélet védelmére vonatkozó hatásvizsgálatra akkor van szükség, ha az adatkezelés „*valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*".

[3] Ugyanez a fogalom más szövegösszefüggésekben gyakran a „magánélet védelmére vonatkozó hatásvizsgálatként" fordul elő.

[4] Az általános adatvédelmi rendelet hivatalosan nem határozza meg külön az adatvédelmi hatásvizsgálat fogalmát, de:

- minimális tartalmát a 35. cikk (7) bekezdése rögzíti az alábbiak szerint:
    - „*a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;*
    - *b) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;*
    - *c) az (1) bekezdésben említett, az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és*
    - *d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat";*
- jelentését és szerepét a (84) preambulumbekezdés tisztázza a következők szerint: „*Az e rendeletnek való megfelelés olyan esetek érdekében történő előmozdítása érdekében, amikor valószínűsíthető, hogy az adatkezelési műveletek magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, az e kockázat forrását, jellegét, egyediségét és súlyosságát felmérő adatvédelmi hatásvizsgálat elvégzéséért az adatkezelő felel.*"

[5] Lásd még a (84) preambulumbekezdést: „*A hatásvizsgálat megállapításait figyelembe kell venni annak meghatározásakor, hogy mely intézkedések a megfelelőek annak bizonyítására, hogy a személyes adatok kezelése megfelel e rendeletnek*".

bekezdése), helytelen elvégzése (a 35. cikk (2) és (7)–(9) bekezdése), vagy szükség esetén az illetékes felügyeleti hatósággal való egyeztetés elmulasztása (a 36. cikk (3) bekezdésének e) pontja) 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.

II. Az iránymutatás hatálya

Ez az iránymutatás az alábbi dokumentumok figyelembevételével készült:

- a 29. cikk szerinti adatvédelmi munkacsoport 14/EN WP 218. számú közleménye[6];
- a 29. cikk szerinti adatvédelmi munkacsoport 16/EN WP 243. számú iránymutatása az adatvédelmi tisztviselőről[7];
- a 29. cikk szerinti adatvédelmi munkacsoport 13/EN WP 203. számú véleménye a célhoz kötöttségről[8];
- nemzetközi szabványok[9].

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*” (a 35. cikk (1) bekezdése). Ez az iránymutatás elsősorban arra szolgál, hogy az adatvédelmi hatásvizsgálatot szükségessé tevő körülmények egységes értelmezése érdekében (a 35. cikk (3) bekezdése) tisztázza az említett fogalmat, és meghatározza azokat a szempontokat, amelyeket az adatvédelmi hatóságok által a 35. cikk (4) bekezdése értelmében elfogadandó jegyzékek összeállítása során figyelembe kell venni.

A 70. cikk (1) bekezdésének e) pontja szerint az Európai Adatvédelmi Testület iránymutatásokat, ajánlásokat és bevált módszereket fogalmazhat meg, hogy ezzel elősegítse az általános adatvédelmi rendelet egységes alkalmazását. Ennek a dokumentumnak a célja, hogy megalapozza az Európai Adatvédelmi Testület ilyen jellegű későbbi munkáját, és erre tekintettel egyértelművé tegye az általános adatvédelmi rendelet vonatkozó rendelkezéseit, hogy segítséget nyújtson az adatkezelőknek a

---

[6] A 29. cikk szerinti adatvédelmi munkacsoport 2014. május 30-án elfogadott 14/EN WP 218. számú közleménye az adatvédelmi jogi keretekre vonatkozó kockázatalapú megközelítés szerepéről (Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks).
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] A 29. cikk szerinti adatvédelmi munkacsoport 2016. december 13-án elfogadott 16/EN WP 243. számú iránymutatása az adatvédelmi tisztviselőről (Guidelines on Data Protection Officer 16/EN WP 243).
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] A 29. cikk szerinti adatvédelmi munkacsoport 2013. április 2-án elfogadott 03/2013. (13/EN WP 203) számú véleménye a célhoz kötöttségről.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Például ISO 31000:2009 *Kockázatkezelés – Elvek és iránymutatások* (Risk management — Principles and guidelines), Nemzetközi Szabványügyi Szervezet (ISO); ISO/IEC 29134 (projekt) *Informatika – Biztonságtechnika – A magánélet védelmére vonatkozó hatásvizsgálat – Iránymutatások* (Information technology – Security techniques – Privacy impact assessment – Guidelines), a Nemzetközi Szabványügyi Szervezet (ISO).

jogszabályok betartásában, és gondoskodjon az adatvédelmi hatásvizsgálat elvégzésére kötelezett adatkezelők jogbiztonságáról.

Ez az iránymutatás továbbá támogatni hivatott a következők kidolgozását:

- azoknak az adatkezelési műveleteknek a közös európai uniós jegyzéke, amelyekre vonatkozóan kötelező adatvédelmi hatásvizsgálatot végezni (a 35. cikk (4) bekezdése);
- azoknak az adatkezelési műveleteknek a közös uniós jegyzéke, amelyekre vonatkozóan nem szükséges adatvédelmi hatásvizsgálatot végezni (a 35. cikk (5) bekezdése);
- az adatvédelmi hatásvizsgálat módszereire vonatkozó közös szempontok (a 35. cikk (5) bekezdése);
- azoknak az eseteknek a meghatározására vonatkozó közös szempontok, amikor egyeztetni kell a felügyeleti hatósággal (a 36. cikk (1) bekezdése);
- lehetőség szerint az uniós tagállamokban gyűjtött tapasztalatokra épülő ajánlások.

III. Adatvédelmi hatásvizsgálat: a rendelet rendelkezéseinek magyarázata

Az általános adatvédelmi rendelet arra kötelezi az adatkezelőket, hogy a rendelkezései betartásának biztosítása és bizonyítása céljából hajtsanak végre megfelelő intézkedéseket, többek között „a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével" (a 24. cikk (1) bekezdése). Az adatkezelőknek az adatvédelmi hatásvizsgálat elvégzésére vonatkozó kötelezettségét a személyes adatok kezeléséből eredő kockáztok megfelelő kezelésére[10] vonatkozó általános kötelezettséggel összefüggésben kell értelmezni.

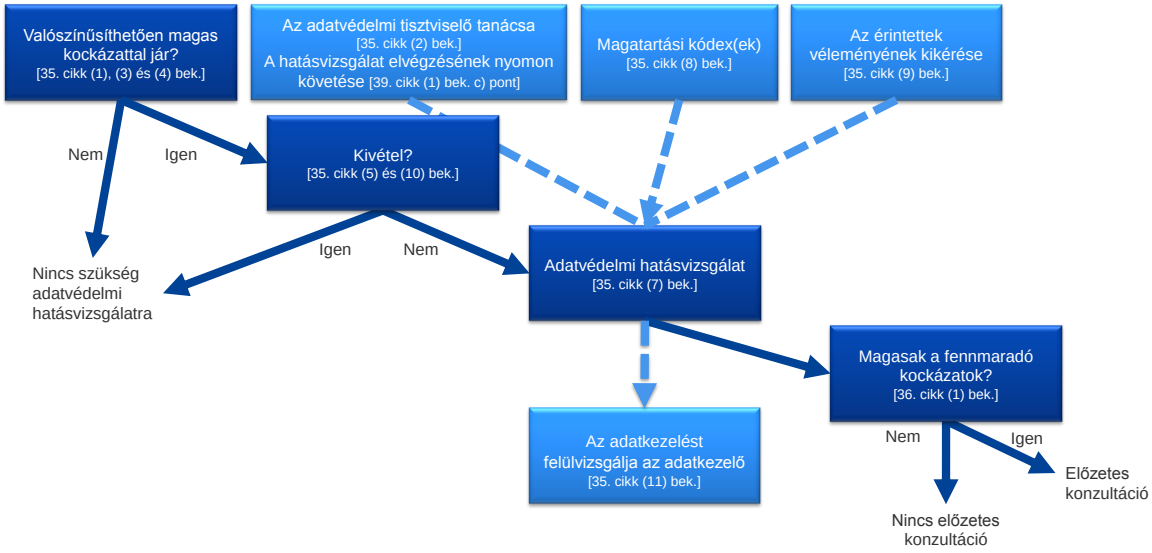
A „kockázat" olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. A „kockázatkezelés" viszont a szervezet kockázati vonatkozású irányítására és ellenőrzésére szolgáló összehangolt tevékenységek összességeként határozható meg.

