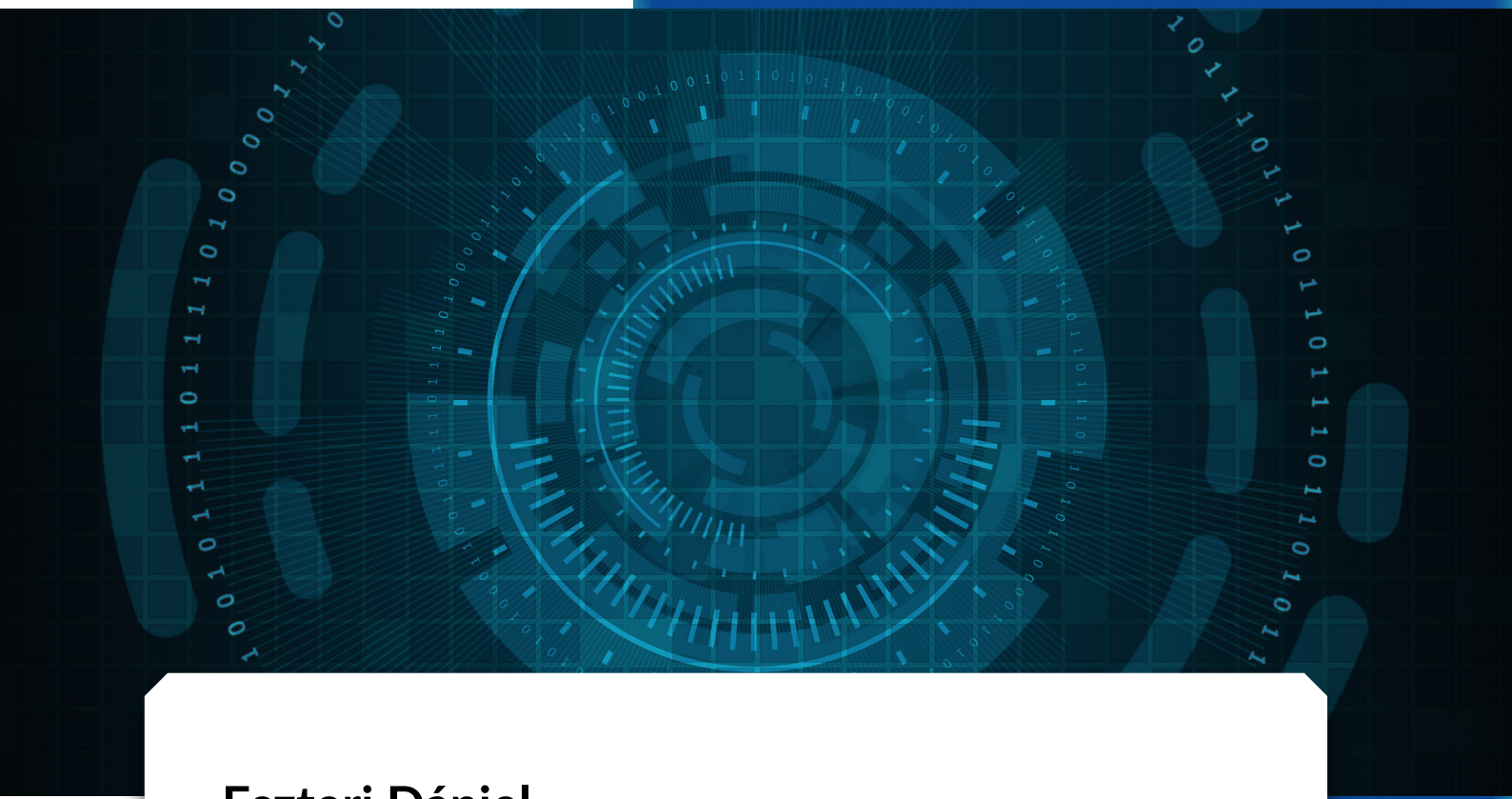
Az adatvédelmi hatásvizsgálat és az előzetes konzultáció



Eszteri Dániel

NEMZETI KÖZSZOLGÁLATI EGYETEM
BUDAPEST

Szerző:
© Eszteri Dániel

Szakmai lektor:
Péterfalvi Attila

Olvasószerkesztő:
Császár-Biró Anna

A kézirat lezárásának dátuma:
2019. november 21.

Kiadja:
© NKE, 2019

Felelős kiadó:
Prof. Dr. Kis Norbert
rektorhelyettes

TARTALOM

1. Az adatvédelmi hatásvizsgálat fogalma és előzményei 5

1.1 Az adatvédelmi hatásvizsgálat fogalma 5
1.2 Az adatvédelmi hatásvizsgálat történeti előzményei 6
1.3 Az adatvédelmi hatásvizsgálat előnyei. 6

2. Az adatvédelmi hatásvizsgálat elvégzésének kötelezettsége 7

2.1 Mely esetekben szükséges lefolytatni az adatvédelmi hatásvizsgálatot? . . . 7
2.2 Általános szempontok a magas kockázatú adatkezelések beazonosításához. 9
2.3 Példák az adatvédelmi hatásvizsgálat lefolytatásának szükségességével kapcsolatban 10
2.4 Mikor nincs szükség adatvédelmi hatásvizsgálat lefolytatására? 12
2.5 A már folyamatban lévő adatkezelési műveletekkel kapcsolatos adatvédelmi hatásvizsgálat szükségessége. 13
2.6 Az adatvédelmi hatásvizsgálat lefolytatásának ideje 14
2.7 Az adatvédelmi hatásvizsgálat lefolytatásának felelőse 14

3. Az adatvédelmi hatásvizsgálat tartalma és szakaszai 17

3.1 Az adatvédelmi hatásvizsgálat főbb szakaszai 17
3.2 Első szakasz: előkészületi szakasz. 17
3.3 Második szakasz: hatásvizsgálati elemzés 18
3.4 Harmadik szakasz: a biztonsági intézkedések alkalmazása 18
3.5 Összefoglaló dokumentáció készítése, újbóli ellenőrzés szükségessége . . 19
3.6 Az adatvédelmi hatásvizsgálat nyilvánossága 20

4. Az adatvédelmi hatásvizsgálat lefolytatásának módszertana és eszközei . . . 21

4.1 Általános módszertan. 21
4.2 A hatásvizsgálat során lefolytatandó kockázatelemzés módszertana és néhány alapfogalom 22
4.3 Az adatkezelés során felmerülő kockázatok felmérésének módszertana . . 24
4.4 A kockázatok csökkentésére szolgáló biztonsági intézkedések kategóriái . 26
4.5 Példa kockázatelemzés lefolytatására egy konkrét eseten keresztül. 30
4.6 A francia adatvédelmi hatóság által közzétett ingyenes hatásvizsgálati szoftver. 34

5. A Nemzeti Adatvédelmi és Információszabadság Hatóság szerepe az adatvédelmi hatásvizsgálatokkal kapcsolatosan 35

5.1 A felügyeleti hatóság bírságolási jogköre. 35
5.2 A hatásvizsgálattal kapcsolatos hatósági jegyzékek (fekete és fehér listák) elfogadása és nyilvánosságra hozatala. 35
5.3 A NAIH által összeállított kötelező hatásvizsgálati jegyzék elemei. 37

6. Az előzetes konzultáció a felügyeleti hatósággal 42
6.1 Előzetes konzultáció a felügyeleti hatósággal az adatkezelő részéről 42
6.2 Előzetes konzultáció a felügyeleti hatósággal
a jogszabályok előkészítése során 43
6.3 A jogszabály előkészítése során készített adatvédelmi
hatásvizsgálat tartalmi kritériumai 44

7. Irodalomjegyzék 46

1. AZ ADATVÉDELMI HATÁSVIZSGÁLAT FOGALMA ÉS ELŐZMÉNYEI

1.1. Az adatvédelmi hatásvizsgálat fogalma

Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelyet az adatkezelő folytat le egy új, még meg nem kezdett – tulajdonképpen még tervezési szakaszban lévő – adatkezelés megkezdése előtt. A hatásvizsgálat célja, hogy az adatkezelő még az új adatkezelés megkezdése előtt felmérje azt, hogy az meg fog-e felelni az adatvédelmi jog előírásainak.

Az adatvédelmi hatásvizsgálat az érintettek jogait érintő kockázatok kezelésére szolgál, így az ő szemszögükből készül, ahogy az bizonyos más szakterületeken is megfigyelhető (például társadalmi biztonság). Ugyanakkor más szakterületeken (például információbiztonság) a szervezet áll a középpontban.[1] Az adatvédelmi hatásvizsgálatot lefolytató adatkezelőnek tehát az eljárás során gyakorlatilag bele kell helyezkednie az érintettek (adatalanyok) helyzetébe, úgy kell eljárnia, mintha az adatkezelést az ő szemszögükből vizsgálná, és nem az adatkezelést lefolytató szervezet üzleti, gazdasági vagy más céljait kell elsősorban szem előtt tartania.

Az adatvédelmi hatásvizsgálat lényege tehát az adatkezelés előzetes kontrollja. Ennek keretében az adatkezelő feltárja az érintett személyek szemszögéből az adatkezeléssel járó kockázatokat és értékeli a kockázatok mérséklésére teendő intézkedéseket. Az adatvédelmi hatásvizsgálat során az adatkezelő feladata 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 a GDPR előírásainak teljesítését könnyítik meg az adatkezelők számára, de a betartása érdekében hozott megfelelő intézkedések végrehajtásának bizonyítását is. A 29-es Munkacsoport vonatkozó iránymutatása úgy határozza meg az adatvédelmi hatásvizsgálat fogalmát, mint a GDPR betartásának elérésére és bizonyítására szolgáló eljárást.[2]

Maga a GDPR szövege hivatalosan nem határozza meg külön az adatvédelmi hatásvizsgálat fogalmát, de minimális tartalmát rögzíti annak 35. cikk (7) bekezdésében. A tartalmi elemek részletes elemzésére a tananyag későbbi részeiben kerül sor.

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

---

1 WP29, 2017.

2 WP29, 2017.

1.2. Az adatvédelmi hatásvizsgálat történeti előzményei

A jogirodalomban először a privacy-hatásvizsgálat (*Privacy Impact Assessment*, rövidítve: PIA) fogalma terjedt el, amely az adatvédelmi hatásvizsgálat előképének tekinthető. Az elnevezésbeli különbség egyebek között az általános személyiségvédelem amerikai és európai fejlődési modelljei közötti eltérésben gyökerezik. Míg az Amerikai Egyesült Államokban a személyiségi jogi védelem a magánszférához való jog *(right to privacy)* keretein belül teljesedett ki, addig Európában a titokszféra védelme, majd a személyes adatok védelme vált annak meghatározó elemévé.[3]

A privacy-hatásvizsgálat gyökerei jellemzően az angolszász jogrendszerekben (például az Amerikai Egyesült Államokban, Ausztráliában, Új-Zélandon, Kanadában, az Egyesült Királyságban) találhatók; kialakulásuk az 1990-es évek derekára tehető.[4]

A privacy-hatásvizsgálathoz kapcsolódóan nem létezik egységes módszertan, továbbá az erre vonatkozó jogforrások szintjei között is tapasztalhatóak eltérések: míg egyes országok (például Kanada, Új-Zéland, Amerikai Egyesült Államok) hard law-eszközökkel szabályozzák, máshol a soft law-eszközök a meghatározóak.[5]

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 az általános adatvédelmi rendeletben szabályozott adatvédelmi hatásvizsgálat előtt részletesen szabályozásra kerültek. Mind az angol,[6] mind pedig a francia[7] adatvédelmi hatóságok által kidolgozott vizsgálati eljárás egy checklist (ellenőrző lista) alapú eljárás. Ezen checklistalapú vizsgálati eljárások 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.[8]

1.3. Az adatvédelmi hatásvizsgálat előnyei

Az adatvédelmi 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, az érintettekre jelentett negatív hatások elkerülése vagy csökkentése.[9]

A vonatkozó szakirodalmi álláspontok szerint a hatásvizsgálat nem csupán egy eszköz, hanem egy olyan eljárás, amelyet az adatkezelést integráló projekt legelején, annak megkezdését megelőzően célszerű és kell 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 magában a hatásvizsgálati eljárásban külső szereplők is részt vesznek, hiszen így az adatkezelők számára független ajánlások is segíthetnek a kockázatok kezelésében, csökkentésében.[10]

---

3 Balogh et. al., 2014.
4 Wright – De Hert, 2012.
5 Balogh et. al., 2014.
6 ICO, 2014.
7 CNIL, 2015.
8 Péterfalvi et.al., 2018.
9 Wright – De Hert, 2012.
10 Wright – De Hert, 2012.

2. AZ ADATVÉDELMI HATÁSVIZSGÁLAT ELVÉGZÉSÉNEK KÖTELEZETTSÉGE

2.1. Mely esetekben szükséges lefolytatni az adatvédelmi hatásvizsgálatot?

Az uniós jogforrások közül a rendelet egy olyan jogalkotási aktus, amely az Unió területén közvetlenül és teljes egészében alkalmazandó.[11] A GDPR egy ilyen jogszabály, tehát azt 2018. május 25. napjától alkalmazni kell, és az teljes egészében kötelező és közvetlenül alkalmazandó az EU valamennyi tagállamában.[12] A GDPR előírásai (tehát az adatvédelmi hatásvizsgálatra vonatkozó részek is) egységesen és közvetlenül alkalmazandóak az Európai Unió egész területén. Azt, hogy a GDPR mely adatkezelések esetén teszi kötelező az előzetes hatásvizsgálat elvégzését, az alábbiakban tekintjük át.

A GDPR 35. cikkében találhatóak az adatvédelmi hatásvizsgálattal kapcsolatos rendelkezések. A 35. cikk (1) bekezdése az alábbiak szerint foglalja össze a hatásvizsgálat lefolytatásának lényegét:

35. cikk (1) bekezdés: „Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek."

A GDPR fenti előírásai alapján nem mindegyik adatkezelési művelet megkezdése előtt kötelező adatvédelmi hatásvizsgálatot végezni. Csak akkor van szükség adatvédelmi hatásvizsgálatra, ha az adatkezelés „*valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve*".[13] A GDPR tehát csak az úgy nevezett *magas kockázatú* adatkezelések esetén írja elő a hatásvizsgálat lefolytatásának kötelezettségét. A „kockázat" egyébként egy olyan kulcsfogalom, amely nem csak a hatásvizsgálattal kapcsolatban, hanem más részeiben is visszaköszön a GDPR-nak.

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.[14]

Az adatkezelési kockázatok azonosítása tehát kulcskérdés. Felmerül továbbá a kérdés, hogy adatvédelmi szempontból tulajdonképpen mit is tekintünk, tekinthetünk kockázatnak, és melyek azok az adatkezelések, amelyek kockázattal járnak a személyes adatok kezelése szempontjából. E tekintetben a GDPR preambulum bekezdései, valamint a 35. cikkben foglaltak adnak iránymutatást az alábbiak szerint.

A GDPR (76) preamublumbekezdése szerint az érintett jogait és szabadságait érintő kockázat valószínűségét és súlyosságát az adatkezelés jellegének, hatókörének, körülményeinek és céljainak

---

11 Az Európai Unió működéséről szóló szerződés 288. cikke alapján.
12 GDPR 99. cikk (2) bekezdése alapján.
13 GDPR 35. cikk (1) bekezdés.
14 WP29, 2017.

függvényében kell meghatározni. Objektív értékelés alapján kell felmérni, hogy az adatkezelési műveletek kockázattal, illetve magas kockázattal járnak-e.

Az adatkezelőknek az adatvédelmi hatásvizsgálat elvégzésére vonatkozó kötelezettségét a személyes adatok kezeléséből eredő kockázatok megfelelő kezelésére vonatkozó általános kötelezettséggel összefüggésben kell értelmezni. Hangsúlyozandó, hogy a természetes személyek jogait és szabadságait érintő kockázatok csak akkor kezelhetők, ha rendszeresen beazonosítják, elemzik, felmérik, értékelik, orvosolják és felülvizsgálják őket. Az adatkezelők nem bújhatnak ki felelősségük alól azzal, hogy biztosításokat kötnek a kockázatokra.