A 35. cikk az egyének „jogaira és szabadságaira nézve" valószínűsíthetően magas kockázatot említ. A 29. cikk szerinti adatvédelmi munkacsoport az adatvédelmi jogi keretekre vonatkozó kockázatalapú megközelítés szerepéről szóló közleményében rámutatott, hogy az érintettek „jogaira és szabadságaira" való utalás elsősorban az adatvédelemhez és a magánélet tiszteletben tartásához való joghoz kapcsolódik, de érinthet más alapvető jogokat, úgymint a szólásszabadságot, a gondolatszabadságot, a mozgás szabadságát, a hátrányos megkülönböztetés tilalmát, a szabadsághoz való jogot, valamint a lelkiismereti és vallásszabadságot is.

Az általános adatvédelmi rendeletben kifejezésre juttatott kockázatalapú megközelítéssel összhangban nem mindegyik adatkezelési művelet esetében kötelező adatvédelmi hatásvizsgálatot végezni. Ehelyett csak akkor van szükség adatvédelmi hatásvizsgálatra, ha az adatkezelés valamely fajtája „*valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*" (a 35. cikk (1) bekezdése). Azonban önmagában az a tény, hogy az adatvédelmi hatásvizsgálat elvégzésének kötelezettségét keletkeztető feltételek nem teljesülnek, semmit nem von le az adatkezelők azon általános kötelezettségéből, hogy intézkedéseket hajtsanak végre az érintettek jogait és szabadságait érintő kockázatok megfelelő kezelése érdekében. A gyakorlatban ez azt jelenti, hogy az adatkezelőknek folyamatosan értékelniük kell az adatkezelési tevékenységeikből eredő kockázatokat, hogy felismerjék, ha az adatkezelés valamely fajtája „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve".

[10] Hangsúlyozandó, hogy a természetes személyek jogait és szabadságait érintő kockázatok csak akkor kezelhetők, ha rendszeresen beazonosítják, elemzik, felmérik, értékelik, orvosolják (például csökkentik stb.) és felülvizsgálják őket. Az adatkezelők nem bújhatnak ki felelősségük alól azzal, hogy biztosításokat kötnek a kockázatokra.

Az alábbi ábra az általános adatvédelmi rendeletben az adatvédelmi hatásvizsgálattal kapcsolatosan megfogalmazott elveket szemlélteti:



A. Mi az adatvédelmi hatásvizsgálat tárgya? Egyetlen adatkezelési művelet vagy egymáshoz hasonló típusú adatkezelési műveletek.

Az adatvédelmi hatásvizsgálat érinthet egyetlen adatkezelési műveletet. A 35. cikk (1) bekezdése azonban a következőképpen rendelkezik: „*[o]lyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek*”. A (92) preambulumbekezdés ezt azzal egészíti ki, hogy „*[b]izonyos 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, vagy ha több adatkezelő közös alkalmazást vagy adatkezelési környezetet kíván bevezetni valamely ágazat vagy szegmens, vagy valamely széles körben végzett horizontális tevékenység tekintetében*”.

Egyetlen adatvédelmi hatásvizsgálat végezhető több, jellegét, hatókörét körülményeit, célját és kockázatait tekintve egymáshoz hasonló adatkezelési művelet értékeléséhez is. Az adatvédelmi hatásvizsgálatok tehát azoknak az új helyzeteknek a módszeres elemzésére irányulnak, amelyek a természetes személyek jogaira és szabadságaira nézve magas kockázattal járhatnak, ezért a már vizsgált esetekben (vagyis meghatározott körülmények között és konkrét céllal végzett adatkezelési műveletnél) nincs szükség adatvédelmi hatásvizsgálatra. Ez akkor fordulhat elő, ha hasonló technológiát használnak ugyanolyan jellegű adatok azonos céllal való gyűjtéséhez. Például hasonló zártláncú televíziós rendszert kiépítő települési önkormányzatok csoportja végezhet egyetlen adatvédelmi hatásvizsgálatot az ezen önálló adatkezelők által végzett adatkezelésről, és egy vasúti üzemeltetőnek (egyedüli adatkezelőnek) is elegendő egyetlen adatvédelmi hatásvizsgálatot végeznie az összes vasútállomásán végzett videokamerás megfigyelésre vonatkozóan. Ez az elv a különböző más adatkezelők által végzett hasonló adatkezelési műveletekre is alkalmazható. Ilyen esetekben meg kell osztani vagy a nyilvánosság számára hozzáférhetővé kell tenni a hivatkozási alapként használható adatvédelmi hatásvizsgálat részleteit, végre kell hajtani az adott adatvédelmi hatásvizsgálatban meghatározott intézkedéseket, és indokolni kell, miért egyetlen adatvédelmi hatásvizsgálatot végeznek.

Amikor közös adatkezelők vesznek részt az adatkezelési műveletben, pontosan meg kell határozniuk a kötelezettségeiket. Adatvédelmi hatásvizsgálatuk keretében meg kell határozniuk, melyik fél felel a kockázatok kezelésére és az érintettek jogainak és szabadságainak védelmére irányuló különféle intézkedésekért. Mindegyik adatkezelőnek titoksértés (például üzleti titkok, szellemi tulajdon és bizalmas üzleti információk védelme) és sebezhetőségek felfedése nélkül kell kifejeznie az igényeit, és megosztania hasznos információkat.

Az adatvédelmi hatásvizsgálat valamely technológiai termék, például hardver vagy szoftver adatvédelmi hatásainak felmérésekor is hasznosnak bizonyulhat, ha az adott terméket valószínűleg különböző adatkezelők használják, különféle adatkezelési műveletek elvégzésére. A terméket üzembe helyező adatkezelő természetesen változatlanul köteles saját adatvédelmi hatásvizsgálatot végezni a konkrét megvalósításról, de ehhez adott esetben felhasználható a termék szolgáltatója által elvégzett adatvédelmi hatásvizsgálat. Erre példa az intelligens fogyasztásmérők gyártói és a közműszolgáltató vállalatok közötti kapcsolat. Mindegyik termékszolgáltatónak vagy adatfeldolgozónak titoksértés és a sebezhetőségek felfedéséből fakadó biztonsági kockázatok előidézése nélkül kell megosztania hasznos információkat.

B. Mely adatkezelési műveletekre vonatkozóan kell adatvédelmi hatásvizsgálatot végezni? A kivételektől eltekintve akkor, ha az adatkezelési művelet „*valószínűsíthetően magas kockázattal jár*”.

Ez a szakasz arról nyújt felvilágosítást, mikor kötelező, és mely esetekben nem szükséges adatvédelmi hatásvizsgálatot végezni.

Amennyiben az adatkezelési művelet nem tartozik a kivételek körébe (a III. fejezet B. szakaszának a) pontja), adatvédelmi hatásvizsgálatot kell végezni, ha az adatkezelési művelet „*valószínűsíthetően magas kockázattal jár*” (a III. fejezet B. szakaszának b) pontja).

a) Mikor kötelező az adatvédelmi hatásvizsgálat? Amikor az adatkezelés „*valószínűsíthetően magas kockázattal jár*”.

Az általános adatvédelmi rendelet nem írja elő adatvédelmi hatásvizsgálat elvégzését minden olyan adatkezelési művelet esetében, amely természetes személyek jogaira és szabadságaira nézve kockázattal járhat. Csak akkor kötelező adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés „*valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*” (a 35. cikk (1) bekezdése, részletesen kifejti a 35. (3) bekezdése, és kiegészíti 35. cikk (4) bekezdése). Ez különösen új adatkezelési technológiák bevezetésekor lényeges[11].

Azokra az esetekre, amikor nem egyértelmű, hogy szükség van-e adatvédelmi hatásvizsgálatra, a 29. cikk szerinti adatvédelmi munkacsoport azt ajánlja, hogy az adatkezelők mindenképpen végezzék az adatvédelmi hatásvizsgálatot, mivel segítséget jelenthet számukra az adatvédelmi jogszabályok betartásában.

Az adatvédelmi hatásvizsgálat ugyan más körülmények között is kötelező lehet, mindazonáltal a 35. cikk (3) bekezdése néhány példával szolgál azokra az esetekre, amikor az adatkezelési művelet „*valószínűsíthetően magas kockázattal jár*”:

[11] További példák a (89) és (91) preambulumbekezdésben, valamint a 35. cikk (1) és (3) bekezdésében találhatók.

- „*a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek*[12]*;*
- *b) a 9. cikk (1) bekezdésében említett személyes adatok különleges kategóriái, vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése*[13]*; vagy*
- *c) nyilvános helyek nagymértékű, módszeres megfigyelése*”.