A GDPR (75) preambulum bekezdése felsorolásszerűen rögzíti, hogy a természetes személyek jogait és szabadságait érintő, tehát adatvédelmi szempontból releváns kockázatok elsősorban miből származhatnak. A felsorolás egyébként nem kimerítő jellegű. Ezek szerint eredendően kockázatos a személyes adatok kezelése, ha az alábbi felsorolásban foglaltak jellemzőek rá:

- A (nem megfelelő) adatkezelés eredménye lehet fizikai, vagyoni, nem vagyoni kár.
- Abból hátrányos megkülönböztetés származhat.
- Abból személyazonosság lopás, vagy személyazonossággal való visszaélés következhet.
- Szakmai titoktartási kötelezettség által védett személyes adat bizalmas jellegének sérülése következhet be.
- Az álnevesítés engedély nélküli feloldása következhet be.
- Gazdasági vagy szociális hátrányt okozhat a (nem megfelelő) adatkezelés.
- Az érintettek az adatkezeléssel összefüggésben nem gyakorolhatják jogaikat.
- Az érintettek nem rendelkezhetnek saját személyes adataik felett.
- Olyan személyes adatok kezelése történik, amely faji vagy etnikai származásra vagy politikai véleményre, vallási, illetve világnézeti meggyőződésre, szakszervezeti tagságra utalnak (a személyes adatok különleges kategóriái).
- 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 viselkedés, tartózkodási hely vagy mozgás elemzésére és előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából (tkp. profilalkotásra kerül sor az adatokkal).

Az előbbi felsorolás nem mondja ki, hogy ezek a kategóriák eredendően magas kockázatú adatkezelést takarnak, csupán annyit, hogy kockázatosak. Az adatkezelőnek tehát a felsorolásban szereplő körülmények fennállása esetén még nem biztos, hogy mindenképpen el kell végeznie az adatkezelés megkezdése előtt a hatásvizsgálatot, mivel az csak a „magas kockázatú" adatkezeléseknél kötelező. Minden esetre, ha az adatkezelő a felsorolásban szereplő tényezőt is magában foglaló adatkezelést szeretné kialakítani, mindenképpen meg kell vizsgálnia, hogy nincs-e hatásvizsgálati kötelezettsége. Ilyen lehet például, hogy a fenti elemek mellett egy másik kockázatot növelő tényező is megvalósul, például nagyszámú személyes adat kezelése.

Némi segítségül szolgálhat a fentieken túl a magas kockázatú adatkezelések beazonosításához a GDPR 35. cikk (3) bekezdése, amely néhány példával szolgál azokra az esetekre, amikor az adatkezelési művelet *valószínűsíthetően magas kockázattal jár*.

- Az első példa **„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."**
- A másik esetkör, ha a GDPR **„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 kezelésére kerül sor."**

- Végül általánosságban hozza fel példaként a GDPR **„a nyilvános helyek nagymértékű, módszeres megfigyelését."**

A GDPR 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.[15]

Általánosságban tehát elmondhatjuk, hogy adatvédelmi hatásvizsgálatot az olyan adatkezelések megkezdése előtt kell elvégeznie az adatkezelőnek, amely magas kockázattal jár a természetes személyek jogaira és szabadságára nézve. Maga a GDPR azonban sajnos nem tartalmaz egy egyértelmű, taxatív felsorolást e magas kockázatú adatkezelésekkel kapcsolatban, csupán támpontokat ad és általános példákkal szolgál ilyen adatkezelésekre. A rendelet tehát elsősorban az adatkezelőkre telepíti a kötelezettséget annak megállapításával kapcsolatban, hogy vajon az általuk tervezett adatkezelés magas kockázattal jár-e és ezért hatásvizsgálati kötelezettség alá esik-e.

2.2. Általános szempontok a magas kockázatú adatkezelések beazonosításához

Az alábbiakban összesen kilenc olyan esetet sorolunk fel (a 29-es Munkacsoport kapcsolódó véleménye alapján), amelyek szinte minden esetben valószínűsíthetően magas kockázattal járó adatkezelést eredményeznek. Amennyiben az alábbi szempontok az adatkezelés során fennállnak, úgy az adatkezelés magas kockázatúnak minősül, így a hatásvizsgálat lefolytatása kötelező lesz:[16]

- Értékelési vagy pontozási rendszer használata, ideértve a profilozást és az előrejelzést is: Ilyen lehet, ha az adatkezelő munkahelyi teljesítményük, gazdasági helyzetük, egészségi állapotuk, személyes preferenciáik vagy érdeklődési körük, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzőik alapján pontozza, profilozza az érintetteket. Erre példaként említhető a pénzügyi vállalkozás, amely pénzmosás, hitelreferencia és a terrorizmus finanszírozása elleni, vagy csalásellenes adatbázist használ ügyfelei szűrésére. Másik példa lehet a biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje és előre jelezze a betegségekkel kapcsolatos és az egészségügyi kockázatokat.
- Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: Olyan adatkezelések tartoznak ide, amelyek 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.
- Módszeres megfigyelés: Érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés (jellemzően közterületeken vagy nyilvános helyeken történő megfigyelés például: bevásárlóközpontok, nyilvános könyvtárak kamerás megfigyelése).
- Különleges adatok vagy fokozottan személyes jellegű adatok kezelése: Idesorolhatóak a GDPR 9. cikke szerinti különleges adatok, továbbá a GDPR 10. cikkében meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok kezelése. 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.

[15] WP29, 2017.
[16] WP29, 2017.

- Nagy számban kezelt adatok: Annak megállapításakor, hogy az adatkezelés nagyszámú érintettet érint-e, 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 két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal.
- Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok: Például gyermekek, munkavállalók, idősek, mentális betegségben szenvedők adatai.
- Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: Példa lehet az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében. További példa a „dolgok internetét" használó alkalmazások használata, mivel az ilyen applikációk által gyűjtött adatok kezelése jelentős hatást gyakorolhat az egyének mindennapi életére és magánéletére. Az ilyen technológiák használatához újfajta adatgyűjtési és felhasználási formák kapcsolódhatnak, amelyek magas kockázattal járhatnak az egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének előre nem láthatóak a személyes és társadalmi következményei, ezért indokolják a hatásvizsgálat elvégzését.
- Azok az esetek, amikor az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják, vagy szolgáltatásokat vegyenek igénybe, vagy szerződést érvényesítsenek.[17] Erre példa, ha egy bank hitelreferencia-adatbázis alapján szűri ügyfeleit annak érdekében, hogy eldöntse, kínál-e nekik hitelt.

A hatásvizsgálat folyamatosan ismétlődő jellegét a 29-es Munkacsoport is kihangsúlyozta, így az adatkezelőknek a gyakorlatban valószínűleg a vizsgálat mindegyik szakaszát többször el kell végezniük a hatásvizsgálat lezárása 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.

Előfordulhat az is természetesen, hogy egy adatkezelési művelet ugyan megfelel a fent ismertetett szempontrendszer valamelyik pontjának, az adatkezelő azonban úgy ítéli meg, hogy nem folytat le hatásvizsgálatot, mivel az adatkezelés nem jár véleménye szerint „valószínűsíthetően magas kockázattal". Ilyenkor az adatkezelőnek viszont indokolnia és dokumentumokkal igazolnia kell az adatvédelmi hatásvizsgálat mellőzésének okait, és ezzel összefüggésben az adatvédelmi tisztviselő álláspontját is rögzítenie kell.

Azokra az esetekre, amikor nem egyértelmű, hogy szükség van-e adatvédelmi hatásvizsgálatra, a Munkacsoport azt ajánlja, hogy az adatkezelők inkább végezzék az adatvédelmi hatásvizsgálatot, mivel segítséget jelenthet számukra az adatvédelmi jogszabályok betartásában.[18]

2.3. Példák az adatvédelmi hatásvizsgálat lefolytatásának szükségességével kapcsolatban

Az alábbiakban olvasható példákon keresztül próbáljuk meg szemléltetni, hogyan kell felhasználni az előző pontban kifejtett szempontrendszert annak értékeléséhez, hogy az adott adatkezelési műveletre vonatkozóan el kell-e végezni adatvédelmi hatásvizsgálatot:

[17] GDPR 22. cikke és (91) preambulumbekezdése.
[18] WP29, 2017.

Példák adatkezelésre	Lényeges szempontok	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	Igen
Az alkalmazottai tevékenységeit módszeresen megfigyelő, így az alkalmazottak munkaállomását, internetes tevékenységeit stb. nyomon követő vállalkozás.	• Módszeres megfigyelés • Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok	Igen
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	Igen
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	Igen
Kutatási projektekben vagy klinikai vizsgálatokban részt vevő, kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, álnevesített, különleges személyes adatok tárolása archiválás céljából.	• Különleges adatok • Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok • Megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénye vagy szerződést érvényesítsenek	Igen
Egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adatainak feldolgozása.	• Különleges adatok vagy fokozottan személyes jellegű adatok • Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok • De! Kivételszabály a hatásvizsgálat kötelezettsége alól [(91) preambulumbekezdés]	Nem
A feliratkozóknak általános napi sajtószemle küldéséhez levelezőlistát használó internetes magazin.	• Nagy számban kezelt adatok • Nincs más kockázati tényező • Nem kezel érzékeny (például különleges, pénzügyi) személyes adatokat	Nem
A honlapon megtekintett vagy megvásárolt árucikkek alapján végzett profilalkotás révén veterán járművek alkatrészeire vonatkozó hirdetéseket megjelenítő e-kereskedelmi honlap.	• Értékelés vagy pontozás • Nincs más kockázatnövelő tényező • Nem kezel érzékeny (például különleges, pénzügyi) személyes adatokat	Nem

2.4. Mikor nincs szükség adatvédelmi hatásvizsgálat lefolytatására?

Léteznek olyan adatkezelések, amelyek esetén nincs szükség adatvédelmi hatásvizsgálat lefolytatására. Ezeket az eseteket is meghatározta a 29-es Munkacsoport az adatvédelmi hatásvizsgálatról szóló ajánlásában. A leírt esetekkel kapcsolatban, az előírt feltételek teljesülését elsősorban az adatkezelőnek kell ellenőriznie, mielőtt az adatvédelmi hatásvizsgálat lefolytatásának szükségességéről döntene.[19]

Általános előírás a GDPR-ban, hogy ha az adatkezelés valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és szabadságaira nézve, úgy az adatkezelőnek nem kell adatvédelmi hatásvizsgálatot lefolytatnia az adatkezelés megkezdése előtt. Ezen felül a 29-es Munkacsoport az alábbi eseteket emelte ki:

- 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. Ezt az iránymutatás a GDPR 35. cikk (1) bekezdéséből vezető le, amely konkrétan úgy fogalmaz, hogy **„olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek."** Igaz, a rendelet ezen megfogalmazása inkább a nagyon hasonló adatkezelések egyetlen hatásvizsgálat alá vonásának lehetőségére utal, azonban az iránymutatás szerint nincs akadálya annak sem, hogy a korábbi a hatásvizsgálatot egészítse ki az adatkezelő új nagyon hasonló adatkezelései műveletekkel, vagy szintén a korábbi hatásvizsgálat eredményeit használja fel.
- Ha az adatkezelési műveleteket a tagállam adatvédelmi felügyeleti hatósága meghatározott, azóta változatlan feltételek mellett 2018. május 25-e (a GDPR alkalmazandó válása) előtt ellenőrizte.
- Ha a hatásvizsgálat alá vonandó adatkezelési műveletre a jogalkotó jogalapot alkotott az uniós vagy a tagállami jogban [a 6. cikk (1) bekezdés c) vagy e) pontjának megfelelően], e jog pedig szabályozza az adott adatkezelési műveletet, **és** az említett jogalap megállapítása során már készített a jogszabály előkészítője adatvédelmi hatásvizsgálat. Kivétel lehet ez alól, ha a tagállam kimondta a jogszabályban, hogy az adatkezelési műveletet megelőzően az adatkezelőnek kell lefolytatnia a hatásvizsgálatot.
- Ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni [a 35. cikk (5) bekezdése]. Ez a jegyzék olyan adatkezelési tevékenységeket tartalmazhat, amelyek megfelelnek a felügyeleti hatóság által – különösen iránymutatások, egyedi határozatok vagy engedélyek, megfelelési szabályok stb. útján – megállapított feltételeknek. Ilyen esetekben 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 a GDPR által támasztott követelményeknek.

A GDPR explicit kimondja [a (91) preambulumbekezdésben] egyfajta értelmezésként azt is, hogy a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik. Ilyen esetekben sem kötelező az adatvédelmi hatásvizsgálat és azt nem kell lefolytatni.

[19] WP29, 2017.

2.5. A már folyamatban lévő adatkezelési műveletekkel kapcsolatos adatvédelmi hatásvizsgálat szükségessége

Adatvédelmi hatásvizsgálatot fő szabály szerint előzetesen, tehát az adatkezelés tényleges megkezdése előtt kell elvégeznie az adatkezelőnek. A hatásvizsgálati kötelezettség azonban bizonyos esetekben a már folyamatban lévő adatkezelésekkel kapcsolatban is fennáll.

Első ilyen eset, ha a már folyamatban lévő adatkezelés is magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és később utólag ezen adatkezelés esetében megváltoztak a kockázatok, figyelemmel az adatkezelés jellegére, hatókörére, körülményére és céljára.

Nincs szükség adatvédelmi hatásvizsgálatra olyan adatkezelési műveleteknél, amelyeket a GDPR alkalmazandóvá válása előtt (a 95/46/EK irányelv 20. cikke értelmében) a tagállami adatvédelmi felügyeleti hatóság vagy az adatvédelmi tisztviselő már korábban 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 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.

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 ezért folyamatosan felülvizsgálni, és rendszeresen újraértékelni.[20]

[20] WP29, 2017.

2.6. Az adatvédelmi hatásvizsgálat lefolytatásának ideje

Az adatvédelmi hatásvizsgálatot fő szabály szerint az adatkezelés megkezdését megelőzően kell elvégezni.[21] Ez a rendelkezés összhangban van és segít érvényre juttatni a beépített- és az alapértelmezett adatvédelem elveit is.[22] 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 lehet érv az adatvédelmi hatásvizsgálat elhalasztása vagy mellőzése mellett. Az adatvédelmi hatásvizsgálat egy folyamat, különösen akkor, ha az adatkezelési művelet dinamikus, és állandóan változik. Ezért vonatkozó iránymutatásában a 29-es Munkacsoport is kihangsúlyozza, hogy az adatvédelmi hatásvizsgálatot nem egyetlen alkalommal, hanem folyamatosan, periodikusan kell végezni.[23]

2.7. Az adatvédelmi hatásvizsgálat lefolytatásának felelőse

Az adatvédelmi hatásvizsgálat elvégzéséről az adatkezelőnek kell gondoskodnia [35. cikk (1) bekezdése]. Az adatvédelmi hatásvizsgálatot elvégezheti az adatkezelő szervezetén belül ezzel megbízott személy, de nincs akadálya annak sem, hogy egy külön ebből a célból megbízott külső személy folytassa azt le. Az adatkezelőt terheli azonban végső felelősség e feladat teljesítéséért.

A GDPR 35. cikk (2) bekezdése határozottan kimondja, hogy **„abban az esetben, ha rendelkezik adatvédelmi tisztviselővel, a hatásvizsgálat lefolytatása során az adatkezelőnek kötelező kikérnie az ő tanácsát is."** Az adatvédelmi tisztviselő tanácsának kikérése tehát semmilyen esetben sem kerülhető meg az adatkezelő részéről, ha ilyennel rendelkezik.

A tisztviselőtől kapott tanácsokat és az adatkezelő által hozott döntéseket írásba kell foglalni az adatvédelmi hatásvizsgálat során. Az adatvédelmi tisztviselőnek emellett nyomon kell követnie a hatásvizsgálat lefolytatását és kérésre szakmai tanácsot kell adnia az adatvédelmi hatásvizsgálatra vonatkozóan [lásd: az adatvédelmi tisztviselő e feladataival kapcsolatban a GDPR 39. cikk (1) bekezdésének c) pontját].

Ha az adatkezelést teljes egészében vagy részben adatfeldolgozó végzi, segítenie kell az adatkezelőt az adatvédelmi hatásvizsgálat lefolytatásában, és közölnie kell vele a hatásvizsgálat lefolytatása szempontjából szükséges információkat [lásd: az adatfeldolgozó e feladataival kapcsolatban a GDPR 28. cikk (3) bekezdésének f) pontját].

A GDPR 35. cikk (9) bekezdése a fentieken túl lehetőséget biztosít arra is, hogy az adatkezelő adott esetben kikérje az érintettek vagy képviselőik véleményét a hatásvizsgálat lefolytatásával kapcsolatban. Ezt az adatkezelőnek a kereskedelmi érdekek, vagy a közérdek védelmének, vagy az adatkezelési műveletek biztonságának sérelme nélkül kell megtennie. A GDPR ezen meglehetősen

[21] GDPR 35. cikk (1) és (10) bekezdése, valamint a (90) és a (93) preambulumbekezdése.
[22] GDPR. 25. cikk és (78) preambulumbekezdés.
[23] WP29, 2017.

szűkszavú előírásával kapcsolatban a 29-es Munkacsoport az alábbi értelmezést tette közzé az iránymutatásában:[24]

- 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 a személyes adatok feldolgozásához szükséges jogalappal. Megjegyzendő, hogy az adatkezeléshez való hozzájárulás nyilvánvalóan nem minősül az érintetti vélemények kikérésének.
- Ha az adatkezelő végleges döntése eltér az érintettek véleményétől, akkor megfelelően indokolnia és dokumentumokkal alá kell támasztania az eltérő döntés okait.
- Az adatkezelőnek dokumentumokkal kell indokolnia azt is, hogy miért nem kéri ki az érintettek véleményét, amennyiben úgy dönt, hogy erre nincs szükség. Jó példák lehetnek az ilyen esetekre, ha a vélemény kikérésével a vállalkozások üzleti tervének titkossága sérülne, illetve aránytalan vagy kivitelezhetetlen lenne ez az intézkedés.

Az adatvédelmi hatásvizsgálat lefolytatása során pedig végül az adatkezelő belső szabályzataitól és eljárásaitól függően érdemes meghatározni és írásba foglalni az egyéb szerep- és felelősségi köröket, például az alábbi esetekben:

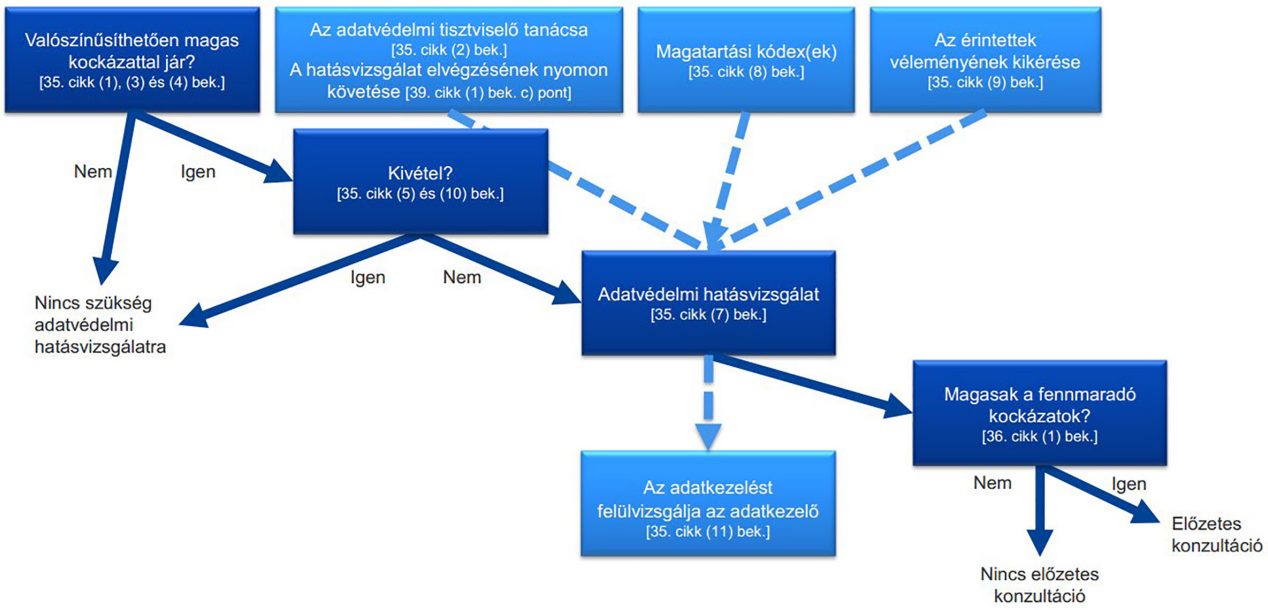
- Amennyiben egyes üzleti egységek adatvédelmi hatásvizsgálat elvégzését javasolják, akkor adatokat kell szolgáltatniuk az adatvédelmi hatásvizsgálathoz, valamint érdemes közreműködniük az adatvédelmi hatásvizsgálat jóváhagyási eljárásában.
- Adott esetben ajánlott tanácsot kérni különböző szakterületek független szakértőitől (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 felelőst vagy vezetőt, 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 adatkezelés körülményeivel kapcsolatos konkrét ismeretek fejlesztésében.
- Ha kijelölnek információbiztonsági felelőst vagy vezetőt, 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.

A GDPR továbbá azt is kimondja, 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.[25] 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.

[24] WP29, 2017.

[25] GDPR (92) preambulumbekezdés.

Az alábbi ábra végül a fentiekben bemutatott folyamatokat foglalja össze az adatvédelmi hatásvizsgálat lefolytatásának szükségességével és szakaszaival kapcsolatban.[26]



1. ábra: Az adatvédelmi hatásvizsgálat lefolytatásának szükségessége
Forrás: WP29, 2017.

[26] Forrás: WP29, 2017.

3. AZ ADATVÉDELMI HATÁSVIZSGÁLAT TARTALMA ÉS SZAKASZAI

3.1. Az adatvédelmi hatásvizsgálat főbb szakaszai

Mint ahogy már a tananyag elején is hangsúlyoztuk, a GDPR szerinti adatvédelmi hatásvizsgálat az érintettek jogait érintő kockázatok kezelésére szolgál, így az ő szemszögükből készül. Az adatkezelőnek tehát elsősorban az adatalanyok szempontjait kell szem előtt tartania annak elkészítése során.

A GDPR-ban rögzített lényeges előírások összessége széles, általános keretet nyújt az adatvédelmi hatásvizsgálat kialakításához és elvégzéséhez. Az adatvédelmi hatásvizsgálat gyakorlati végrehajtása a rendeletben foglalt előírásoktól függ, amelyeket részletesebb gyakorlati útmutatások egészíthetnek ki. Az adatvédelmi hatásvizsgálat a mérethez igazítható, ami azt jelenti, hogy még a kis adatkezelők is kialakíthatnak és elvégezhetnek a saját adatkezelési műveleteikhez igazodó adatvédelmi hatásvizsgálatot.

A vonatkozó szakirodalom a hatásvizsgálati eljárás alábbi három főbb szakaszát különbözteti meg:[27]

- előkészületi szakasz;
- hatásvizsgálati elemzés;
- a személyes adatok védelmét szolgáló biztonsági intézkedések alkalmazása.

3.2. Első szakasz: előkészületi szakasz

Az első szakasz, azaz az „előkészületi szakasz” során az adatkezelőnek elsőként azt kell megállapítania, hogy egyáltalán szükséges-e lefolytatni az adatvédelmi hatásvizsgálatot. Ennek eldöntéséhez az előző, második fejezetben említett, a GDPR 35. cikk (1) bekezdésében foglaltak az irányadók, azaz, először azt kell az adatkezelőnek mérlegelnie és eldöntenie, hogy az adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira és szabadságaira nézve.

Abban az esetben, ha az adatvédelmi hatásvizsgálatot le kell folytatni, tehát az adatkezelő szerint a tervezett adatkezelés valószínűsíthetően magas kockázatú, akkor először annak célját, valamint a vizsgálat terjedelmét kell megállapítani. E körben ugyancsak fontos, hogy az a személy, amely/aki a hatásvizsgálati eljárás lefolytatására kerül kijelölésre, megfelelő szakértelemmel és forrásokkal rendelkezzen annak lefolytatásához.

A hatásvizsgálatot lefolytató személy, a hatásvizsgálati célkitűzések és a terjedelmi határok kijelölését követően fel kell állítani azt a modellt, azaz vizsgálati tervet, amely alapján lefolytatására kerül a hatásvizsgálat.

---

[27] Bieker et. al., 2016.

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.

3.3. Második szakasz: hatásvizsgálati elemzés

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.).[28]

A GDPR 35. cikk (7) bekezdése a)-c) pontjai tartalmazzák, hogy a hatásvizsgálati elemzési szakasznak legalább mire kell kiterjednie az alábbiak szerint:

GDPR 35. cikk (7) bekezdés: **„A hatásvizsgálat kiterjed legalább:**

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; […]"

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 szükségesség-arányosság elvére is.

3.4. Harmadik szakasz: a biztonsági intézkedések alkalmazása

A harmadik szakasz, azaz „a személyes adatok védelmét szolgáló biztonsági intézkedések alkalmazásának szakasza" során el kell készíteni az úgynevezett *kockázatkezelési tervet.* Ezt a kötelezettséget a GDPR 35. cikk (7) bekezdése fogalmazza az alábbiak szerint:

[28] Péterfalvi et.al., 2018.

GDPR 35. cikk (7) bekezdés: **„A hatásvizsgálat kiterjed legalább:**
[…]

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."

A kockázatkezelési tervnek a fentiek alapján részletesen tartalmazni kell:

- Azon intézkedéseket, illetve mechanizmusokat, amelyek az érintettek jogaira és szabadságaira kockázatot jelentő elemeket megszüntetni vagy csökkenteni képesek.
- A biztonsági intézkedéseket, illetve mechanizmusokat alkalmazó személy megnevezését, illetve azon a személyt, akivel szükség esetén konzultálni lehet.
- Azt az időpontot, amikorra a biztonsági intézkedéseket és mechanizmusokat átültetik az ahhoz kapcsolódóan elérhető források megjelölésével.
- A biztonsági intézkedések és mechanizmusok eredményeinek elemzéséhez szükséges szempontokat.
- Azon személy megnevezését, aki jogosult a biztonsági intézkedések, mechanizmusok elemzésére, értékelésére.[29]

3.5. Összefoglaló dokumentáció készítése, újbóli ellenőrzés szükségessége

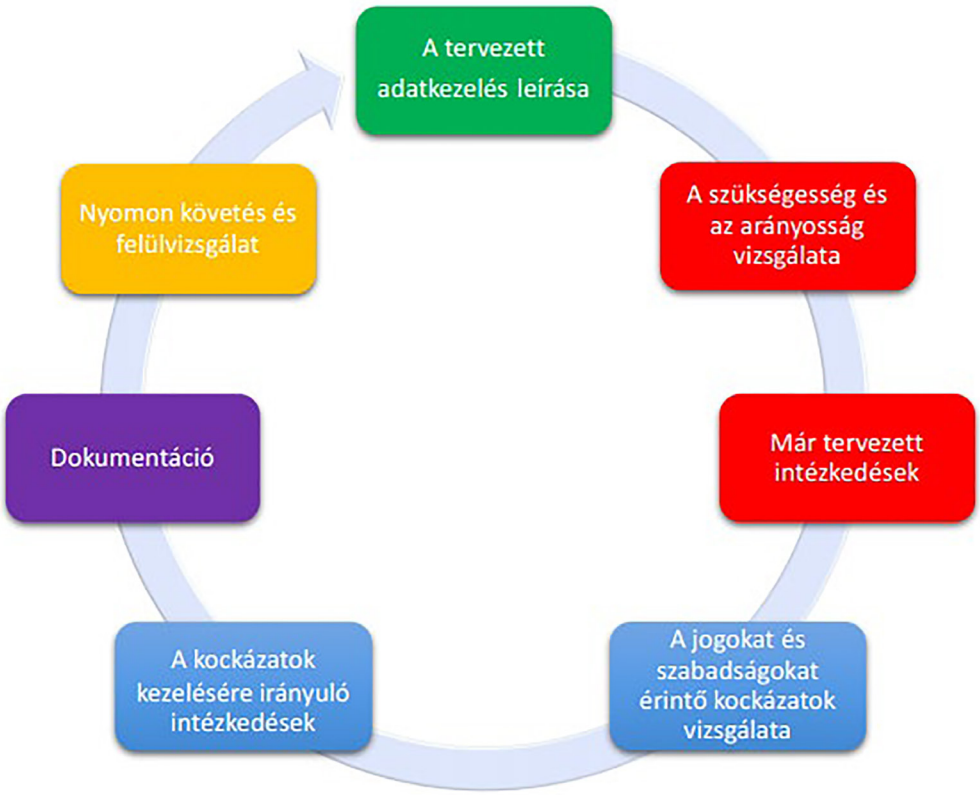
Annak érdekében, hogy a hatásvizsgálat kívánt céljai megvalósuljanak, elengedhetetlen egy a fenti elemzések eredményeit összefoglaló dokumentáció elkészítése, illetve annak hozzáférhetővé tétele. E körben az adatkezelőknek célszerű lehet egy rövidebb összefoglalót is összeállítaniuk az elkészült dokumentáció 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.[30]

A rendelet is előírja a fentieken túl az elvégzett adatvédelmi hatásvizsgálat meghatározott esetekben történő (újbóli) ellenőrzését. A Rendelet 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 például 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.[31]

[29] Péterfalvi et.al., 2018.
[30] Péterfalvi et.al., 2018.
[31] Péterfalvi et.al., 2018.

Az alábbi ábra az adatvédelmi hatásvizsgálat főbb lépéseit és elvégzésének általános, ismétlődő folyamatát szemlélteti:[32]



2. ábra: Az adatvédelmi hatásvizsgálat főbb szakaszai
Forrás: WP29, 2017.

3.6. Az adatvédelmi hatásvizsgálat nyilvánossága

A GDPR 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 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 például 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.[33]

[32] WP29, 2017.
[33] WP29, 2017.

4. AZ ADATVÉDELMI HATÁSVIZSGÁLAT LEFOLYTATÁSÁNAK MÓDSZERTANA ÉS ESZKÖZEI

4.1. Általános módszertan

A GDPR 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 GDPR 35. cikk (7) bekezdésében és a (90) preambulumbekezdésében felsorolt elemeket. Bármilyen formát ölt is az adatvédelmi hatásvizsgálat, a kockázatok valódi értékelésére kell irányulnia, mivel így az adatkezelők intézkedéseket hozhatnak azok kezelésére.

A 29-es Munkacsoport hatásvizsgálatról szóló iránymutatásának 2. számú mellékletében az Uniós adatvédelmi hatóságok közös szempontrendszert dolgoztak ki annak érdekében, hogy az adatkezelők választani tudjanak a különböző adatvédelmi hatásvizsgálati módszertanok között. A Munkacsoport álláspontja szerint az adatkezelő választja ki a módszertant, a kiválasztott módszereknek azonban meg kell felelnie az alábbiakban megadott szempontoknak:

1. Módszeres leírás készült az adatkezelésről/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 (ha vannak ilyenek) előírásainak teljesítését [a 35. cikk (8) bekezdése].
2. Értékelték a szükségességet és az arányosságot [a 35. cikk (7) bekezdésének b) pontja]:
   - A GDPR 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).