Az általános adatvédelmi rendelet 35. cikke (3) bekezdésének bevezető mondatában szereplő „*különösen*” szó is jelzi, hogy a felsorolás nem kimerítő jellegű. Előfordulhatnak olyan „magas kockázatú” adatkezelési műveletek, amelyek ugyan nem szerepelnek a felsorolásban, mégis hasonlóan nagy kockázattal járnak. Az ilyen adatkezelési műveletek esetében szintén adatvédelmi hatásvizsgálatot kell végezni. Következésképpen az alábbiakban kifejtett szempontok néha túlmutatnak az általános adatvédelmi rendelet 35. cikkének (3) bekezdésében megadott három példa egyszerű magyarázatán.

Az eredendően magas kockázatuk miatt kötelező adatvédelmi hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének pontosabb meghatározása érdekében a 35. cikk (1) bekezdésében és (3) bekezdésének a)–c) pontjában szereplő különös elemekre, a 35. cikk (4) bekezdése, valamint a (71), (75) és (91) preambulumbekezdés értelmében tagállami szinten elfogadandó jegyzékre, továbbá az általános adatvédelmi rendeletben a „*valószínűsíthetően magas kockázattal járó*” adatkezelési műveletekre tett egyéb utalásokra[14] figyelemmel a következő kilenc szempontot kell mérlegelni:

1. Értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is, különösen *“az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők”* alapján ((71) és (91) preambulumbekezdés). Erre példaként említhető a pénzügyi vállalkozás, 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, vagy a vállalkozás, amely viselkedési vagy üzletszerzési profilokat készít a honlapjának használata vagy böngészése alapján.
2. Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a „*természetes személy tekintetében joghatással bíró*” vagy „*a természetes személyt hasonlóképpen jelentős mértékben érintő*” döntések meghozatala (a 35. cikk (3)

[12] Lásd a (75) preambulumbekezdést: „*különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából*”.

[13] Lásd a (75) preambulumbekezdést: „*ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak*”.

[14] Lásd például a (75), (76), (92) és (116) preambulumbekezdést.

bekezdésének a) pontja). Az adatkezelés adott esetben például egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti. Az egyénekre nézve csekély vagy semmilyen hatással nem járó adatkezelés nem felel meg ennek a konkrét szempontnak. Az itt említett fogalmakról további felvilágosítást nyújt majd a 29. cikk szerinti adatvédelmi munkacsoport soron következő, profilalkotásról szóló iránymutatása.

3. Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a „*nyilvános helyek nagymértékű, módszeres megfigyelése*" (a 35. cikk (3) bekezdésének c) pontja)[15]. Az ilyen jellegű megfigyelés azért tartozik a figyelembe veendő szempontok közé, mivel a személyes adatok gyűjtése olyan körülmények között folyhat, ahol előfordulhat, hogy az érintettek nem tudják, ki gyűjti és hogyan használja fel adataikat. Ezenkívül az egyéneknek talán nincs lehetőségük elkerülni, hogy közterületeken (vagy nyilvános helyeken) érintetté váljanak ilyen adatkezelésben.
4. Különleges adatok vagy fokozottan személyes jellegű adatok: ide tartoznak a személyes adatok 9. cikkben meghatározott különleges kategóriái (például az egyének politikai véleményére vonatkozó adatok), valamint a 10. cikkben meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok. Példaként említhető az általános kórház, amely nyilvántartást vezet a betegek kórtörténetéről, vagy a magánnyomozó, aki megőrzi az elkövetők adatait. Az általános adatvédelmi rendelet e rendelkezésein túlmenően bizonyos adatkategóriák tekinthetők úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat. Ezek a személyes adatok (a fogalom általánosan ismert jelentését tekintve) különlegesnek minősülhetnek, mivel otthoni vagy magánjellegű tevékenységekhez kapcsolódnak (például elektronikus hírközlési tevékenységekhez, amelyek bizalmassága védendő), kihatnak valamely alapvető jog gyakorlására (például helymeghatározó adatok, amelyek gyűjtése megkérdőjelezi a mozgás szabadságát), vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére (például pénzügyi adatok, amelyek csalásra használhatók). 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. Ez a szempont olyan adatokra is vonatkozhat, mint például a személyes iratok, e-mailek, naplók, jegyzetelési funkcióval rendelkező e-olvasókból származó jegyzetek, valamint az életnaplózó alkalmazásokban tárolt, rendkívül személyes jellegű adatok.
5. Nagy számban kezelt adatok: az általános adatvédelmi rendelet nem határozza meg, mi értendő nagy szám alatt, jóllehet a (91) preambulumbekezdés nyújt némi iránymutatást. Mindenesetre a 29. cikk szerinti adatvédelmi munkacsoport ajánlása szerint különösen az

[15] A 29. cikk szerinti adatvédelmi munkacsoport a "*módszeres*" szót úgy értelmezi, hogy az alábbiak közül egy vagy több jelentéstartalommal rendelkezik (lásd a 29. cikk szerinti adatvédelmi munkacsoport adatvédelmi tisztviselőről szóló 16/EN WP 243. számú iránymutatását):

- módszer szerint zajlik;
- előre meghatározott, szervezett vagy tervszerű;
- általános adatgyűjtési terv részeként megy végbe;
- stratégia részeként történik.

A 29. cikk szerinti adatvédelmi munkacsoport értelmezése szerint a "*nyilvános hely*" a nyilvánosság bármely tagja előtt nyitva álló bármely terület, például köztér, bevásárlóközpont, utca, piactér, vasútállomás vagy közkönyvtár.

alábbi tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e[16]:

a. az érintettek száma konkrét számadatként vagy a lakosság arányában;
b. a kezelt adatok mennyisége vagy adatfajták köre;
c. az adatkezelési tevékenység időtartama vagy állandó jellege;
d. az adatkezelési tevékenység földrajzi kiterjedése.

6. Adatkészletek egymással való megfeleltetése vagy összevonása például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon[17].
7. Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok ((75) preambulumbekezdés): az ilyen jellegű adatok kezelése azért tartozik a figyelembe veendő szempontok közé, mivel nincs hatalmi egyensúly az érintettek és az adatkezelő között, ami azt jelenti, hogy az egyének adott esetben nem tudják adataik kezelését könnyen engedélyezni vagy ellenezni, illetve nem tudják a jogaikat gyakorolni. A kiszolgáltatott helyzetben lévő érintettek közé sorolhatók a gyermekek (ők úgy tekintendők, mint akik nem tudják tudatosan és átgondoltan ellenezni vagy engedélyezni adataik kezelését), a munkavállalók, a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei (mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb.), valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki.
8. Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása, például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében stb. Az általános adatvédelmi rendelet egyértelműen megfogalmazza (a 35. cikk (1) bekezdése, valamint a (89) és a (91) preambulumbekezdés), hogy "*a technológia elismert állásának megfelelő*" módon meghatározott új technológia ((91) preambulumbekezdés) használata szükségessé teheti az adatvédelmi hatásvizsgálat elvégzését. Ennek oka, hogy az ilyen technológiák használatához újfajta adatgyűjtési és -felhasználási formák kapcsolódhatnak, ami magas kockázattal járhat az egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek. Az adatvédelmi hatásvizsgálat révén az adatkezelő megismerheti és orvosolhatja az ilyen jellegű kockázatokat. Például bizonyos, a „dolgok internetét" használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését.
9. Azok az esetek, amikor az adatkezelés önmagában véve *"megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek"* (22. cikk és (91) preambulumbekezdés). Ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek. Erre példa, ha egy bank hitelreferencia-adatbázis alapján szűri ügyfeleit, hogy eldöntse, kínál-e nekik hitelt.

Az esetek többségében az adatkezelő tekintheti úgy, hogy két szempontnak megfelelő adatkezelés esetében szükség van adatvédelmi hatásvizsgálatra. A 29. cikk szerinti adatvédelmi munkacsoport általában véve úgy véli, hogy minél több szempontnak felel meg az adatkezelés, annál nagyobb a

[16] Lásd a 29. cikk szerinti adatvédelmi munkacsoport adatvédelmi tisztviselőről szóló 16/EN WP 243. számú iránymutatását.

[17] A magyarázatot lásd a 29. cikk szerinti adatvédelmi munkacsoport célhoz kötöttségről szóló 13/EN WP 203. számú véleményének 24. oldalán.

valószínűsége annak, hogy magas kockázattal jár az érintettek jogaira és szabadságaira nézve, ezért pedig az adatkezelő által végrehajtani tervezett intézkedésektől függetlenül szükségessé teszi az adatvédelmi hatásvizsgálat elvégzését.

Bizonyos esetekben viszont **az adatkezelő tekintheti úgy, hogy a mindössze egy szempontnak megfelelő adatkezelés esetében is szükség van adatvédelmi hatásvizsgálatra**.