3. Az érintett jogait és szabadságait érintő kockázatokat kezelik [a 35. cikk (7) bekezdésének c) pontja]:
- o A kockázatok forrását, jellegét, egyediségét és súlyosságát felmérték [(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].
- o Az említett kockázatok orvoslására irányuló intézkedéseket meghatározták [a 35. cikk (7) bekezdésének d) pontja és a (90) preambulumbekezdés],

4. Az érdekelteket bevonták:
- o Kikérték az adatvédelmi tisztviselő tanácsát [a 35. cikk (2) bekezdése],ó.
- o Adott esetben kikérték az érintettek véleményét [a 35. cikk (9) bekezdése].

A 29-es Munkacsoport a fentieken túl 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.[34]

A fentiekből adódóan a magasabb szintű megfelelés érdekében olyan módszertan kiválasztása javasolt, amelyet az adott adatvédelmi hatóság már összhangba hozott a GDPR rendelkezéseivel. Ilyen például a francia adatvédelmi hatóság (Commission Nationale de l'Informatique et des Libertés, röviden: CNIL) módszertana, amely alkalmazását tovább erősíti, hogy a CNIL közzétett egy nyílt forráskódú szoftvert (általános ismertetését lásd később), amellyel az adatkezelők könnyen elkészíthetik a módszertannak megfelelő adatvédelmi hatásvizsgálatot.

Az adatkezelőnek egyébként a felügyeleti hatóság felé sem bejelentési, sem egyéb nyilvántartásba vételi kötelezettsége nincs a hatásvizsgálattal kapcsolatban.

4.2. A hatásvizsgálat során lefolytatandó kockázatelemzés módszertana és néhány alapfogalom

Az adatvédelmi hatásvizsgálat elkészítése során a kockázatok elemzéséhez több módszertan is ismert, nincs egységesen elfogadott, kötelezően alkalmazandó módszertan. Az adatkezelő tehát teljesen szabadon választja azt meg, hogy milyen kockázatelemzési rendszert alkalmaz a hatásvizsgálat elkészítése során. Az alábbiakban több különböző, a piacon rendelkezésre álló módszertan általános ismertetésére kerül sor, majd konkrét példák segítségével próbáljuk bemutatni a kockázatelemzés menetét és fő elemeit.

[34] WP29, 2017.

Az adatkezelők rendelkezésére áll a kockázatelemzés elvégzésére többek között a francia adatvédelmi hatóság által kidolgozott, a kockázatokat értékelő módszertan, illetve az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (továbbiakban: ENISA) ajánlása az adatvédelmi incidensek súlyosságának felmérésére szolgáló módszerről. Ez utóbbi nem az adatvédelmi hatásvizsgálat során végzett kockázatelemzésre szolgál, hanem az incidensek súlyosságának megítélésére, azonban mindkét módszer során, a kockázatok besorolása tekintetében sok a hasonló elem, így az ENISA ajánlás szempontrendszere akár egy hatásvizsgálat lefolytatása során is használható lehet.[35]

A francia adatvédelmi hatóság által kidolgozott kockázatértékelési módszertan az ENISA-tól némiképp eltérő megközelítést alkalmaz. A kockázatértékelés középpontjában az adatkezelés hatásai és a lehetséges veszélyek állnak.[36]

A francia módszertan szerint a kockázatelemzés során meg kell állapítani a kockázatok forrásait. A módszertan szerint ilyenek lehetnek:

- az adatkezelő szervezetén belül található kockázatok (felhasználó, munkavállaló stb.),
- az adatkezelő szervezetén kívül található kockázatok (versenytárs, szolgáltató, harmadik személy stb.),
- illetve nem-emberi kockázatok (kártékony kód, természeti katasztrófa stb.).

Az azonosított kockázati források ezt követően vagy szándékosan, vagy véletlenül hatást gyakorolnak arra a kiszolgáló környezetre, amelyen az adatkezelő a személyes adatokat tárolja (papír alapú dokumentumok, felhők, szerverek stb.). A kiszolgáló környezetre gyakorolt hatások különböző fenyegetések lehetnek, példaként említi a módszertan a kiszolgáló környezet megsemmisítését, megváltoztatását, jogosulatlan megismerését vagy ellopását.

A kockázat szintjét a módszertan szerint a súlyosság és a valószínűség összege adja meg. Az incidens súlyosságát az adatok azonosíthatósága és az incidens lehetséges hatásai jelölik, míg a valószínűséget a kiszolgáló környezet sebezhetősége és a kockázati források ereje határozza meg.

Az alábbiakban a kockázatok értékelése, elemzése során fontos kulcsfogalmak jelentésének meghatározása szerepel:

Kockázatforrás: Kockázatot okozó személy vagy egyéb forrás, mely lehet véletlenül vagy szándékosan előidézett. A forrás lehet szervezeten belüli emberi tényező, szervezeten kívüli emberi tényező és nem emberi tényező.

Szervezeten belüli emberi tényezőre példák: hanyag vagy tisztességtelen munkavállaló; képzetlenség és tájékozatlanság; hanyag vagy tisztességtelen felhasználó, családtag vagy barát, aki hozzáfér a rendszerhez. Több indíték is lehetséges: ilyenek lehetnek például ügyetlenség, hiba, hanyagság, játék, rosszindulat, bosszú, kémkedés.

Szervezeten kívüli emberi tényezőre példák: Tisztességtelen vagy naiv szomszéd, aki a fizikai közelség miatt meghackeli az eszköz adatait; a hacker azért szemeli ki a felhasználót, mert vannak háttérinformációi a kiszemelt felhasználóval kapcsolatban; a hacker azért szemel ki egy vállalatot, mert olyan ismeret birtokában van, amellyel alááshatja annak jóhírnevét stb.

Nem emberi tényezők: Ezen kockázatforrásra példaként szolgálhat valamely szervezetet sújtó incidens vagy káresemény (áramszünet, tűz, árvíz stb.).

Fenyegető veszély: Egy vagy több cselekvésből álló eljárás az adatok kezelésére szolgáló eszközökön, mely megvalósulhat szándékosan vagy más módon.

Súlyosság: A súlyosság jelöli a kockázat mértékét. Elsősorban a lehetséges behatások ártalmas jellegén múlik.

Valószínűség: A valószínűség a kockázat bekövetkezésének a lehetőségét jelöli. Elsősorban a veszélynek kitett eszközök sérülékenységén és a kockázatforrások mértékén múlik.

35 ENISA, 2013.
36 CNIL, 2012.

4.3. Az adatkezelés során felmerülő kockázatok felmérésének módszertana

A francia módszertan szerint a hatásvizsgálat során a kockázat mértékét az adatkezelés kapcsán:

- az érintett jogaira és szabadságaira nézve közvetlenül vagy közvetve megjelenő fizikai, társadalmi, környezeti és morális következmények, **hatások** mértéke és **súlyossága**, illetve
- a kockázat bekövetkezésének gyakorisága, **valószínűsége**

együttesen határozza meg, azok mértékének szorzata fejezi ki.

Az érintettre nézve megjelenő **hatás** a következő kategóriák alapján kerül meghatározásra:

1. Elhanyagolható: az érintettre nem lesz hatással, vagy néhány kisebb kellemetlenséget tapasztalhat, amelyek minden probléma nélkül leküzdhetők.
2. Korlátozott: az érintett jelentősebb kényelmetlenséget, hátrányt tapasztalhat, amelyet azonban kisebb nehézségek árán képes lehet leküzdeni.
3. Jelentős: az érintett jelentős következményekkel szembesülhet, amelyeket valós és komoly nehézségek árán képes csak megoldani, leküzdeni.
4. Maximális: az érintett jelentős vagy akár visszafordíthatatlan következményekkel is szembesülhet, amelyeket nem tud leküzdeni.

Az adatkezelés kapcsán bekövetkező fenyegetettség **valószínűsége** az alábbiak szerint került értékelésre:

1. Elhanyagolható: A vizsgált környezet tulajdonságai alapján nem látszik valószínűnek, hogy a kockázatforrások a személyes adatok kezelésére szolgáló eszközöket kihasználó valós veszélyt jelentenének. Egyáltalán nem valószínű, hogy az esemény bekövetkezik.
2. Korlátozott: A vizsgált környezet tulajdonságai alapján kicsi a valószínűsége annak, hogy a kockázatforrások a személyes adatok kezelésére szolgáló eszközöket kihasználó valós veszélyt jelentenének (például papír alapú iratok eltulajdonítása belépőkártyával és belépési kóddal védett helyiségből). Kicsi a valószínűsége, hogy az esemény bekövetkezik.
3. Jelentős: A vizsgált környezet tulajdonságainak kihasználásával a kockázatforrások a személyes adatok kezelésére valós veszélyt jelentenek (például papír alapú iratok eltulajdonítása olyan helyiségből, amelybe csak a recepciónál való bejelentkezés után lehet belépni). Nagyobb a valószínűsége, hogy az esemény bekövetkezik.
4. Maximális: A vizsgált környezet tulajdonságainak kihasználása, így a fenyegetés bekövetkezése a kiválasztott kockázati források miatt rendkívül könnyűnek tűnik, a vizsgált környezet tulajdonságainak kihasználásával a kockázatforrások a személyes adatok kezelésére súlyos veszélyt jelentenek. (például papír alapú iratok eltulajdonítása bárki számára nyitva álló, nyilvános előtérből). Szinte biztos a valószínűsége, hogy az esemény bekövetkezik.

A hatásvizsgálat során **az adatkezelő a vizsgált fenyegetés** bekövetkezési hatását (0-4 pont) és valószínűségét (0-4 pont) együtt (hatás és valószínűség) vizsgálja, és ezek szorzata alapján sorolja be a kockázati értékét összesen négy kategóriába. Amennyiben az alkalmazott biztonsági intézkedések alapján a kockázati szint nem lesz elfogadható mértékű, úgy a kockázatok kezelésére további szervezési és technikai intézkedéseket kell meghatározni.

A fentiek alapján a hatásvizsgálat első lépése a kockázati tényezők azonosítása, majd azok besorolása a fenti kategóriák alapján 1-4. súlyossági fokozatba. Ezek után a kockázatok csökkentése érdekében tervezett védelmi intézkedések meghatározása a következő lépés.

A tervezett adatkezelés kockázatainak értékelése a hatásvizsgálat lefolytatása során például (a francia módszertant figyelembe véve) az alábbi mátrix szerint történhet. A hatás és a valószínűség szorzata alapján határozandó meg a kockázati szint. Az oldalsó oszlopban szereplő kategóriák

csak nagyon általános kockázati forrásokat jelölnek, ennél a gyakorlatban természetesen sokkal konkrétabban szükséges meghatározni a kockázatok forrásait (lásd például jelen fejezet 4.5-ös pontját).

Kockázati forrás	Hatás (0;1;2;3;4)	Valószínűség (0;1;2;3;4)	Kockázati szint (1;2;3;4)
Fizikai, vagyoni vagy nem vagyoni károk			
Az érintett nem rendelkezhet adatai felett, nem gyakorolhatja jogait és szabadságait			
Személyes adatok különleges kategóriáit tervezik kezelni			
Személyes jellemzők értékelésére, előrejelzésére kerül sor			
Kiszolgáltatott érintetti pozícióban lévő adatainak kezelésére kerülne sor			
Nagy mennyiségű személyes adat, jelentős számú érintettre kiterjedő kezelése			

1. táblázat: Kockázati szintbe való besorolásra szolgáló mátrix

Egy adatkezelési tevékenység kockázati szintjét a táblázat „Kockázati szint” oszlopban található legmagasabb érték határozza meg. Az 1-től 4-ig besorolható kockázati szintekhez kapcsolódó értékeléseket az érintettek jogai és szabadságai szempontjából az alábbi táblázat szemlélteti:

Kockázatértékelés		
Besorolás	**Kockázati szint**	**Leírás**
0-4 pont	1. szint: Elhanyagolható	Az adatkezelési tevékenység valószínűsíthetően egyáltalán nem vagy csak nagyon elhanyagolható kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Az érintettek nem szenvednek kárt, vagy néhány kellemetlenséget kell csupán elviselniük, amelyen könnyen túlteszik magukat. Ilyenek például: fizikai/testi következmény: átmeneti fejfájás; anyagi következmény: időveszteség a formaságok ismétlése vagy teljesítése miatt, kéretlen levelek (például spamek) érkezése, weboldalakon közölt adatok újbóli felhasználása célzott reklámok küldése céljából stb.; erkölcsi következmények: egyszerű bosszúság, magánszférába való beavatkozás érzése valóságos vagy objektív sérelem nélkül stb.
5-8 pont	2. szint: Korlátozott	Az adatkezelési tevékenységnek valószínűsíthetően van kockázata a természetes személyek jogaira és szabadságaira nézve, de ez a megfelelő szervezési és technikai intézkedésekkel könnyen mérsékelhető. Az érintettek jelentősebb kellemetlenségeket tapasztalhatnak, de néhány nehézség ellenére könnyebben túlteszik magukat rajtuk. Például: testi kellemetlenség (enyhe betegség az ellenjavallatok be nem tartása miatt); becsületsértés, amely fizikai vagy pszichológiai megtorláshoz vezet stb.; anyagi kellemetlenségek: váratlan költségek (tévesen kiszabott kisebb bírságok), közigazgatási vagy kereskedelmi szolgáltatások igénybevételétől való eltiltás; kéretlen üzenetek érkezése, ami árt az érintettek jóhírnevének; erkölcsi kellemetlenségek: kisebb, de objektív pszichés betegség, a magánszféra megsértésének érzése visszafordíthatatlan sérelem nélkül, megalázás közösségi hálókon stb.

Kockázatértékelés		
Besorolás	**Kockázati szint**	**Leírás**
9-12 pont	3. szint: Jelentős	Az adatkezelési tevékenységnek valószínűsíthetően magas kockázata van a természetes személyek jogaira és szabadságaira nézve. A természetes személyek a megfelelő intézkedések hiányában a magánszférájuk szempontjából komoly és jelentős következményekkel szembesülhetnek, azokat képesek lehetnek leküzdeni, de csak nehézségek árán. Az érintettek komoly következményekkel szembesülhetnek, amelyeken ugyan túlteszik magukat, de jelentős és valós nehézségek árán. Ilyenek például a testi következmény: komoly betegségek hosszú távú következményekkel (egészségromlás szakszerűtlen gondozás vagy az ellenjavallatok be nem tartása miatt), a testi épség megváltozása például erőszak, otthoni vagy munkahelyi baleset folytán; anyagi következmény: pénz hűtlen kezelése kártalanítás nélkül, tervezett, egyedi és meg nem ismételhető lehetőségek elvesztése (lakáshitel, tanulmányi, gyakornoki vagy munkahelyi felvétel elutasítása, eltiltás vizsgázástól), lakás vagy állás elvesztése stb.; komoly pszichológia betegség (depresszió, fóbia kialakulása), a magánszféra megsértésének érzése maradandó sérelemmel, zsarolás, kibermegfélemlítés és zaklatás áldozatává válás stb.
13-16 pont	4. szint: Maximális	Az adatkezelési tevékenységnek valószínűsíthetően magas kockázata van a természetes személyek jogaira és szabadságaira nézve. A természetes személyek a magánszférájuk szempontjából kiemelkedően jelentős vagy akár visszafordíthatatlan következményekkel szembesülhetnek, melyeken nem tudják túltenni magukat, ha az adatkezeléssel kapcsolatban az adatkezelő nem alkalmaz megfelelő intézkedéseket. Ilyen például: az egészségkárosodás: hosszú távú vagy állandó testi betegség, a testi épség maradandó károsodása, halál; anyagi következmény: pénzügyi kockázat, adósság, munkaképtelenség, áthelyezkedésre való képtelenség, bizonyítékvesztés peres eljárásban, létfontosságú közművektől való elzárás stb.; erkölcsi következmény: hosszú távú vagy állandó pszichológiai betegség, büntetőjogi szankció, emberrablás áldozatává válás, családi kötelékek elvesztése, jogállás megváltozása és/vagy jogi önállóság elvesztése (gyámság) stb.