Az alábbiakban olvasható példák azt szemléltetik, hogyan kell felhasználni a szempontokat annak értékeléséhez, hogy az adott adatkezelési műveletre vonatkozóan kell-e végezni adatvédelmi hatásvizsgálatot:

Példák adatkezelésre	**Lehetséges lényeges szempontok**	**Valószínűsíthetően szükség van-e adatvédelmi hatásvizsgálatra?**
A betegek genetikai és egészségügyi adatait kezelő kórház (kórházi információs rendszer).	- Különleges adatok vagy fokozottan személyes jellegű adatok. - Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok. - Nagy számban kezelt adatok.	Igen
Kamerarendszer használata a vezetői magatartás megfigyelésére az autópályákon. Az adatkezelő intelligens videoelemző rendszer használatát tervezi járművek kiszűrése és automatikus rendszámfelismerés céljából.	- Módszeres megfigyelés. - Technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása.	
Az alkalmazottai tevékenységeit módszeresen megfigyelő, így az alkalmazottak munkaállomását, internetes tevékenységeit stb. nyomon követő vállalkozás.	- Módszeres megfigyelés. - Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok.	
A közösségi médiából származó nyilvános adatok gyűjtése profilalkotás céljából.	- Értékelés vagy pontozás. - Nagy számban kezelt adatok. - Adatkészletek egymással való megfeleltetése vagy összevonása. - Különleges adatok vagy fokozottan személyes jellegű adatok:	
Országos hitelminősítési vagy csalásellenes adatbázist létrehozó pénzügyi vállalkozás.	- Értékelés vagy pontozás. - Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal. - Megakadályozza, hogy az érintett a jogait gyakorolja vagy szolgáltatást vegyen igénybe vagy szerződést érvényesítsen. - Különleges adatok vagy fokozottan személyes jellegű adatok:	
Kutatási projektekben vagy klinikai vizsgálatokban részt vevő, kiszolgáltatott	- Különleges adatok. - Kiszolgáltatott helyzetben lévő	

Példák adatkezelésre	Lehetséges lényeges szempontok	Valószínűsíthetően szükség van-e adatvédelmi hatásvizsgálatra?
helyzetben lévő érintettekkel kapcsolatos, álnevesített, különleges személyes adatok tárolása archiválás céljából.	érintettekkel kapcsolatos adatok. - Megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek.	
„Egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes [adatainak]" feldolgozása ((91) preambulumbekezdés).	- Különleges adatok vagy fokozottan személyes jellegű adatok. - Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok.	Nem
A feliratkozóknak általános napi sajtószemle küldéséhez levelezőlistát használó internetes magazin.	- Nagy számban kezelt adatok.	
A honlapon megtekintett vagy megvásárolt árucikkek alapján végzett profilalkotás révén veterán járművek alkatrészeire vonatkozó hirdetéseket megjelenítő e-kereskedelmi honlap.	- Értékelés vagy pontozás.	

Ezzel szemben előfordulhat, hogy egy adatkezelési művelet ugyan megfelel a fent ismertetett esetek egyikének, az adatkezelő azonban mégsem úgy ítéli meg, hogy „valószínűsíthetően magas kockázattal jár". Ilyenkor az adatkezelőnek indokolnia és dokumentumokkal igazolnia kell az adatvédelmi hatásvizsgálat mellőzésének okait, és ezzel összefüggésben az adatvédelmi tisztviselő álláspontját is közölnie/rögzítenie kell.

Ezenkívül az elszámoltathatósági elv értelmében mindegyik adatkezelő "*a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet*", amely szerepelnek egyebek mellett az adatkezelés céljai, az adatkategóriák leírása, az adatok címzettjei és „*ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása*" (a 30. cikk (1) bekezdése). Az adatkezelőknek emellett értékelniük kell, hogy valószínűsíthető-e magas kockázat, még abban az esetben is, ha végül úgy döntenek, hogy nem végeznek adatvédelmi hatásvizsgálatot.

Megjegyzés: a felügyeleti hatóságoknak össze kell állítaniuk, nyilvánosságra kell hozniuk, és az Európai Adatvédelmi Testületnek továbbítaniuk kell az olyan adatkezelési műveletek jegyzékét, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni (a 35. cikk (4) bekezdése)[18]. A felügyeleti hatóságok a fentiekben meghatározott szempontok alapján elkészíthetik ezt a listát, amelynek tartalmát idővel konkrétabb információkkal egészíthetik ki, ha szükséges. Például bármely

[18] Ezzel összefüggésben „*az illetékes felügyeleti hatóság igénybe veszi a 63. cikkben említett egységességi mechanizmust, ha ezek a jegyzékek olyan adatkezelési tevékenységeket tartalmaznak, amelyek az érintettek számára történő, több tagállamra kiterjedő áru- vagy szolgáltatás nyújtásához vagy az érintettek viselkedésének több tagállamra kiterjedő megfigyeléséhez kapcsolódnak, vagy érdemben érinthetik a személyes adatok Unión belüli szabad áramlását*" (a 35. cikk (6) bekezdése).

fajta biometrikus vagy gyermekekkel kapcsolatos adat is lényegesnek tekinthető a 35. cikk (4) bekezdése szerinti jegyzék kidolgozásához.

b) Mikor nincs szükség adatvédelmi hatásvizsgálatra? Ha az adatkezelés „*valószínűsíthetően nem jár magas kockázattal*", már készült hasonló adatvédelmi hatásvizsgálat, az adatkezelést 2018 májusa előtt engedélyezték, jogalapja van, vagy szerepel azoknak az adatkezelési műveleteknek a jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

A 29. cikk szerinti adatvédelmi munkacsoport megítélése szerint a következő esetekben nincs szükség adatvédelmi hatásvizsgálatra:

- **ha az adatkezelés valószínűsíthetően nem jár „*magas kockázattal […] a természetes személyek jogaira és szabadságaira nézve*"** (a 35. cikk (1) bekezdése);
- **ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat**. Ilyen esetekben felhasználhatók a hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei (a 35. cikk (1) bekezdése)[19];
- ha az adatkezelési műveleteket felügyeleti hatóság meghatározott, azóta változatlan feltételek mellett 2018. május előtt ellenőrizte[20] (lásd a III. fejezet C. szakaszát);
- **ha a** 6. cikk (1) bekezdésének c) vagy e) pontja szerinti **adatkezelési művelet jogalappal rendelkezik** az uniós vagy tagállami jogban, a jog szabályozza az adott adatkezelési műveletet, **és** az említett jogalap megállapítása során **már készült adatvédelmi hatásvizsgálat** (a 35. cikk (10) preambulumbekezdése)[21], kivéve, ha a tagállam kimondta, hogy az adatkezelési műveletet megelőzően hatásvizsgálatot szükséges végezni;
- **ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) nem kötelező jegyzékében,** amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni (a 35. cikk (5) bekezdése). Ez a jegyzék olyan adatkezelési tevékenységeket tartalmazhat, amelyek megfelelnek a hatóság által – különösen iránymutatások, egyedi határozatok vagy engedélyek, megfelelési szabályok stb. útján – megállapított feltételeknek (Franciaországban például engedélyek, kivételek, egyszerűsített szabályok, megfelelési csomagok stb.). Ilyen esetekben az értékelés illetékes hatóság általi megismétlése mellett nem szükséges adatvédelmi hatásvizsgálatot végezni, de csak akkor, ha az adatkezelés szigorúan a jegyzékben megjelölt eljárás hatálya alá tartozik, és továbbra is teljes mértékben megfelel az általános adatvédelmi rendelet vonatkozó követelményeinek.

C. <u>Mi a helyzet a már folyamatban lévő adatkezelési műveletekkel? Bizonyos körülmények között adatvédelmi hatásvizsgálatot kell végezni.</u>

[19] „*Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.*"

[20] „*A 95/46/EK irányelv alapján a Bizottság által hozott határozatok, valamint a felügyeleti hatóságok által kiadott engedélyek hatályban maradnak mindaddig, amíg módosításukra, felváltásukra vagy hatályon kívül helyezésükre sor nem kerül*" ((171) preambulumbekezdés).

[21] Ha az adatkezelés jogalapjául szolgáló jogszabály kidolgozása során végeznek adatvédelmi hatásvizsgálatot, akkor az adatkezelési műveletek megkezdése előtt valószínűleg szükség lesz felülvizsgálatra, mivel az elfogadott jogszabály magánéleti és adatvédelmi kérdéseket illetően eltérhet a jogszabály-javaslattól. Emellett előfordulhat, hogy a jogszabály elfogadásakor nem állnak rendelkezésre elegendő technikai adatok a tényleges adatkezelésről, még akkor sem, ha készült mellette adatvédelmi hatásvizsgálat. Ilyen esetekben mégis szükség lehet külön adatvédelmi hatásvizsgálat elvégzésére a tényleges adatkezelési tevékenységek megkezdése előtt.

Az adatvédelmi hatásvizsgálat elvégzésére vonatkozó követelmény azokra a folyamatban lévő adatkezelési műveletekre vonatkozik, amelyeknél valószínűsíthető, hogy magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, és amelyek esetében megváltoztak a kockázatok, figyelemmel az adatkezelés jellegére, hatókörére, körülményére és céljára.

Nincs szükség adatvédelmi hatásvizsgálatra olyan adatkezelési műveleteknél, amelyek a 95/46/EK irányelv 20. cikke értelmében a felügyeleti hatóság vagy az adatvédelmi tisztviselő ellenőrzött, és amelyeket az előzetes ellenőrzés óta változatlan módon hajtanak végre. Sőt, „*[a] 95/46/EK irányelv alapján a Bizottság által hozott határozatok, valamint a felügyeleti hatóságok által kiadott engedélyek hatályban maradnak mindaddig, amíg módosításukra, felváltásukra vagy hatályon kívül helyezésükre sor nem kerül*” ((171) preambulumbekezdés).

Ez ugyanakkor azt is jelenti, hogy adatvédelmi hatásvizsgálatnak kell alávetni azokat az adatkezelési műveleteket, amelyek végrehajtásának körülményei (hatókör, cél, a gyűjtött személyes adatok köre, az adatkezelők vagy címzettek kiléte, az adatmegőrzési időszak, a technikai és szervezési intézkedések stb.) a felügyeleti hatóság vagy az adatvédelmi tisztviselő által végzett előzetes ellenőrzés óta megváltoztak, és amelyek esetében valószínűsíthető, hogy magas kockázattal járnak.

Ezenfelül akkor is szükség lehet adatvédelmi hatásvizsgálatra, ha az adatkezelési műveletekből eredő kockázatok[22] megváltoznak, például azért, mert új technológiákat kezdenek el használni, vagy a személyes adatokat eltérő célra használják fel. Az adatkezelési műveletek gyorsan átalakulhatnak, és új sebezhetőségek merülhetnek fel. Ezért megjegyzendő, hogy az adatvédelmi hatásvizsgálat felülvizsgálata nemcsak a folyamatos fejlődés szempontjából hasznos, de az idővel változó környezetben az adatvédelem szintjének fenntartásához is elengedhetetlen. Akkor is szükségessé válhat az adatvédelmi hatásvizsgálat, ha az adatkezelési tevékenység szervezeti vagy társadalmi körülményei megváltoznak, például bizonyos automatizált döntések hatása felerősödik, vagy érintettek új kategóriái válnak kiszolgáltatottá a hátrányos megkülönböztetéssel szemben. Mindegyik említett példa olyan tényező lehet, amely az adott adatkezelési tevékenységből eredő kockázatok megváltozásához vezet.

Ugyanakkor bizonyos változások csökkenthetik is a kockázatokat. Az adatkezelési művelet például átalakulhat úgy, hogy a döntések már nem automatizáltan születnek, vagy a megfigyelési tevékenység már nem módszeresen zajlik. Ez esetben az elvégzett kockázatelemzés felülvizsgálata kimutathatja, hogy már nincs szükség adatvédelmi hatásvizsgálatra.

Az adatvédelmi hatásvizsgálatot érdemes folyamatosan felülvizsgálni, és rendszeresen újraértékelni. Jóllehet tehát, hogy 2018. május 25-ig nincs szükség adatvédelmi hatásvizsgálatra, az adatkezelőnek azonban az általános elszámoltathatósági kötelezettségei részeként el kell majd végeznie a megfelelő időben.

D. <u>Hogyan kell elvégezni az adatvédelmi hatásvizsgálatot?</u>

a) Mikor kell elvégezni az adatvédelmi hatásvizsgálatot? Az adatkezelés megkezdése előtt.

[22] A körülmények, a gyűjtött adatok, a célok, a funkciók, a kezelt személyes adatok, a címzettek, az adatkombinációk, a kockázatok (támogató eszközök, kockázatforrások, lehetséges hatások, veszélyek stb.), a biztonsági intézkedések és a nemzetközi adattovábbítás szempontjából.

Az adatvédelmi hatásvizsgálatot „*az adatkezelést megelőzően*” kell elvégezni (a 35. cikk (1) és (10) bekezdése, valamint a (90) és a (93) preambulumbekezdés)[23]. Ez összhangban van a beépített adatvédelem és az alapértelmezett adatvédelem elvével (25. cikk és (78) preambulumbekezdés). Az adatvédelmi hatásvizsgálatot az adatkezeléssel kapcsolatos döntések meghozatalát segítő eszköznek kell tekinteni.

Az adatvédelmi hatásvizsgálatot az adatkezelési művelet kialakítása során a lehető leghamarabb meg kell kezdeni, akkor is, ha az adatkezelési műveletek egy része még nem ismert. A projekt időtartama alatt az adatvédelmi hatásvizsgálat folyamatos aktualizálásával biztosítható az adatvédelem és a magánélet figyelembevétele, és ösztönözhető az előírások betartását előmozdító megoldások kidolgozása. Előfordulhat, hogy a kidolgozási folyamat előrehaladásával meg kell ismételni a hatásvizsgálat egyes lépéseit, mivel bizonyos technikai és szervezési intézkedések kiválasztása befolyásolhatja az adatkezelésből eredő kockázatok súlyosságát vagy valószínűségét.

Az, hogy az adatvédelmi hatásvizsgálatot talán úgyis aktualizálni kell az adatkezelés megkezdése után, nem érv amellett az adatvédelmi hatásvizsgálat elhalasztása vagy mellőzése mellett. Az adatvédelmi hatásvizsgálat egy folyamat, különösen akkor, ha az adatkezelési művelet dinamikus, és állandóan változik. **Az adatvédelmi hatásvizsgálatot nem egyetlen alkalommal, hanem folyamatosan kell végezni**.

b) Ki köteles végrehajtani az adatvédelmi hatásvizsgálatot? Az adatkezelő az adatvédelmi tisztviselővel és az adatfeldolgozóval együtt.

Az adatkezelőnek kell gondoskodnia arról, hogy az adatvédelmi hatásvizsgálatot elvégezzék (a 35. cikk (2) bekezdése). Az adatvédelmi hatásvizsgálatot elvégezheti a szervezeten belül vagy kívül más is, de az adatkezelőt terheli végső felelősség e feladat teljesítéséért.

Ha van kijelölt adatvédelmi tisztviselő, az adatkezelőnek az ő tanácsát is ki kell kérnie (a 35. cikk (2) bekezdése), a kapott tanácsokat és az adatkezelő által hozott döntéseket pedig írásba kell foglalni az adatvédelmi hatásvizsgálat során. Az adatvédelmi tisztviselőnek emellett nyomon kell követnie a hatásvizsgálatot (a 39. cikk (1) bekezdésének c) pontja). További útmutatások a 29. cikk szerinti adatvédelmi munkacsoport adatvédelmi tisztviselőről szóló 16/EN WP 243. számú iránymutatásában találhatók.

Ha az adatkezelést teljes egészében vagy részben adatfeldolgozó végzi, **segítenie kell az adatkezelőt az adatvédelmi hatásvizsgálat lefolytatásában**, és közölnie kell a szükséges információkat (a 28. cikk (3) bekezdésének f) pontja).

Az adatkezelő „*adott esetben*” „*kikéri az érintettek vagy képviselőik véleményét*” (a 35. cikk (9) bekezdése). A 29. cikk szerinti adatvédelmi munkacsoport álláspontja a következő:

- az érintettek véleménye különféleképpen kikérhető a helyzettől (például az adatkezelési művelet céljával és eszközével kapcsolatos általános vizsgálat, a személyzet képviselőihez intézett kérdés vagy az adatkezelő leendő ügyfeleihez intézett szokványos felmérés) függően, ügyelve arra, hogy az adatkezelő rendelkezzen az e véleményekben foglalt személyes adatok

[23] Kivéve a felügyeleti hatóság által előzetesen ellenőrzött, már folyamatban lévő adatkezelés esetén, amikor az adatvédelmi hatásvizsgálatot a jelentős változások végrehajtása előtt el kell végezni.

feldolgozásához szükséges jogalappal. Ugyanakkor megjegyzendő, hogy az adatkezeléshez való hozzájárulás nyilvánvalóan nem minősül az érintetti vélemények kikérésének;
- ha az adatkezelő végleges döntése eltér az érintettek véleményétől, akkor dokumentumokkal alá kell támasztania annak végrehajtásának vagy elvetésének okait;
- az adatkezelőnek dokumentumokkal kell indoklnia azt is, hogy miért nem kéri ki az érintettek véleményét, amennyiben úgy dönt, hogy erre nincs szükség, például azért mert ezzel vállalkozások üzleti tervének titkossága sérülne, illetve aránytalan vagy kivitelezhetetlen lenne ez az intézkedés.