2. táblázat: Egyes kockázati szintekhez tartozó következmények értékelése az érintettek szemszögéből

4.4. A kockázatok csökkentésére szolgáló biztonsági intézkedések kategóriái

A francia adatvédelmi hatóság módszertana a kockázatok csökkentése érdekében alkalmazható védelmi intézkedéseket három kategóriába sorolja, amelyek a következők:

- logikai biztonságvédelem,
- fizikai biztonságvédelem és
- szervezeti (adminisztratív) védelmi intézkedések.

Ezeken a fő kategóriákon belül megnevez konkrét biztonsági intézkedéseket, amelyek közül a hatásvizsgálatot lefolytató adatkezelő kiválaszthatja a vizsgált adatkezelés során alkalmazottakat. Fontos, hogy az egyes védelmi intézkedésekbe tartozó kategóriák és eszközeik nem kerültek mind felsorolásra. Az adatkezelőnek tehát lehetősége van arra, hogy az adatkezelés kockázatainak csökkentésére további védelmi intézkedéseket vezessen be az adatkezelés és a kiszolgáló környezet jellemzői, továbbá a tudomány és technika mindenkori állásának megfelelően.

A francia módszertan alapján a kategóriák egyes elemei a következők:

a. Logikai biztonságvédelem

- Titkosítás: Személyes adatokat az illetéktelenek számára felismerhetetlenné tevő intézkedés (szimmetrikus vagy aszimmetrikus titkosítás, a köztudottan erős, nyilvános algoritmusok, hitelesítő tanúsítványok stb. használata).
- Anonimizálás: Az anonimizálás olyan technika, amelyet a személyes adatok személyazonosításra való alkalmatlanná tétele céljából alkalmaznak. Lásd ezzel kapcsolatban bővebben: A 29-es Adatvédelmi Munkacsoport 05/2014. számú véleményét az anonimizálási technikákról.[37]
- Álnevesítés: A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik. Ennek feltétele, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.
- Az adatok különválasztása: Amennyiben a különböző adatokat elválasztva kezelik, csökkenhet annak az esélye, hogy a személyes adatok egymással összefüggésbe hozhatók legyenek egy esetleges adatvédelmi incidens bekövetkezése esetén.
- Logikai hozzáférés szabályozás: Olyan kockázatcsökkentő eszközök alkalmazása, amelyek meggátolják az illetéktelenek személyes adatokhoz való hozzáférését, és amelyek egyebek közt a következőket feltételezik: a felhasználói profilok kezelése a feladatok és felelősségi körök elválasztásával (lehetőség szerint központosítottan) azért, hogy csak az illetékes felhasználók – a szükséges ismeret és legkisebb jogosultság elveinek betartásával – férhessenek hozzá a személyes adatokhoz. Továbbá a munkavállalók, a szerződő és a harmadik felek jogosultságainak megvonása, ha azok már nem jogosultak hozzáférni a hivatali eszközökhöz, illetve, ha már lejárt a munkaszerződésük.
- Nyomon követhetőség (naplózás): Naplózó rendszer kialakítása (például a rendszerbe történő bejelentkezésekkel, a benne eszközölt változtatásokkal kapcsolatban stb.), amely lehetővé teszi az adatvédelmi incidensek korai észlelését, illetve olyan információk gyűjtését, amelyek alapján elemzéseket lehet végezni, illetve amelyek bizonyítékul szolgálhatnak.
- Jelszó: Javaslatok a jelszóképzéssel kapcsolatban: A jelszónak legalább nyolc karakterből kell állnia, újat kell megadni a veszély legcsekélyebb gyanúja esetén, illetve lehetőleg rendszeresen (félévente vagy évente) meg kell újítani. A négy karaktertípusból legalább hármat kell tartalmaznia (kis- és nagybetű, szám és egyéb jel). Jelszó cseréjekor az utolsó öt nem használható újra. Ugyanaz a jelszó nem használható más hozzáférés esetén. A jelszó ne kapcsolódjon személyes adatokhoz (beleértve a nevet vagy a születési időt). Meg kell határozni a belépési kísérletek maximális számát, amelynek elérése után figyelmeztetést kell küldeni, és a belépést megtagadni.
- Archiválás: A személyes adatokat tartalmazó elektronikus archívumok megőrzését és további kezelését, azok minőségét (főként jogi minőségét) az egész érintett időszakban biztosító eljárások kidolgozása (így például továbbítás, tárolás, áthelyezhetőség, hozzáférhetőség, eltávolítás, archiválási elvek, bizalmas kezelés védelme stb.).
- Adatminimalizálás, adattakarékosság: A GDPR-ban is nevesített adattakarékosság elvének való megfelelés biztosítása különböző technikai intézkedésekkel. A GDPR 5. cikk (1) bekezdés c) pontjában foglalt elv alapján **„a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.”**

[37] A vélemény magyar nyelven elérhető: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf

b. Fizikai biztonságvédelem

- Üzembiztonság: A személyes adatok kezelésére szolgáló eszközök kockázati kitettségét csökkentő intézkedések tartoznak ebben a kategóriába. Például érzékeny adatokat tartalmazó iratok/adathordozók zárható páncélszekrényben történő tárolása.
- Rosszindulatú software-ek kiszűrése: A munkaállomásokra és a szerverekre telepített olyan programok vagy eszközök, amelye a rosszindulatú szoftverekkel szemben védik az informatikai infrastruktúrát. Ez a védelem a kevésbé biztonságos hálózatokhoz, weboldalakhoz csatlakozás esetén fontos.
- A munkaállomások kezelése: Ez a kategória a munkaállomásokra telepített védelmi eszközöket fogja össze. Például munkaállomás automatikus lezárása egy bizonyos időkorlát után, rendszeres frissítés, konfiguráció.
- Webhelybiztonság: Ez a kategória a weboldalakkal kapcsolatos biztonsági intézkedések alkalmazását jelenti. Például az adatátvitelre szolgáló kommunikációs csatorna titkosított (HTTPS protokoll, hitelesítés stb.) formában történő használata a webhelyen.
- Biztonsági mentés: A személyes adatok kezelése során az adatok rendelkezésre állását biztosító eszközök tartoznak ebbe a kategóriába. A biztonsági mentés fontosságát egyébként a GDPR 32. cikk (1) bekezdés c) pontja is általánosságban kihangsúlyozza, amikor azt írja elő megfelelő adatbiztonsági intézkedésként az adatkezelők részére, hogy fizikai vagy műszaki incidens esetén képesnek kell lenniük arra, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza tudják állítani.
- Karbantartás: Az adatkezelés során használt hardverek és ezeket irányító szoftverek (például firmware) karbantartására szolgáló eljárások tartoznak ide. Fontos tényező adatbiztonsági szempontból például, hogy a karbantartást az adatkezelő kiszervezi-e külső cégnek. A kiszervezés során engedélyezett-e az applikációk távoli karbantartása, és milyen feltételekkel. A meghibásodott berendezések kezelésére szolgáló eljárások is ide tartoznak végül.
- Adatfeldolgozók igénybevétele során alkalmazandó követelmények: Az adatkezelés megtervezése során kizárólag olyan adatfeldolgozók vehetők igénybe, akik ehhez megfelelő garanciát biztosítanak, különösen a szakértelem, megbízhatóság és a megfelelő források terén. Az adatfeldolgozóknak dokumentálniuk kell a garanciák hatékonyságának biztosítását.
- Hálózatbiztonság: Az adatkezelés során alkalmazott hálózat fajtájától (elkülönült, magánhálózat, Internet) függően ebbe a kategóriába tartoznak azon biztonsági intézkedések, amely a hálózat biztonságáért felelnek. Például tűzfal, behatolásérzékelő rendszer stb.
- Hálózati tevékenységek megfigyelése: A klasszikus hálózatbiztonsági intézkedésektől elkülönült kategória. Olyan speciális szoftverek, eszközök tartoznak ide, amelyek a hálózat (vezetékes hálózat, wifi, rádióhullám, száloptika) valós idejű adatforgalmát elemzik és ellenőrzik és így észlelik a kibertámadás-gyanús tevékenységeket.
- Fizikai hozzáférésvédelem: Ebbe a kategóriába leginkább az épületbiztonsággal kapcsolatos fizikai biztonsági intézkedések tartoznak, így például az épület szakaszolása, vendégek kísérete, belépők viselése, ajtók zárása, kulcsok leadása, riasztórendszer telepítése stb. A cél az épületbe, illetve az adatkezelés során releváns helyiségekbe történő illetéktelen belépés, behatolás megakadályozása.
- Hardverbiztonság: A szerverek és munkaállomások fizikai biztonságát befolyásoló védelmi intézkedések tartoznak ebbe a kategóriába, például biztonságos tárolás, biztonsági kábelek, biztonsági törlés adathordozók selejtezése, kidobása, megsemmisítése előtt.
- A nem emberi eredetű kockázatokkal szembeni védelem, azok elkerülése: Ebbe a kategóriába tartoznak például a telepítési helyszín, környezet dokumentációja; tűzvédelmi

eszközök, tűzjelző és tűzoltó berendezések leírása; vízkár elleni védelem eszközei, ha vannak ilyenek; áramellátás ellenőrzésére és biztosítására szolgáló eszközök (például szünetmentes táp) és a kármentesítés eszközei.

c. Szervezeti (adminisztratív) védelmi intézkedések

- Szervezeti felépítés: Ezen kategória alatt lehet ismertetni, hogy van-e adatvédelmi tisztviselő, vagy egyéb adatvédelemért felelős személy a szervezeten belül. Van-e esetleg kijelölve olyan belső munkacsoport/bizottság/egység, amely ellenőrző mechanizmusként működik az adatvédelmi vonatkozású tevékenységek kapcsán, iránymutatással szolgál és felel az utánkövetésért is.
- Szabályzatok: Az adatvédelemmel kapcsolatos belső szabályzatok ismertetése és azok alkalmazhatósága, illetve megfeleltetése a hatóságvizsgálattal érintett adatkezelésre.
- Adatvédelmi kockázatok kezelése: Azok a rendelkezések tartoznak ide, amelyek megállapítják a szervezet által végzett, az adatkezelésre és az érintettek magánszférájára kockázatot jelentő adatkezelési műveletek megvizsgálására irányuló eljárásrendeket (például kockázatértékelési módszertan, eljárásrend stb.).
- Az adatvédelem beépítése a projektekbe („privacy-by-design”, avagy „beépített adatvédelem” elve): Az egyes újonnan bevezetett adatkezelési műveletek esetén a személyes adatok védelmét integráló intézkedések bevezetése. A hatásvizsgálat szempontjából mint biztonsági intézkedés, olyan belső eljárásrendek tartozhatnak ide, amelyek előírják, hogy minden újonnan megkezdett adatkezelési művelet esetén beépítsék a folyamatokba a személyes adatok védelmének biztosítását. A beépített és alapértelmezett adatvédelem elvét a GDPR 25. cikke is részletesen tartalmazza.
- A személyes adatokkal kapcsolatos jogsértések kezelése: Van-e olyan személy vagy szervezeti egység az adatkezelőnél, amely a személyes adatokat érintő jogsértés esetén eljár, lehet hozzá közvetlenül érintetti panasszal fordulni, kezeli az adatvédelmi incidenseket stb.
- Humánerőforrás-menedzsment: Ide olyan intézkedések, belső eljárások tartoznak, hogy az újonnan felvett alkalmazottak esetében milyen adatvédelmi ismereteiket bővítő és adatvédelmi tudatosságukat növelő mechanizmusokat kell alkalmazni, továbbá milyen intézkedéseket alkalmaznak abban az esetben, ha kilép (felmond, nyugdíjba megy stb.) egy munkavállaló, aki hozzáféréssel rendelkezik a kezelt személyes adatokhoz.
- Kapcsolat harmadik felekkel: Rendelkezik-e az adatkezelő olyan szabályzattal és eljárásrenddel, amely a személyes adatokhoz való harmadik fél általi (jogszerű) hozzáférést szabályozza.
- Felügyeleti intézkedések: Végül ebbe a kategóriába az olyan intézkedések, belső eljárások tartoznak, amelyek meghatározzák, hogy mely esetben kell külső felügyeleti szervet bevonni az adatkezelés során felmerülő problémák, kockázatot jelentő események kezelésére.

A fenti biztonságvédelmi kategóriákból az adatkezeléssel foglalkozó adatbiztonsági szakember feladata, hogy kiválassza azt, hogy melyikeket alkalmazza. Tehát végső soron a hatásvizsgálatot lefolytató személy vagy csapat mérlegelésétől és döntésétől függ, hogy éppen melyiket alkalmazzák az adatkezelés kockázatainak csökkentése függvényében.

4.5. Példa kockázatelemzés lefolytatására egy konkrét eseten keresztül[38]

Az alábbiakban egy konkrét hatásvizsgálat során végzett kockázatelemzést ismertetünk a téma jobb megértése érdekében.

Az eset alapján egy bevásárlóközpontot üzemeltető cég, az általa fejlesztett kamerás kasszafelügyeleti rendszerrel kapcsolatban végeztetett el egy adatvédelmi hatásvizsgálatot, amely során a kockázatok elemzésére az alábbiakban bemutatott módszertan és táblázatok szerint került sor.

- A táblázat alapján az első oszlopban található meg, hogy a hatásvizsgálat lefolytatása során az adatvédelmi tisztviselő a bevezetendő rendszerrel kapcsolatban milyen lehetséges kockázati tényezőket, tehát a személyes adatokra jelentett „fenyegetéseket" azonosított („Fenyegetés").
- Ezek után a tisztviselő meghatározta azt is, hogy a lehetséges fenyegetés mely környezetét vagy komponensét érinti a bevezetendő rendszernek („Érintett környezet vagy komponens").
- A tisztviselő megnézte, hogy a tervezett rendszerben milyen védelmi intézkedéseket terveznek beépíteni. Ezeket a tisztviselő logikai, fizikai és adminisztratív intézkedésre osztotta fel és külön-külön ismertette a táblázat következő oszlopában („Alkalmazott védelmi intézkedés").
- A tisztviselő mérlegelte azt, hogy a fenyegetés bekövetkezése milyen hatással járhat az érintettek jogaira és szabadságaira nézve, és azt a 0-4 közötti skálán értékelte.
- A tisztviselő mérlegelte azt, hogy az adatkezelésre jelentett fenyegetés milyen valószínűséggel következhet be az adatkezelő szervezetén belül az alkalmazott védelmi intézkedések figyelembe vételével, és ezt is értékelte 0-4 közötti skálán.
- A kockázati szintet ezek után a „hatás" és „valószínűség" oszlopokban található értékek szorzataként számolta ki a tisztviselő. A fenyegetés kockázati szintjét összesen négy lehetséges kategóriába sorolta be („elhanyagolható", „korlátozott", „jelentős", „maximális").
- A táblázatot végül a tisztviselő három különböző részre osztotta, abból a szempontból, hogy a fenyegetés által jelentett kockázatot „bizalmassági", „sértetlenségi" vagy „rendelkezésre állási" kockázatnak azonosította. Ezek alapján három különböző táblázat született, amelyek az alábbiak szerint néznek ki.

A) Bizalmasság – Az érintettről gyűjtött adatok rosszhiszeműség eredményeként vagy gondatlanságból bekövetkező nyilvánosságra kerülése, jogosulatlan megismerhetővé válása (adatszivárgás).

Fenyegetés	**Érintett környezet vagy komponens**	**Alkalmazott védelmi intézkedés**			**Kockázat súlya**		**Kockázati szint**
		logikai	*fizikai*	*szervezési (adminisztratív)*	*hatás*	*valószínűség*	
Adatok szivárgása közvetlenül az adatcserére használt hálózatból, hálózat lehallgatása – „man in the middle" támadás	Kommunikációs csatorna	Hálózatfelügyeleti eszközök, határvédelem	Zárt rendszer, árnyékolt vezeték, titkosított kommunikáció	Más eszköz csatlakoztatásának tilalma a hálózatra	3	1	3x1=3 pont Elhanyagolható

[38] Az eset egy létező adatkezelővel kapcsolatban lefolytatott hatásvizsgálat kockázatelemzéssel kapcsolatos részének bemutatása anonimizált és a tananyag szerzője által kiegészített változatban.