Végül pedig a belső politikáktól, eljárásoktól és szabályoktól függően érdemes meghatározni és írásba foglalni az egyéb szerep- és felelősségi köröket, például az alábbi esetekben:
- amennyiben egyes üzleti egységek adatvédelmi hatásvizsgálat elvégzését javasolhatják, akkor lehetőleg adatokat kell szolgáltatniuk az adatvédelmi hatásvizsgálathoz, valamint érdemes közreműködniük az adatvédelmi hatásvizsgálat jóváhagyási eljárásában;
- adott esetben ajánlott tanácsot kérni különböző szakterületek független szakértőitől[24] (jogászok, informatikai szakértők, biztonsági szakértők, szociológusok, etikai szakértők stb.);
- az adatfeldolgozó szerep- és felelősségi körét szerződésben kell rögzíteni, az adatvédelmi hatásvizsgálatot pedig az adatfeldolgozó segítségével kell elvégezni, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat (a 28. cikk (3) bekezdésének f) pontja);
- ha kijelölnek információbiztonsági igazgatót, akkor az adatvédelmi tisztviselővel együtt javaslatot tehet arra, hogy az adatkezelő valamely konkrét adatkezelési műveletre vonatkozóan végezzen adatvédelmi hatásvizsgálatot, emellett segítséget kell nyújtania az érdekelteknek a módszerekkel kapcsolatosan, a kockázatértékelés színvonalának és a fennmaradó kockázat elfogadhatóságának felmérésében, valamint az adatkezelő körülményeivel kapcsolatos konkrét ismeretek fejlesztésében;
- ha kijelölnek információbiztonsági igazgatót, akkor neki, illetve az informatikai szervezeti egységnek segítenie kell az adatkezelőt, emellett a biztonsági és működési igényektől függően javasolhatja adatvédelmi hatásvizsgálat elvégzését valamely konkrét adatkezelési műveletre vonatkozóan.

c) Milyen módszerrel kell elvégezni az adatvédelmi hatásvizsgálatot? A módszerek különbözőek, de a szempontok azonosak.

[24] *A magánélet védelmére vonatkozó hatásvizsgálat európai uniós keretével kapcsolatos ajánlások (Recommendations for a privacy impact assessment framework for the European Union), D3. leszállítandó anyag:*
http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Az általános adatvédelmi rendelet meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit (a 35. cikk (7) bekezdése, valamint a (84) és a (90) preambulumbekezdés):

- „*a tervezett adatkezelési műveletek […] [leírása] és az adatkezelés céljainak [ismertetése]*”;
- „*az [adatkezelés] szükségességi és arányossági [vizsgálata]*”;
- „*az érintett jogait és szabadságait érintő kockázatok [vizsgálata]*”;
- az alábbiakat „*célzó intézkedések”*:
    - „*a kockázatok [kezelése]*”*;*
    - „*az e rendelettel való összhang [igazolása]*”.

Az alábbi ábra az adatvédelmi hatásvizsgálat elvégzésének általános, ismétlődő folyamatát szemlélteti[25]:

A magatartási kódex (40. cikk) betartását figyelembe kell venni (a 35. cikk (8) bekezdése) az adatkezelési művelet hatásának értékelése során. Ez hasznos lehet annak alátámasztása szempontjából, hogy megfelelő intézkedéseket választottak ki vagy hajtottak végre, feltéve, ha a magatartási kódex az adatkezelési művelet szempontjából megfelelő. Az adatkezelők és az adatfeldolgozók által végrehajtott adatkezelési műveletek általános adatvédelmi rendelettel való összhangját igazoló tanúsítványokat, bélyegzőket és jelöléseket (42. cikk), valamint a kötelező erejű vállalati szabályokat szintén figyelembe kell venni.

Az általános adatvédelmi rendeletben rögzített lényeges előírások összessége széles, általános keretet nyújt az adatvédelmi hatásvizsgálat kialakításához és elvégzéséhez. Az adatvédelmi hatásvizsgálat

[25] Hangsúlyozandó, hogy az itt bemutatott folyamat ismétlődő: a gyakorlatban valószínűleg mindegyik szakaszát többször el kell végezni az adatvédelmi hatásvizsgálat lezárulta előtt.

gyakorlati végrehajtása az általános adatvédelmi rendeletben foglalt előírásoktól függ, amelyeket részletesebb gyakorlati útmutatások egészíthetnek ki. Az adatvédelmi hatásvizsgálat ezért a mérethez igazítható. Ez azt jelenti, hogy még a kis adatkezelők is kialakíthatnak és elvégezhetnek a saját adatkezelési műveleteikhez igazodó adatvédelmi hatásvizsgálatot.

Az általános adatvédelmi rendelet (90) preambulumbekezdése az adatvédelmi hatásvizsgálat több olyan elemét is megjelöli, amely egybevág jól körülhatárolt kockázatkezelési elemekkel (lásd például az ISO 31000 szabványt[26]). A kockázatkezelés szempontjából az adatvédelmi hatásvizsgálat célja, hogy a természetes személyek jogait és szabadságait érintő "kockázatokat kezelje" a következő eljárások felhasználásával:

- a körülmények meghatározása: „*az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve*";
- a kockázatok értékelése: „*felmérje a magas kockázat különös valószínűségét és súlyosságát*";
- a kockázatok orvoslása: „*az említett kockázat mérséklését*", „*a személyes adatok védelmét*" és „*az e rendeletnek való megfelelés bizonyítását*".

Megjegyzés: az általános adatvédelmi rendelet szerinti adatvédelmi hatásvizsgálat az érintettek jogait érintő kockázatok kezelésére szolgál, így az ő szemszögükből készül, ahogy az bizonyos szakterületeken megfigyelhető (például társadalmi biztonság). Ugyanakkor más szakterületeken (például információbiztonság) a szervezet áll a középpontban.

Az általános adatvédelmi rendelet rugalmasságot biztosít az adatkezelők számára abból a szempontból, hogy saját belátásuk szerint határozhatják meg az adatvédelmi hatásvizsgálat pontos felépítését és formáját, így igazodhatnak a már meglévő munkamódszereikhez. Az Európai Unióban és világszerte is többféle bevett eljárás létezik, amely figyelembe veszi a (90) preambulumbekezdésben felsorolt elemeket. Bármilyen formát ölt is az adatvédelmi hatásvizsgálat, a kockázatok valódi értékelésére kell irányulnia, mivel így az adatkezelők intézkedéseket hozhatnak azok kezelésére.

Különböző módszerek (az adatvédelmi és a magánélet védelmére vonatkozó hatásvizsgálat módszereire néhány példa az 1. mellékletben olvasható) használhatók fel az általános adatvédelmi rendeletben rögzített alapvető előírások végrehajtásának elősegítésére. Közös szempontok (lásd a 2. mellékletet) készültek azért, hogy lehetővé váljon ezeknek a különböző megközelítéseknek az alkalmazása, egyúttal pedig az adatkezelők is be tudják tartani az általános adatvédelmi rendeletet. Ezek a szempontok tisztázzák a rendelet alapvető előírásait, ugyanakkor elegendő mozgásteret biztosítanak a különböző formában történő végrehajtáshoz. A szempontok alapján alátámasztható, hogy egy adott adatvédelmi hatásvizsgálati módszer megfelel az általános adatvédelmi rendeletben rögzített előírásoknak. **Az adatkezelő választhatja ki a módszert, a kiválasztott módszernek azonban meg kell felelnie a 2. mellékletben megadott szempontokkal**.