Az összes adat megismerhetővé válik az adattároló megszerzése, vagy jogosulatlan/jogosultságot meghaladó hozzáféréssel, vírus és rosszindulatú szoftver útján	Adattároló egység	Egyedi fájlformátum, titkosított adathordozó, megőrzési idő után automatikus felülírás, portok tiltása, jogosultsági rend	Fizikailag zárt tárolóegység, külön elemző helyiség, proxy kártyás beléptető rendszer	Elhelyezésre és adatkimentésre vonatkozó eljárásrend, szállítás és beléptetés rendje szabályozott, patch management és	3	2	3x2=6 pont Korlátozott
A szolgáltató alkalmazásában álló személyen, vagyonőrön kívül más is megfigyelést végez, kifürkész adatokat, összejátszik a kasszással	Ellenőrző monitor vagy távfelügyeletet ellátó monitor	Képmaszkolási funkció; érzékeny árucikkek nevének automatikus kitakarása; monitoron csak megjelölés, kimentést vagyonőr nem tud végezni, jelszókezelés	Illetéktelenek rálátását korlátozó, elkülönített elhelyezés, távfelügyelet esetén külön helyiség	Háromlépcsős felhasználási rend, elhelyezésre és vagyonőrökre vonatkozó szabályzat, nem maradhat őrizetlenül az eszköz,	2	1	2x1=2 pont Elhanyagolható
Adatok jogosulatlan kimentése, továbbítása, sebezhető szoftver alkalmazása miatt szivárgás, szándékos backdoor, konfigurációs adatok nem megfelelő beállítása	Elemző szoftver	Szűkített jogosulti kör, felhasználó kezelés, jelszókezelés, naplózás, fejlesztői biztonsági tesztelés és változáskövetés	Külön eszközön, belépés rendje ellenőrzött	Naplózásra vonatkozó előírások, négy szem elve, frissítési és tesztelési eljárásrend	3	2	3x2=6 pont Korlátozott
Az adathordozó szállítása követhetővé válik, ismertté válik ki elemzi, továbbítja az adatokat	Dokumentáció (naplók)	Felhasználó kezelés, jogosultságok kezelése, patch menedzsment, frissítési rend, végpontvédelem	Zárt szekrényben tárolt papíralapú napló, korábbi naplók külön telephelyen tárolva	Átadás-átvételi rend, betekintési jogok korlátozása	2	2	2x2=4 pont Elhanyagolható
Adatok jogosulatlan kimentése, továbbítása, szociális hackelés (manipuláció) áldozatává válik, elégtelen rendszerismeret	Szolgáltató elemzést végző munkatársa	Négy szem elve a szoftverben, biztonsági naplózás, felhasználói jogosultság kezelés	Külön elemző helyiség	Titoktartási nyilatkozat, eljárásrend, felettes ellenőrzése, rendszeres biztonság-tudatossági oktatások, IBSZ[39]	3	2	3x2=6 pont Korlátozott
Rosszul beállított felhasználói jogosultság, adatok jogosulatlan kimentése, továbbítása, adattároló hiányos törlése, szociális hackelés (manipuláció) áldozatává válik, karbantartási hiba	Szolgáltató kiemelt jogosultsággal rendelkező felhasználója	Biztonsági naplózás	–	Titoktartási nyilatkozat, adatvédelmi tisztviselő ellenőrzi, több admin jogosult, egymást is ellenőrzik, rendszeres biztonság-tudatossági oktatások, IBSZ	3	2	3x2=6 pont Korlátozott

[39] Informatikai Biztonsági Szabályzat

B) Sértetlenség – Személyes adatok kéretlenül bekövetkező megváltozása, hitelességének sérülése (illetéktelen módosítása)

Fenyegetés	Érintett környezet vagy komponens	Alkalmazott védelmi intézkedés			Kockázat súlya		Kockázati szint
		logikai	*fizikai*	*szervezési (adminisztratív)*	*hatás*	*valószínűség*	
Jel módosítása „man in the middle" támadás kertében, túlterhelt hálózat, fizikai vagy logika hálózati meghibásodás	Kommunikációs csatorna	Hálózatfelügyeleti eszközök	Zárt rendszer, árnyékolt vezeték, titkosított kommunikáció	Más eszköz csatlakoztatásának tilalma	2	1	2x1=2 pont Elhanyagolható
Zsarolóvírus, vírus és rosszindulatú szoftver, felvételek összekeveredése, adathordozó meghibásodása miatt adatsérülés	Adattároló egység	Egyedi fájlformátum, időbélyeg, portok tiltása, jogosultsági rend, naplózás, végpontvédelem, adathordozó élettartam elemzés	Nyílt internettől elválasztott tárolóegység, külön elemző helyiség	Elhelyezésre és adatkimentésre vonatkozó eljárásrend, élettartam követés alapján csere	3	2	3x2=6 pont Korlátozott
Beavatkozik a megfigyelést végző az adatrögzítés folyamatába	Ellenőrző monitor, távfelügyeleti megjelenítő eszköz	Háromlépcsős felhasználási jogok (monitoron csak megjelölés, nem módosítható az adat), naplózás	Elkülönített elhelyezés	Elhelyezésre és vagyonőrökre vonatkozó szabályzat, nem maradhat őrizetlenül az eszköz	3	1	3x1=3 pont Elhanyagolható
Sebezhető szoftververzió következtében módosulás, szándékos backdoor, konfigurációs adatok nem megfelelő beállítása	Elemző szoftver	Szűkített jogosulti kör, felhasználó kezelés, naplózás, patch menedzsment, frissítési rend, fejlesztői biztonsági tesztelés és változáskövetés	Külön eszközön, belépés rendje ellenőrzött	Naplózásra vonatkozó előírások, négy szem elve, IBSZ	2	1	2x1=2 pont Elhanyagolható
Utólag átírják ki fért hozzá az adatokhoz	Dokumentáció (naplók)	Felhasználó kezelés, jogosultságok kezelése, időbélyegző	Elzártan kezelt papíralapú naplózás, korábbi naplók külön telephelyen tárolva	Átadás-átvételi rend, bejegyzési jogok korlátozása	2	1	2x1=2 pont Elhanyagolható
Felhasználói hiba, szociális hackelés (manipuláció) áldozatává válik, elégtelen rendszerismeret	Szolgáltató elemzést végző munkatársa	Négy szem elve a szoftverben, biztonsági naplózás, felhasználói jogosultság kezelés	Külön elemző helyiség, ellenőrzött beléptetés	Titoktartási nyilatkozat, eljárásrend, felettes ellenőrzése, rendszeres biztonság-tudatossági oktatások, IBSZ	3	2	3x2=6 pont Korlátozott
Rosszul beállított felhasználói jogosultság, adatok jogosulatlan módosítása, szociális hackelés (manipuláció) áldozatává válik, karbantartási hiba	Szolgáltató kiemelt jogosultsággal rendelkező felhasználója	Biztonsági naplózás	-	Titoktartási nyilatkozat, adatvédelmi tisztviselő ellenőrzi, több admin jogosult, egymást is ellenőrzik, rendszeres biztonság-tudatossági oktatások, IBSZ	3	2	3x2=6 pont Korlátozott

C) **Rendelkezésre állás** – Sérül a személyes adatok elérhetősége, adatvesztés

Fenyegetés	Érintett környezet vagy komponens	Alkalmazott védelmi intézkedés			Kockázat súlya		Kockázati szint
		logikai	*fizikai*	*(szervezési) adminisztratív*	*hatás*	*valószínűség*	
Megszakad a távfelügyelet során a jel, fizikai vagy logika hálózati meghibásodás (átvágják a vezetéket, DDOS támadás, túláram keletkezik)	Kommunikációs csatorna	Hálózatfelügyeleti eszközök, a rögzítés az adatkezelőnél folytatódik, így utólag elemezhető	Zárt rendszer, árnyékolt vezeték	Más eszköz csatlakoztatásának tilalma	1	2	1x2=2 pont Elhanyagolható
Lényeges adatok szándékos kitörlése, meghibásodás, túlmelegedés, beázás, karbantartási hiba, teszteletlen vagy nem megfelelően tesztelt IT eszköz üzembeállítása	Adattároló egység	Jogosultságkezelés, monitorozás	Fizikailag zárt tárolóegység, külön helyiség, beléptetés rendje, áramellátó berendezések és kábelezés kezelése, tartalék eszköz	BCP, elhelyezésre és adatkimentésre vonatkozó eljárásrend, IBSZ	2	3	2x3=6 pont Elhanyagolható
Meghibásodás miatt az érintett szempontjából lényeges eseményt nem tudja megjelölni a vagyonőr	Ellenőrző monitor	Rögzítés független az ellenőrző monitortól, később hozzáférhető	Tartalék eszköz	Karbantartási szabályzat	1	1	1x1=1 pont Elhanyagolható
Nem azonosítható be később az érintett panaszában megjelölt felvétel vagy kasszainformáció, hibás kód frissítés, szándékos vagy véletlen törlés	Elemző szoftver	Fejlesztői biztonsági tesztelés és változáskövetés, jogosultsági rend	Adathordozó felülírási rend	Naplózásra vonatkozó előírások, négy szem elve	2	1	2x1=2 pont Elhanyagolható
Elvesztik a papír alapú naplót, olvashatatlanná válik a fájl, így nem állapítható meg ki fért hozzá az adatokhoz	Dokumentáció (naplók)	Külön naplófájlok, automatikus biztonsági mentés	Elzártan kezelt, korábbi naplók külön telephelyen tárolva	Átadás-átvételi rend, bejegyzési jogok korlátozása	2	2	2x2=4 pont Elhanyagolható

A fentiek alapján a lehetséges fenyegetések beazonosítása megtörtént és bekövetkezésük valószínűsége megállapítása került az alkalmazott védelmi intézkedések ismeretében, továbbá mérlegelésre került, hogy az milyen hatással lehet az érintettekre. A táblázat a kiszámított kockázati szint alapján megmutatta, hogy vajon szükségesek-e további védelmi intézkedések, ahhoz, hogy a kockázatokat elfogadható szintűre (így legalább korlátozott mértékűre) csökkentse az adatkezelő. Jelen esetben az adatvédelmi kockázatokat mindegyik esetben sikerült elfogadható szintűre csökkenteni, így további intézkedések az adatkezelő részéről a tisztviselő által lefolytatott kockázatelemzés alapján nem szükségesek.

4.6. A francia adatvédelmi hatóság által közzétett ingyenes hatásvizsgálati szoftver

A francia adatvédelmi hatóság létrehozott egy szoftvert, amelynek a célja segítséget nyújtani a GDPR rendelkezéseivel összhangban álló adatkezelés kialakításában és az annak történő megfelelés bizonyításában. A szoftver több nyelven – köztük magyar nyelven is – elérhető.[40]

Ezt az eszközt az adatkezelőknek, főképpen azon adatkezelőknek címezték, akik az adatvédelmi hatásvizsgálat folyamatát illetően alapszintű ismeretekkel rendelkeznek. A szoftver önállóan futtatható verziója letölthető és könnyen elindítható a felhasználó számítógépén. Emellett a szoftver használata oly módon is lehetséges, hogy azt a szervezet saját szerverére telepítik annak érdekében, hogy a már meglévő egyéb eszközök és rendszerek közé integrálják.

A hatásvizsgálati szoftver három elv mentén került kialakításra:

Átlátható és felhasználóbarát felület: a hatásvizsgálati szoftver felhasználóbarát felületet biztosít a hatásvizsgálat lefolytatásához és egyszerű elvégzéséhez. Egyszerűen áttekinthető módon végigvezeti a felhasználót a hatásvizsgálat módszertanának egyes lépésein. A szoftver alkalmazása során számos vizuális eszköz biztosítja például az egyes kockázatok mértékének gyors megértését.

Jogi és technikai ismeretek: a szoftver felhasználói felületén jogi és technikai jellegű tudásanyag is elhelyezésre került az adatkezelés jogszerűségének és az érintettek jogainak biztosítása érdekében. Ennek keretében tartalmazza a GDPR szövegéből hivatkozott rendelkezéseket is. A szoftver a hatásvizsgálat lefolytatása során oly módon nyújt útmutatást a felhasználók számára, hogy azok az egyes lépéseknél a felületen aktuálisan megnyitott menüpontokhoz kapcsolódóan jelennek meg.

Egymásra épülő modulokból álló eszköz: a hatásvizsgálati szoftver mindemellett egy egymásra épülő modulokból álló eszköz: úgy alakították ki, hogy segítséget nyújtson az adatvédelmi szabályoknak történő megfelelés kialakításában, a felhasználó ezen kívül egyéniesíteni tudja a szoftvert az saját igényeinek, valamint a szektorális sajátosságoknak megfelelően. Tekintettel arra, hogy a hatásvizsgálati szoftver szabadon terjeszthető, a felhasználóknak arra is lehetőségük van, hogy a forráskódjának módosítása révén további funkciókat adjanak hozzá, vagy beintegrálják a szervezeten belül már alkalmazott egyéb eszközök közé.

A szoftver használatának további részletes ismertetésétől jelen tananyag eltekint, mivel a szoftver használata a hatásvizsgálat lefolytatása során nem kötelező, az csupán egy szabadon használható ingyenes eszköz. Ettől függetlenül annak felhasználói szintű kipróbálására a szerző bátorítja a hatásvizsgálatban mélyebben elmerülni kívánó olvasót.

[40] A szoftver magyar változata ingyenesen letölthető a NAIH honlapjáról is: https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html

5. A NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG SZEREPE AZ ADATVÉDELMI HATÁSVIZSGÁLATOKKAL KAPCSOLATOSAN

5.1. A felügyeleti hatóság bírságolási jogköre

A GDPR vonatkozó szabályai értelmében az adatvédelmi hatásvizsgálatra vonatkozó előírások be nem tartása esetén az illetékes adatvédelmi 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, előzetes konzultáció elmulasztása közigazgatási bírsággal sújtható, amelynek összege legfeljebb 10 millió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-a. A kettő közül a magasabb összeget kell kiszabni.[41]

5.2. A hatásvizsgálattal kapcsolatos hatósági jegyzékek (fekete és fehér listák) elfogadása és nyilvánosságra hozatala

A GDPR gyakorlati alkalmazása során néhány esetben az adatkezelőknek komoly kihívás lehet a hatásvizsgálat szükségességének eldöntése. Ezt figyelembe véve az Uniós jogalkotó a Rendelet 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. Ezt a listát nevezzük az hatásvizsgálati „*fekete listának*”.

A GDPR ezt a kötelezettséget az alábbiak szerint határozza meg:

35. cikk (4) bekezdés: „A felügyeleti hatóságnak össze kell állítania és nyilvánosságra kell hoznia az olyan adatkezelési műveletek típusainak a jegyzékét, amelyekre vonatkozóan […] adatvédelmi hatásvizsgálatot kell végezni. A felügyeleti hatóság továbbítja az említett jegyzékeket a[z Európai Adatvédelmi] Testület részére.”

A hatásvizsgálat hatékony alkalmazásának előfeltétele, hogy a hatóságok összehangolják tevékenységüket ezen a téren, ezért a GDPR előírja, hogy a hatósági jegyzékek elfogadását megelőzően az egységességi mechanizmus keretében egyeztessenek egymással, ha több tagállamra kiterjedő hatása lehet az adatkezelésnek, illetve emiatt érintheti a személyes adatok Unión belüli szabad áramlását az alábbiak szerint:

---

41 GDPR 83. cikk (4) bekezdés a) pontja alapján.

35. cikk (6) bekezdés: „A […] jegyzékek elfogadását megelőzően 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."