A 29. cikk szerinti adatvédelmi munkacsoport ágazatspecifikus adatvédelmi hatásvizsgálati keretek kidolgozását szorgalmazza. Ennek oka, hogy a keretek ezáltal az egyedi ágazati ismeretekre épülhetnek, így az adatvédelmi hatásvizsgálatok az adott jellegű adatkezelési művelet sajátosságaira összpontosíthatnak (például bizonyos adatfajták, vállalati eszközök, lehetséges hatások, veszélyek,

[26] A kockázatkezelési eljárások: kommunikáció és egyeztetés, a körülmények meghatározása, kockázatértékelés, a kockázatok orvoslása, nyomon követése és felülvizsgálata (lásd a fogalommeghatározásokat és a tartalomjegyzéket az ISO 31000 szabvány előnézetében: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

intézkedések). Ennek értelmében az adatvédelmi hatásvizsgálatok az adott gazdasági ágazatban, illetve bizonyos technológiák használatakor vagy meghatározott jellegű adatkezelési műveletek végrehajtásakor felmerülő kérdésekkel foglalkozhatnak.

Végül pedig „*[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*” (a 35. cikk (11) bekezdése[27]).

d) Kötelező-e nyilvánosságra hozni az adatvédelmi hatásvizsgálatokat? Nem, de összefoglalók közzétételével növelhető a bizalom, a teljes adatvédelmi hatásvizsgálatról pedig előzetes egyeztetés esetén vagy az adatvédelmi hatóság kérésére tájékoztatni kell a felügyeleti hatóságot.

Az általános adatvédelmi rendelet nem követeli meg az adatvédelmi hatásvizsgálat nyilvánosságra hozatalát, erről az adatkezelő saját belátása szerint dönt. Az adatkezelőknek azonban érdemes mérlegelniük a legalább a hatásvizsgálat egyes részeinek közzétételét, például összefoglaló vagy következtetések formájában.

Ezáltal növelhető az adatkezelő adatkezelési műveletei iránti bizalom, valamint kifejezésre juttatható az elszámoltathatóság és az átláthatóság. Különösen akkor érdemes nyilvánosságra hozni az adatvédelmi hatásvizsgálatot, ha az adatkezelési művelet a nyilvánosságot érinti. Ez különösen akkor fordulhat elő, ha közhatalmi szerv végez adatvédelmi hatásvizsgálatot.

A nyilvánosságra hozott adatvédelmi hatásvizsgálatnak nem kell tartalmaznia a vizsgálat teljes anyagát, különösen akkor, ha az adatvédelmi hatásvizsgálat konkrét információkat tartalmazhat az adatkezelőt érintő biztonsági kockázatokról, illetve üzleti titkokat vagy bizalmas üzleti adatokat fedhet fel. Ilyen helyzetekben elegendő, ha a közzétett változat mindössze az adatvédelmi hatásvizsgálat főbb megállapításainak összefoglalójából vagy csak az adatvédelmi hatásvizsgálat elvégzéséről szóló közleményből áll.

ezenkívül abban az esetben, ha az adatvédelmi hatásvizsgálat jelentős fennmaradó kockázatokat tár fel, az adatkezelő köteles az adatkezeléssel kapcsolatos előzetes konzultáció céljából a felügyeleti hatósághoz fordulni (a 36. cikk (1) bekezdése). A konzultáció keretében az adatvédelmi hatásvizsgálatot teljes egészében közölni kell (a 36. cikk (3) bekezdésének e) pontja). A felügyeleti hatóság tanácsot adhat[28], és az egyes tagállamokban a közokiratokba való betekintésre vonatkozó alapelvekre figyelemmel nem sért meg üzleti titkokat, és nem fed fel biztonsági sebezhetőségeket.

E. <u>Mikor kell konzultálni a felügyeleti hatósággal? Amikor jelentősek a fennmaradó kockázatok.</u>

A fenti magyarázat szerint:

- akkor van szükség adatvédelmi hatásvizsgálatra, ha az adatkezelési művelet „*valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*” (a 35. cikk (1) bekezdése; lásd a III. fejezet B. szakaszának a) pontját). Példaként

[27] A 35. cikk (10) bekezdése kifejezetten csak a 35. cikk (1)–(7) bekezdésének alkalmazását zárja ki.

[28] Az adatkezelőnek írásban adott tanácsra a 36. cikk (2) bekezdése szerint csak akkor van szükség, ha a felügyeleti hatóság véleménye szerint a tervezett adatkezelés nincs összhangban a rendelettel.

említhető a nagyszámú egészségügyi adat kezelése, amelyről valószínűsíthető, hogy magas kockázattal jár, ezért adatvédelmi hatásvizsgálatot igényel;

- ezt követően az adatkezelő feladata, hogy értékelje az érintettek jogait és szabadságait érintő kockázatokat, és megállapítsa az e kockázatok elfogadható szintre való csökkentésére irányuló intézkedéseket[29], és igazolja a rendelettel való összhangot (a 35. cikk (7) bekezdése; lásd a III. fejezet C. szakaszának c) pontját). Példaként felhozható, hogy személyes adatok laptopon való tárolása estén a meglévő politikák (értesítés, hozzájárulás, betekintési jog, kifogásolási jog stb.) mellett további megfelelő technikai és szervezési jellegű biztonsági intézkedések (a lemezek tényleges teljes titkosítása, robusztus kulcskezelés, megfelelő hozzáférés-vezérlés, védett biztonsági másolatok készítése stb.) hajthatók végre.

A fenti, laptopról szóló példánál maradva, annak megállapítása esetén, hogy az adatkezelő kellő mértékben csökkentette a kockázatokat, továbbá a 36. cikk (1) bekezdésének, valamint a (84) és (94) preambulumbekezdésnek az értelmezését követően az adatkezelés a felügyeleti hatósággal való konzultáció nélkül folytatódhat. Az adatkezelőnek azokban az esetekben kell konzultálnia a felügyeleti hatósággal, amikor nem tudja kellő mértékben csökkenteni a feltárt kockázatokat (tehát a fennmaradó kockázatok továbbra is jelentősek).

Az elfogadhatatlanul magas fennmaradó kockázatra példa, ha az érintettek olyan jelentős vagy akár visszafordíthatatlan következményekkel szembesülnek, amelyekkel nem tudnak leküzdeni (például adatokhoz való jogosulatlan hozzáférés, amely az érintettek életét fenyegető veszélyt, elbocsátást vagy pénzügyi nehézséget eredményez), és/vagy ha egyértelműnek tűnik, hogy kockázat be fog következni (például azért, mert az adatok megosztásának, felhasználásának vagy terjesztésének módja miatt nem lehet csökkenteni az adatokhoz hozzáférő személyek számát, vagy a közismert sebezhetőségre nem készül javítókészlet).

Amennyiben az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére (tehát a fennmaradó kockázatok továbbra is jelentősek), akkor kötelező konzultálni a felügyeleti hatósággal[30].

Ezenkívül az adatkezelőnek minden olyan esetben konzultálnia kell a felügyeleti hatósággal, amikor a tagállami jog előírja, hogy az adatkezelők konzultáljanak a felügyeleti hatósággal, illetve 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 36. cikk (5) bekezdése).

Ugyanakkor leszögezendő, hogy az adatvédelmi hatásvizsgálat iratainak megőrzésére és az adatvédelmi hatásvizsgálat kellő időben történő aktualizálására vonatkozó kötelezettségek attól függetlenül fennállnak, hogy a fennmaradó kockázatokra tekintettel kötelező-e konzultálni a felügyeleti hatósággal.

---

[29] Az Európai Adatvédelmi Testület és a felügyeleti hatóságok által már megfogalmazott útmutatásoknak, valamint a 35. cikk (1) bekezdése szerint a technika állásának és a végrehajtás költségeinek figyelembevételével együtt.

[30] Megjegyzés: "*a személyes adatok álnevesítését és titkosítását*" (valamint az adattakarékosságot, a felügyeleti mechanizmusokat stb.) nem feltétlenül lehet megfelelő intézkedéseknek tekinteni. Csak példaként szolgálnak. A megfelelő intézkedéseket az egyes feldolgozási műveletekre jellemző körülményektől és kockázatoktól függően kell megállapítani.

IV. Következtetések és ajánlások

Az adatvédelmi hatásvizsgálatok hasznosak a tekintetben, hogy segítségükkel az adatkezelők az általános adatvédelmi rendeletnek megfelelő adatkezelési rendszereket vezethetnek be, az adatkezelési műveletek bizonyos fajtái esetében pedig kötelező lehet elvégezni őket. Méretezhetőek, és többféle formában megvalósíthatók, ugyanakkor az általános adatvédelmi rendelet meghatározza az eredményes adatvédelmi hatásvizsgálatra vonatkozó alapvető követelményeket. Az adatkezelőknek hasznos és pozitív tevékenységnek kellene tartaniuk az adatvédelmi hatásvizsgálatot, amely segítséget nyújt a jogszabályok betartásához.

A 24. cikk (1) bekezdése állapítja meg az adatkezelők alapvető felelősségét az általános adatvédelmi rendelet betartását illetően: „*[a]z 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*”.