Ettől függetlenül egyéb esetekben is kívánatos, hogy a hatóságok egyeztessenek egymással, hiszen kerülendő az a helyzet, amikor egy adatkezelés típus egy tagállamban hatásvizsgálat alá esik, míg így másikban mentességet élvez.[42]

Megjegyzendő, hogy az adatvédelmi hatásvizsgálat elvégzésének követelménye adott esetben jelentős teher 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. A GDPR a kis- és közepes méretű vállalkozások esetében az adminisztratív terheket a lehető legalacsonyabb szinten szeretné tartani, ezért azzal is számolni lehet, hogy e szektor bizonyos esetekben mentességeket, könnyítéseket kap a többi adatkezelőhöz képest.[43]

Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) hozta nyilvánosságra a honlapján azon adatkezelési típusok jegyzékét, amelyek esetén kötelező a hatásvizsgálati lefolytatása. A jegyzékben szereplő tételeket a fejezet következő pontjában érintjük.

A GDPR 35. cikk (5) bekezdése pedig egy olyan jegyzék összeállítására is lehetőséget biztosít a felügyeleti hatóságnak, amely azon adatkezelési műveletek típusait tartalmazza, amelyre vonatkozóan nem kell adatvédelmi hatásvizsgálatot elvégezni:

35. cikk (5) bekezdés: „A felügyeleti hatóság összeállíthatja és nyilvánosságra hozhatja az olyan adatkezelési műveletek típusainak a jegyzékét is, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni. A felügyeleti hatóság továbbítja ezeket a jegyzékeket a Testület részére."

Az ilyen típusú listát a szaknyelv úgynevezett *„fehér listának"* nevezi. Ez utóbbi összeállítása azonban csak lehetőség az adatvédelmi hatóságok számára. Magyarországon a NAIH nem hozott (egyelőre) nyilvánosságra ilyen listát.

Amennyiben az adott felügyeleti hatóság úgy dönt, hogy nyilvánosságra hoz egy fehér listát, úgy – a fekete listához hasonlóan – először ebben az esetben is igénybe kell vennie a GDPR 63. cikkében említett egységességi mechanizmust, ha a listán határon átnyúló adatkezelési tevékenységek is találhatóak.

A hatósági listák elfogadása során az Európai Adatvédelmi Testület véleményt bocsát ki a jegyzékkel kapcsolatban, amelyet a honlapján is nyilvánosságra hoz.[44] A véleményt a Testület a GDPR 64. cikk (3) bekezdésében foglaltak alapján nyolc héten belül, tagjainak egyszerű többségével fogadja el. Az ügy összetettségére figyelemmel ez a határidő további hat héttel meghosszabbítható.

Összességében tehát elmondható, hogy az adatvédelmi hatóságok által közzétett listák célja, hogy segítségül szolgáljon az adatkezelőknek ahhoz, hogy könnyebben be tudják előzetesen azonosítani a magas kockázatú, és így hatásvizsgálati kötelezettség alá eső, vagy éppen e kötelezettség alól kivett adatkezeléseket. Ezen felül a listák nyilvánosságra hozatala a GDPR egységes alkalmazását is elősegíti az Európai Unióban.

---

42 Szabó, 2016.

43 Szabó, 2016.

44 A magyar fekete listáról szóló véleményt lásd: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_hu_sas_dpia_list_en.pdf

5.3. A NAIH által összeállított kötelező hatásvizsgálati jegyzék elemei

A NAIH által összeállított és az Európai Adatvédelmi Testület által véleményezett jegyzék az alábbiakban felsorolt elemeket tartalmazza (a. – x. pontok). Fontos ismét hangsúlyozni, hogy a listán szereplő adatkezelések nem jelentik azt, hogy csak ezekben az esetekben kell az adatkezelőnek hatásvizsgálatot lefolytatnia, hiszen a listán szereplő elemeken kívül is előfordulhatnak olyan típusú adatkezelések, amelyek magas kockázattal járnak. A listán szereplő elemek esetében viszont a magas kockázati besoroláshoz és így hatásvizsgálat kötelező lefolytatásához nem férhet kétség.

A lista elemei:

a. Ha egy természetes személy egyedi azonosítását célzó biometrikus adatának kezelése módszeres megfigyelésre irányul.
Ezzel az elemmel kapcsolatban arra szükséges felhívni a figyelmet, hogy önmagában a biometrikus adatok kezelése nem feltétlenül esik kötelező hatásvizsgálat alá, mivel a kezelésük önmagában nem minden esetben jelent magas kockázatot. Ezért a listában is a biometrikus adatok kezelése csak abban az esetben estik kötelező hatásvizsgálat alá, hogy azok kezelése az egyén módszeres megfigyelésére irányul.

b. Ha kiszolgáltatott helyzetben lévő érintettekkel – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos egyedi azonosítását célzó biometrikus adatkezelése történik.
Ez az elem abban az esetben teszi kötelezővé az adatvédelmi hatásvizsgálat lefolytatását, ha a biometrikus adatok kezelése olyan érintettek egyedi azonosítása céljából történik, akik egyben kiszolgáltatott helyzetben lévőknek minősülnek (például gyermekek, munkavállalók, idősek, mentális betegségben szenvedők).

c. Ha az adatkezelés egy természetes személy genetikai adatainak egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő hozzákapcsolásával jár.
Ez a pont csak abban az esetben teszi kötelező a genetikai adatok kezelésével kapcsolatban hatásvizsgálat lefolytatását, ha a genetikai adatokat az adatkezelés során összekapcsolják más különleges vagy fokozottan személyes jellegű adatokkal. Például ilyen tevékenység lehet, ha az érintettől felvett genetikai adatokat az elemzésük során valamilyen korábbi (akár a családban korábban előforduló) betegséggel kapcsolatos egészségügyi adatokkal vetik össze.

d. Ha egy természetes személy genetikai adatai kezelésének célja a természetes személy értékelése vagy pontozása.
Az előző ponthoz hasonlóan itt is a genetikai adatok kezeléséhez kapcsolódón társít a lista hatásvizsgálati kötelezettséget. Ebben az esetben azonban az adatok kezelésének célja az értékelés vagy pontozás. Például a genetikai adatok elemzése bizonyos tulajdonságok (például várható sportteljesítmény) felmérése, elemzése és értékelése céljából. Az adatokból csupán általános genetikai következtetések levonása még nem feltétlenül eredményez hatásvizsgálati kötelezettséget.

e. Pontozás: az adatkezelés célja, hogy az érintett bizonyos tulajdonságait felmérje. A felmérés eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.
A pontozásos rendszerek lényege, hogy az érintettek tulajdonságait mérik fel, és ezek alapján besorolják őket bizonyos előre meghatározott vagy akár dinamikusan változó kategóriákba, osztályokba. A pontozás akár teljesítményalapú is lehet. Az érintettek részére nyújtott szolgáltatás is differenciál közöttük, és eltérő tartalmú vagy minőségű lehet. Például egy online játékban a rendszer a játékosok játékon belüli teljesítményét folyamatosan megfigyeli és korábbi eredményeik alapján rangsorolja őket, majd ezek után hasonló képességű ellenfelekkel sorsolja össze őket.

f. Hitelképesség értékelése: az adatkezelés célja, hogy az érintett hitelképességét felmérje a személyes adatok nagyszámú, illetve módszeres értékelése útján.
A hitelintézeteknek van jogszabályi felhatalmazásuk a hitelképesség felmérésére, ellenben például más ilyen típusú adatokat kezelő szervezeteknek, például egy követeléskezelő cégnek nincs erre jogszabályi felhatalmazása. Ennek a tevékenységnek a nagyszámú érzékeny, pénzügyi adat kezelése és értékelése miatt magas az adatvédelmi kockázata. Jogszabályi felhatalmazás hiányában pedig a hatásvizsgálat adatkezelő általi lefolytatásától nem lehet eltekinteni. A NAIH által lefolytatott, követeléskezelőkkel kapcsolatos hatósági eljárások tapasztalata szerint például a követeléskezelő cégek információszerző tevékenysége kiterjed az adós gazdasági helyzetére, családi környezetére, az egészségi állapotára, de akár bűnügyi előéletére is.[45]

g. Fizetőképesség értékelése: az adatkezelés célja, hogy az érintett fizetőképességét felmérje a személyes adatok nagyszámú, illetve módszeres értékelése útján.
A probléma általában itt is jogszabályi felhatalmazás hiánya, amely miatt az ilyen, nagyszámú érzékeny adatot érintő adatkezelést tervező adatkezelő nem mentesülhet a hatásvizsgálat lefolytatása alól.

h. Harmadik személytől gyűjtött adatok további felhasználása: az adatkezelés célja, hogy a harmadik személytől begyűjtött személyes adatokat felhasználják az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.
Ennek a pontnak a tartalma nem a GDPR 6. cikk (4) bekezdésére vonatkozik, ez ettől elkülönülő adatkezelési művelet. Ebben az esetben az adatkezelőn és az érintetten kívül megjelenik a jogviszonyban egy harmadik személy is, aki nem azonos az érintettel. Ezen harmadik személytől származó adatokat használja fel arra az adatkezelő, hogy az érintettre vonatkozóan hozzon meg egy döntést, nevezetesen, hogy tőle a szolgáltatást megtagadja, vagy a meglévő szolgáltatást megszüntesse.

i. Diákok, hallgatók személyes adatainak értékelésre való felhasználása: az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép-vagy felsőfokú.
Ez a pont az alap-, közép- vagy felsőoktatásban tanuló diákok személyes adatainak kezelését teszi abban az esetben előzetesen hatásvizsgálat kötelezetté, ha a cél a felkészültségük, teljesítményük vizsgálata és alkalmasságuk megállapítása, rögzítése. Ilyen adatkezelésre lehet példa az iskolában egy elektronikus vizsgáztatási rendszer alkalmazása.

j. Profilozás: az adatkezelés célja személyes adatok nagyszámú, illetve módszeres értékelése révén végzett profilozás, különösen, ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.
A GDPR 4. cikk 4. pontja tartalmazza a profilalkotás fogalmát, amely szerint ennek minősül a **„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.”** A profilalkotás önmagában nem hatásvizsgálat kötelezett tevékenység, de ha annak során nagy számban kerül sor érzékeny adatok (például munkahelyi teljesítménnyel kapcsolatos, egészségi állapotra vonatkozó, tartózkodási helyre és mozgásra vonatkozó stb.) feldolgozására és azok értékelésére, úgy a hatásvizsgálat lefolytatása kötelező lesz.

[45] Lásd például: https://naih.hu/files/NAIH-2018-3102-6-hatarozat.pdf és https://naih.hu/files/NAIH-2018-3102-1-hatarozat.pdf

k. Csalás elleni fellépés: az adatkezelés célja hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázis felhasználása ügyfelek szűrésére.
Ez a pont a csalás elleni fellépéssel kapcsolatos adatkezelést abban az esetben teszi hatásvizsgálat kötelezetté, ha az egyébként nem konkrét jogszabályi felhatalmazáson alapul (például ezért nem ilyen a NAV pénzmosás elleni tevékenysége).

l. Okosmérők: az adatkezelés célja közműszolgáltatók által telepített „okosmérők" alkalmazása (fogyasztási szokások nyomon követése).
Az úgynevezett okosmérő használatának alapja, hogy a hagyományos mérőkkel ellentétben folyamatosan regisztrálják a pillanatnyi teljesítményfelvételt fogyasztói oldalon. Ezen óriási adatmennyiséget nem a készülékek tárolják, hanem valamilyen kommunikációs csatornán eljuttatják egy adatközpontba. Itt a begyűjtött adatokat – többek között – a fogyasztói szokások elemzésére használják, és ezzel összefüggésben energiagazdálkodási célokból kezelik.

m. Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.
Ennél a kategóriánál a GDPR 22. cikkében szereplő, egyedi ügyekben végrehajtott automatizált döntéshozatal mint adatkezelési forma alkalmazása tartozik hatásvizsgálati kötelezettség alá, ha az ilyen típusú adatkezelés egyének kirekesztését vagy hátrányos megkülönböztetését eredményezi. Fontos, tehát hogy önmagában egy automatizált döntéshozatalt használó rendszer nem esik hatásvizsgálati kötelezettség alá, csak ha az általa hozott döntéseknek ilyen eredménye is lehet. A 29-es Munkacsoport vonatkozó ajánlásban ilyen típusú adatkezelésnek tekinti, ha például olyan döntések születhetnek, amelyek befolyásolják az egyén egészségügyi szolgáltatásokhoz való hozzáférését, vagy befolyásolják valakinek az oktatáshoz való hozzáférését, például: egyetemi felvételét. Ide tartozhat az államhatár átlépéséhez való joggal kapcsolatos döntés meghozatala is, ha azt automatikus úton hozzák.[46]

n. Módszeres megfigyelés: érintettek nagyszámú és módszeres megfigyelése jellemzően közterületeken vagy nyilvános helyeken kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (például Wi-Fi tracking, Bluetooth tracking, testkamera).
A kategóriával kapcsolatban fontos megjegyezni, hogy nem minden térfigyelőkamera-rendszer (vagy akár dróntechnológia) esik automatikusan hatásvizsgálati kötelezettség alá, csak azok, amelyek nagyszámú érintett módszeres megfigyelésére alkalmasak. Így például kötelező a hatásvizsgálat lefolytatása egy nagy bevásárlóközpont, vagy pláza vásárlókat figyelő kamerarendszerével kapcsolatban, azonban egy cég raktárhelyiségét figyelő kamerarendszer esetén – ahol naponta jellemzően csak ugyanaz a kisszámú érintett fordul meg – már nem lesz az.

o. Helymeghatározási adatok kezelése, ha az módszeres megfigyelésre vagy profilalkotásra utal.
A helymeghatározással kapcsolatos adatok kezelése csak akkor esik hatásvizsgálati kötelezettség alá, ha azokat azon célokból is felhasználják, hogy az érintett viselkedését, tulajdonságait is megfigyeljék, elemezzék, továbbá az is, ha a gyűjtött adatok alapján profilt hoznak létre róluk. Például korábbi étteremlátogatásokhoz kapcsolódó helyadatok elemzése alapján hasonló árkategóriát/konyhát képviselő környékbeli éttermek ajánlása a felhasználónak.