Az adatvédelmi hatásvizsgálat a rendelet betartása szempontjából elengedhetetlen, ha az adatkezelő magas kockázatú adatkezelést tervez vagy végez. Ez azt jelenti, hogy az adatkezelőknek az e dokumentumban meghatározott szempontok alapján kell megállapítaniuk, hogy szükséges-e adatvédelmi hatásvizsgálatot végezni. A belső adatkezelői politika az általános adatvédelmi rendelet jogi előírásain túlmutatva kibővítheti ezt a felsorolást. Ennek eredményeképpen erősödhet a bizalom az érintettek részéről az adatkezelők iránt.

Ha valószínűsíthetően magas kockázattal járó adatkezelést tervez, az adatkezelő köteles:

- olyan adatvédelmi hatásvizsgálati módszert (példák az 1. mellékletben) választani, amely megfelel a 2. mellékletben felsorolt szempontoknak, vagy olyan módszeres adatvédelmi hatásvizsgálati eljárást meghatározni és végrehajtani, amely:
  - összhangban van a 2. mellékletben szereplő szempontokkal;
  - a belső eljárásoknak, körülményeknek és kultúrának megfelelően beépül a meglévő tervezési, fejlesztési, módosítási, kockázati és működési felülvizsgálati eljárásokba;
  - a megfelelő érdekeltek részvételével zajlik, és egyértelműen meghatározza felelősségi körüket (adatkezelő, adatvédelmi tisztviselő, érintettek vagy képviselőik, vállalkozás, műszaki szolgálatok, adatfeldolgozók, információbiztonsági tisztviselő, stb.);
- kérésre az adatvédelmi hatásvizsgálatról szóló jelentést benyújtani az illetékes felügyeleti hatóságnak;
- konzultálni a felügyeleti hatósággal, ha nem sikerült megfelelő intézkedéseket hozni a magas kockázatok csökkentésére;
- rendszeresen, de legalább az adatkezelési művelettel járó kockázat megváltozása esetén felülvizsgálni az adatvédelmi hatásvizsgálatot és a tárgyát képező adatkezelést;
- írásba foglalni a hozott döntéseket.

1. melléklet – Példák uniós adatvédelmi hatásvizsgálati keretekre

Az általános adatvédelmi rendelet nem határozza meg, melyik adatvédelmi hatásvizsgálati eljárást kell követni. Ehelyett lehetőséget biztosít az adatkezelők számára, hogy olyan keretet vezessenek be, amely kiegészíti már meglévő munkamódszereiket, feltéve, ha figyelembe veszi a 35. cikk (7) bekezdésében ismertetett elemeket. Ez a keret az adatkezelő egyedi igényeihez igazítható, de az adott ágazaton belül egységes is lehet. A már közzétett, az uniós adatvédelmi hatóságok által kidolgozott vagy uniós ágazatspecifikus keretek közé tartoznak egyebek mellett a következők:

Példa uniós általános keretekre:

- Németország: Szabványos adatvédelmi modell, V.1.0 – próbaverzió, 2016[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- Spanyolország: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- Franciaország: *A magánélet védelmére vonatkozó hatásvizsgálat*, Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798
- Egyesült Királyság: *A magánélet védelmére vonatkozó hatásvizsgálat elvégzésének gyakorlati kódexe* (Conducting privacy impact assessments code of practice), az információs biztos hivatala (Information Commissioner's Office, ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Példák uniós ágazatspecifikus keretekre:

- Az RFID-alkalmazásokra vonatkozó magánélet- és adatvédelmi hatásvizsgálati keret[32]. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- az intelligens energiahálózatok és fogyasztásmérő rendszerek adatvédelmi hatásvizsgálatára vonatkozó sablon[33] http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

---

[31] Egyhangúlag és jóváhagyólag (Bajorország tartózkodása mellett) elfogadta a szövetségi állam és a tartományok független adatvédelmi hatóságainak 92. konferenciája 2016. november 9–10-én Kühlungsbornban.

[32] Lásd még:

- A Bizottság ajánlása (2009. május 12.) a magánélet- és adatvédelmi alapelveknek a rádiófrekvenciás azonosítás által támogatott alkalmazások területén történő alkalmazásáról. https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- 9/2011. számú vélemény az RFID-alkalmazásokra vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretről szóló, felülvizsgált ágazati javaslatról. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] Lásd még az intelligens hálózatokkal foglalkozó bizottsági munkacsoport 2. szakértői csoportja által elkészített, az intelligens hálózatokra és az intelligens fogyasztásmérő rendszerekre vonatkozó adatvédelmi hatásvizsgálati sablonról szóló 07/2013. számú véleményt. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

Nemzetközi szabvány (ISO/IEC 29134[34]) is iránymutatást fog nyújtani az adatvédelmi hatásvizsgálat elvégzéséhez alkalmazott módszerekről.

[34] ISO/IEC 29134 (projekt) *Informatika – Biztonságtechnika – A magánélet védelmére vonatkozó hatásvizsgálat – Iránymutatások* (Information technology – Security techniques – Privacy impact assessment – Guidelines), a Nemzetközi Szabványügyi Szervezet (ISO).

2. melléklet – Az elfogadható adatvédelmi hatásvizsgálatra vonatkozó szempontok

A 29. cikk szerinti adatvédelmi munkacsoport a következő szempontok figyelembevételét javasolja az adatkezelők számára annak értékeléséhez, hogy az adatvédelmi hatásvizsgálat vagy az adatvédelmi hatásvizsgálathoz használt módszer kellően átfogó-e ahhoz, hogy összhangban legyen az általános adatvédelmi rendelettel:

- ☐ módszeres leírás készült az adatfeldolgozásról (a 35. cikk (7) bekezdésének a) pontja):
  - ☐ figyelembe vették az adatkezelés jellegét, hatókörét, körülményeit és céljait ((90) preambulumbekezdés);
  - ☐ a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát rögzítették;
  - ☐ funkcionális leírás készült az adatkezelési műveletről;
  - ☐ a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) azonosították;
  - ☐ figyelembe vették a jóváhagyott magatartási kódexek előírásainak teljesítését (a 35. cikk (8) bekezdése);
- ☐ értékelték a szükségességet és az arányosságot (a 35. cikk (7) bekezdésének b) pontja):
  - ☐ a rendelet betartására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés), figyelembe véve az alábbiakat:
    - ☐ az adatkezelés arányosságát és szükségességét előmozdító intézkedések a következők alapján:
      - ☐ meghatározott, kifejezett és jogos cél(ok) (az 5. cikk (1) bekezdésének b) pontja);
      - ☐ az adatkezelés jogszerűsége (6. cikk);
      - ☐ megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak (az 5. cikk (1) bekezdésének c) pontja);
      - ☐ korlátozott tárolási időtartam (az 5. cikk (1) bekezdésének e) pontja);
    - ☐ az érintettek jogait támogató intézkedések:
      - ☐ az érintetteknek nyújtott tájékoztatás (12., 13. és 14. cikk);
      - ☐ betekintési jog és az adathordozhatósághoz való jog (15. és 20. cikk);
      - ☐ a helyesbítéshez és a törléshez való jog (16., 17. és 19. cikk);
      - ☐ kifogásolási jog és az adatkezelés korlátozásához való jog (18., 19. és 21. cikk);
      - ☐ az feldolgozókkal fennálló kapcsolatok (28. cikk);
      - ☐ a nemzetközi adattovábbításhoz kapcsolódó garanciák (V. fejezet);
      - ☐ előzetes konzultáció (36. cikk);
- ☐ az érintett jogait és szabadságait érintő kockázatokat kezelik (a 35. cikk (7) bekezdésének c) pontja):
  - ☐ a kockázatok forrását, jellegét, egyediségét és súlyosságát felmérték (vö. (84) preambulumbekezdés) vagy konkrétabban mindegyik kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében az érintettek szemszögéből:
    - ☐ figyelembe vették a kockázatforrásokat ((90) preambulumbekezdés);
    - ☐ az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat beazonosították olyan eseményekre vonatkozóan, mint a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése;
    - ☐ az esetleg jogosulatlan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket beazonosították;
    - ☐ felmérték a valószínűséget és a súlyosságot ((90) preambulumbekezdés);
  - ☐ az említett kockázatok orvoslására irányuló intézkedéseket meghatározták (a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés);
- ☐ az érdekelteket bevonták:

- ☐ kikérték az adatvédelmi tisztviselő tanácsát (a 35. cikk (2) bekezdése);
- ☐ adott esetben kikérték az érintettek véleményét (a 35. cikk (9) bekezdése).