[46] Lásd: WP29 véleménye az automatikus döntéshozatalról és a profilalkotásról. WP251rev01., 2017. https://naih.hu/files/wp251rev01_hu.pdf

p. Munkavállaló(k) munkájának megfigyelése: az adatkezelés célja a munkavállaló munkájának megfigyelése során a munkavállaló személyes adatainak nagyszámú és módszeres feldolgozása, illetve értékelése.
A lista alapján ilyenre lehet példa GPS megfigyelő autóban történő elhelyezése annak ellenőrzése céljából, hogy a munkavállaló mely partnerek/ügyfelek címeit látogatta munkaidőben. Az egyértelmű magas kockázatot a kategória esetén a munkavállaló mint kiszolgáltatott helyzetben lévő érintetti kör érintettsége és személyes adataik kiterjedt és módszeres kezelése adja.

q. Különleges adatok nagy számban való kezelése.
Ezen elemmel kapcsolatban a lista is hivatkozik kivételszabályként a GDPR (91) preambulumbekezdésére, amely alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik. Ezen kivételszabályt leszámítva a különleges adatok kezelése azonban minden esetben hatásvizsgálati kötelezettség alá esik, ha nagyszámú érintettre vonatkozik.

r. Nagyszámú személyes adatok kezelése bűnüldözési célból.
A bűnüldözési célú adatkezelés fogalmát, nem a GDPR, hanem az Infotv. 3. § 10a. pontja határozza meg az alábbiak szerint: **„a jogszabályban meghatározott feladat- és hatáskörében a közrendet vagy a közbiztonságot fenyegető veszélyek megelőzésére vagy elhárítására, a bűnmegelőzésre, a bűnfelderítésre, a büntetőeljárás lefolytatására vagy ezen eljárásban való közreműködésre, a szabálysértések megelőzésére és felderítésére, valamint a szabálysértési eljárás lefolytatására vagy ezen eljárásban való közreműködésre, továbbá a büntetőeljárásban vagy szabálysértési eljárásban megállapított jogkövetkezmények végrehajtására irányuló tevékenységet folytató szerv vagy személy (a továbbiakban együtt: bűnüldözési adatkezelést folytató szerv) ezen tevékenység keretei között és céljából – ideértve az ezen tevékenységhez kapcsolódó személyes adatok levéltári, tudományos, statisztikai vagy történelmi célból történő kezelését is – […] végzett adatkezelése."** A lista tehát e célnak megfelelő, az illetékes bűnüldöző hatóságok által végzett adatkezelést vonja hatásvizsgálati kötelezettség alá, ha egyben az nagyszámú érintett adatára vonatkozik.

s. Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő kezelése: például gyermekek, idősek, mentális betegségben szenvedők esetében.
A kiszolgáltatott helyzetben lévők személyes adatainak nagyszámú kezelése jelenti ebben a helyzetben is a magas kockázati tényezőt, azonban fontos plusz követelmény még az eredeti céltól eltérő kezelés is, amely miatt az hatásvizsgálatot igényel.

t. Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.
A gyermekek mint kiszolgáltatott helyzetben lévő érintetti kör adatainak kezelése sok esetben magas kockázatot eredményezhet, amire jó példa a lista ezen pontja, amely a GDPR 22. cikkén alapuló automatikus döntéshozatalt és profilalkotást használó adatkezeléseket vonja kötelező hatásvizsgálat alá. Ezen felül a gyermekek adatainak marketing célú kezelése vagy információs társadalommal összefüggő szolgáltatás ajánlása is ebbe a kategóriába tartozik.

u. Új technológiai megoldások használata az adatkezelés során.
A lista e pontja ide érti az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelését (például okos televízió, okos háztartási eszközök, okos játékok stb.), amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére, és amelyek alapján profilalkotás történik. A kategóriával kapcsolatban meg kell továbbá jegyezni, hogy az új technológiaként való minősítés megítélése az adott időszak és kor technológiai fejlettsége függvényében változik.

v. Egészségügyi adatokra vonatkozó adatkezelések. Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magánegészségügyi szolgáltatók vagy nagyszámú páciensi körrel rendelkező természetgyógyászok által kezelt különleges adatok vonatkozásában. Ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelését is.
Abban az esetben teszi a hatásvizsgálat lefolytatását kötelezővé az egészségügyi adatok kezelése tekintetében, ha azok nagyszámú érintettre vonatkoznak (például kórházak, egészségügyi szolgáltatók, de akár sportlétesítmények is ide tartozhatnak).

w. Amikor több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek.
A lista itt gyakorlatilag az olyan, több adatkezelő által végzett közös adatkezeléseket teszi hatásvizsgálat kötelezetté, ahol különleges adatok kezelésére is sor kerül valamilyen egységes, összekapcsolt rendszer keretein belül. A lista itt nem tartalmazza a „nagyszámú" kitételt, mivel a nagyobb ágazatok által közösen használt platform önmagában is nagyszámú adatkezelést feltételez. Erre tekintettel nem lényeges a nagyszámú kritérium feltüntetése.

x. Az adatkezelés célja a különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása.
A lista ezen utolsó kategóriája az „adatbányászatra", illetve „big data"[47] alapú adatkezelésekre jellemző módszereket vonja hatásvizsgálati kötelezettség alá. Az ilyen típusú adatkezelések során különböző adatbázisokból származó, jellemzően nagy mennyiségű személyes adatot elemeznek automatikus, algoritmikus úton, amely során közös mintákat, megfeleléseket keresnek az adatokban. Az összehasonlítás során létrejövő mintákat, eredményeket aztán a meglévő szolgáltatások tökéletesítéséhez, továbbfejlesztéséhez használják fel jellemzően, vagy teljesen új célú adatkezeléseket építenek rájuk. Klasszikus példa ilyen tevékenységre a bűnügyi, rendőrségi nyilvántartásokban szereplő adatok összehasonlítása egészségügyi szolgáltatóktól származó adatokkal a mentális betegségek és a bűnözés kapcsolatának kutatása céljából.

[47] A Wikipédia vonatkozó szócikke alapján a big data fogalma alatt azt a komplex technológiai környezetet (szoftvert, hardvert, hálózati modelleket) értjük, amely lehetővé teszi olyan adatállományok feldolgozását, amelyek annyira nagy méretűek és annyira komplexek, hogy feldolgozásuk a meglévő adatbázis-menedzsment eszközökkel jelentős nehézségekbe ütközik. Leegyszerűsítve, a big data mint fogalom a nagy mennyiségű, nagy sebességgel változó és nagyon változatos adatok feldolgozásáról szól.

6. AZ ELŐZETES KONZULTÁCIÓ A FELÜGYELETI HATÓSÁGGAL

6.1. Előzetes konzultáció a felügyeleti hatósággal az adatkezelő részéről

A GDPR bizonyos esetekben az adatvédelmi hatásvizsgálat lefolytatásával kapcsolatban kötelezően előírja az előzetes konzultációt az adott tagállam adatvédelmi hatóságával (Magyarországon a NAIH-val).

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 [36. cikk (1) bekezdés és (94) preambulumbekezdés].

Az adatvédelmi hatásvizsgálat eredményéről a fentiek alapján tehát előzetesen konzultálni kell az adatvédelmi 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 rendelet 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 GDPR-ban 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:

- Adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén.
- A tervezett adatkezelés céljairól és módjairól.
- Az érintettek a rendelet értelmében fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról.
- Adott esetben, az adatvédelmi tisztviselő elérhetőségeiről.
- A rendelet 35. cikke szerinti adatvédelmi hatásvizsgálatról.
- A felügyeleti hatóság által kért minden egyéb információról.

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, hogy – szükség esetén kérésre – segíteniük kell az adatkezelőt abban, hogy teljesüljenek az adatvédelmi hatásvizsgálatok elvégzéséből és a felügyeleti hatósággal folytatott előzetes konzultációból eredő kötelezettségek [(95) preambulumbekezdés].
A felügyeleti hatóság az előzetes konzultáció keretében a szervezet által már lefolytatott hatásvizsgálat dokumentációjából azt állapítja meg, hogy az adatvédelmi hatásvizsgálat lefolytatása a GDPR vonatkozó rendelkezései, illetve a hatásvizsgálati iránymutatás előírásai szerint történt-e. Továbbá azt vizsgálja, hogy a fennmaradó kockázatok mérséklésében tud-e segítséget nyújtani.
A GDPR 36. cikkének (3) bekezdése tartalmazza azokat az információkat, amelyeket az adatkezelőnek a konzultáció során ismertetnie kell a hatósággal. A hatóság a konzultáció során az adatkezelés tényleges folyamatát vizsgálja, így a benyújtott adatkezelési folyamatok vonatkozásában elsősorban azt nézi, hogy az adatkezelő pontosan azonosítja-e az adatkezelési tevékenységeket, illetve az adatkezelések kockázatait, valamint sikerül-e a kockázatok kezelésére irányuló intézkedéseket meghozni. Továbbá a hatóság vizsgálja, hogy az adatkezelésben érintett adatok körének vizsgálatánál pontosan szét van-e választva a személyes adatok és a különleges adatok kezelése az adatkezelés folyamatában, az adatkezelések jogszerűek és az adatkezelő lefolytatta-e az érdekmérlegelési tesztet. Mint az már az előző fejezetekben is hangsúlyoztuk, az adatvédelmi hatásvizsgálatot többfajta, különböző módszertan segítségével el lehet végezni, de a hatásvizsgálatnál figyelembe veendő szempontok azonosak, hiszen a GDPR meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit.
A hatóság az előzetes konzultáció során mindig hangsúlyozza, hogy a kockázatelemzés a személyes adatok kezelésével összefüggő folyamatokra, adatkezelési műveletekre vonatkozik, amelyek a hatásvizsgálat lefolytatásának eredményeként az érintett jogait és szabadságait érintő kockázatot jelentenek.[48]

6.2. Előzetes konzultáció a felügyeleti hatósággal a jogszabályok előkészítése során

A GDPR 36. cikk (4) bekezdése a felügyeleti hatósággal való előzetes konzultációt kötelezővé teszi a személyes adatok kezeléséhez kapcsolódó, a nemzeti parlament által elfogadandó jogalkotási intézkedésre – vagy ilyen jogalkotási intézkedésen alapuló szabályozási intézkedésre – irányuló javaslat előkészítése során.

[48] NAIH, 2018.

Magyarországon a jogszabálytervezetek adatvédelmi hatásvizsgálatára vonatkozó részletes szabályokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) tartalmazza. Az Infotv. 25/G. § (6) bekezdése mondja ki, hogy kötelező adatkezelés esetén az adatvédelmi hatásvizsgálatot az adatkezelést előíró jogszabály előkészítője folytatja le. Kötelező adatkezelések alatt a törvény a jogszabály előírásain alapuló adatkezeléseket érti. A fentiek alapján tehát egy személyes adatok kezelését is érintő, azt előíró jogszabály előkészítése során a jogszabály előkészítőjének adatvédelmi hatásvizsgálatot kell készítenie.

A 29-es Adatvédelmi Munkacsoport vonatkozó iránymutatása alapján az adatvédelmi hatásvizsgálat eredményéről akkor kell előzetesen konzultálni a 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).

A NAIH az ajánlásra tekintettel csak azokban az esetben tartja szükségesnek az előzetes konzultáció lefolytatását, ha a hatóságvizsgálat megállapítja, hogy a kockázatok továbbra is jelentősek és az adatkezelő nem képes azokat csökkenteni (lásd előző pont). A NAIH 2018. évi parlamenti beszámolója alapján a magyar hatóság ezt az előírást a jogalkotás során elkészítendő adatvédelmi hatásvizsgálatokkal kapcsolatban is irányadónak tekinti, amennyiben a tervezett adatkezeléssel kapcsolatban a GDPR alkalmazandó.[49]

Amennyiben a jogszabálytervezet előkészítése során az előkészítő által lefolytatott adatvédelmi hatásvizsgálat eredménye alapján megállapítható, hogy a tervezett adatkezelés magas kockázatú és az adatkezelő nem képes azokat csökkenteni, úgy a jogszabály előkészítője konzultációt kezdeményez a NAIH-val. Ez az előírás a GDPR tárgyi hatálya alá tartozó adatkezelésekre irányadó. Így a GDPR hatálya szerinti adatkezelések jogszabályban történő előkészítése esetén csak a fennmaradó, az adatkezelő által nem csökkentett kockázatot jelentő adatkezelések esetén van szükség előzetes konzultációra.

Más a helyzet a GDPR hatálya alá nem tartozó, így kizárólagos magyar joghatóság alá tartozó adatkezelésekkel összefüggésben. Ezekkel kapcsolatban az Infotv. 25/H. § (1) és (2) bekezdésében foglaltak határozzák meg az előzetes konzultáció kezdeményezésének feltételeit. A magas kockázatot és ennek megfelelően az előzetes konzultáció szükségességét a kivett adatkezelések közül a bűnüldözési, nemzetbiztonsági és honvédelmi célú adatkezelések esetén vélelmezni kell a törvény alapján. Ezek szerint valamennyi bűnüldözési, nemzetbiztonsági és honvédelmi célú adatkezelést szabályozó jogszabály előkészítése során hatásvizsgálatot kell készítenie az előkészítőnek és konzultálni is kell a NAIH-val.

Mind a GDPR hatálya, mind a kizárólag magyar joghatóság alá tartozó adatkezelésekkel kapcsolatos jogszabályok előkészítése során fontos, hogy amennyiben előzetes konzultációra kerül sor, úgy azt a hatóság a jogszabály előkészítőjével (ez legtöbbször az illetékes minisztérium) folytatja le. Amennyiben az előkészítés folyamata már lezárult, így jogszabálytervezet már benyújtásra került a parlamentnek elfogadásra, vagy azt esetleg már ki is hirdették, úgy a konzultációs eljárás is lezárul, annak továbbfolytatására az elfogadást követően nincs lehetőség.

6.2. A jogszabály előkészítése során készített adatvédelmi hatásvizsgálat tartalmi kritériumai

A jogszabálytervezet szövegéhez mellékelt adatvédelmi hatásvizsgálati dokumentációval kapcsolatban az Infotv. 25/G. § (5)-(6) bekezdései csupán annyit írnak elő, hogy annak tartalmaznia kell a tervezett adatkezelési műveletek általános leírását, az érintettek alapvető jogainak érvényesülését fenyegető,

[49] NAIH, 2018.

az adatkezelő által azonosított kockázatok leírását és jellegét, az e kockázatok kezelése céljából tervezett, valamint a személyes adatokhoz fűződő jog érvényesülésének biztosítására irányuló, az adatkezelő által alkalmazott intézkedéseket. A jogszabályok előkészítése során elkészített adatvédelmi hatásvizsgálati dokumentációnak tehát elvileg pontosan ugyanazokat az elemeket kell tartalmaznia, mint az adatkezelők által lefolytatott hatásvizsgálatnak.

A hatásvizsgálati dokumentációnak a jogszabály tervezetében meghatározott, előrelátható, konkrét adatkezeléseket kell leírnia (például az adatkezeléshez használt rendszerek működése, használata stb.) valamint azt, hogy az ezzel kapcsolatban kialakult konkrét és beazonosított kockázatokat hogyan kívánja az adatkezelő mérsékelni. Nem elég tehát, ha a hatásvizsgálatban leírják általánosságban, hogy „személyiséglopás kockázata fennáll", hanem le kell írni pontosan, hogy az adott adatkezelés kapcsán ez hogyan következhet be (például jogosulatlan külső támadó hozzáférhet a rendszergazda jelszavához). Az azonosított kockázatok elhárítására tett intézkedéseket is konkrétan le kell írni a hatásvizsgálati dokumentációban (például havonta megváltoztatandó, szoftveresen kikényszerített erős jelszavak használata a bejelentkezéseknél).

A konkrét kockázatok beazonosítására természetesen a jogszabály előkészítője saját hatáskörben a legtöbbször nem képes, mivel nincsen minden információ birtokában az adatkezeléssel kapcsolatban. Ennek feloldására a majdani adatkezelővel való konzultációra lehet szükség, és adott esetben fel kell kérnie arra, hogy egészítse ki észrevételeivel a hatásvizsgálati dokumentációt.

Természetesen az is előfordulhat, hogy a jogalkotás adott szakaszában még az adatkezelésből eredő konkrét kockázatok nem azonosíthatóak be (például a jogszabályszöveg csak egy általános felhatalmazást tartalmaz az adatkezeléssel kapcsolatban). Ebben az esetben egyértelműen utalnia kell a jogalkotónak a hatásvizsgálati dokumentációban erre a körülményre, és a hatásvizsgálat kiegészítésének jövőbeli kötelezettségéről kell döntenie (például az adatkezelő megbízásával a teljes értékű hatásvizsgálat lefolytatására a rendszer beüzemelése és a technikai paraméterek kialakítása előtt).[50]

[50] NAIH, 2018.

7. IRODALOMJEGYZÉK

1. 29-es Adatvédelmi Munkacsoport (WP29) (2017): 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: 2019. október 1.)
2. A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) Beszámolója a 2018. évi tevékenységéről (B/4542). Elérhetőség: https://naih.hu/files/Beszamolo-2018-MR.PDF (utolsó letöltés: 2019. október 1.)
3. Balogh Zsolt György et al. (2014): Az adatvédelmi hatásvizsgálat módszertana. Médiakutató: Médiaelméleti Folyóirat, XV. évf. 4. szám. Elérhetőség: http://epa.oszk.hu/03000/03056/00057/pdf/EPA03056_mediakutato_2014_tel_077-092.pdf (utolsó letöltés: 2019. október 1.)
4. Bieker, Felix et al. (2016): A process for data protection impact assessment under the European General Data Protection Regulation. Springer International Publishing Switzerland, APF, LNCS 9857, Karlsruhe. Elérhetőség: http://www.springer.com/cda/content/document/cda_downloaddocument/9783319447599-c2.pdf?SGWID=0-0-45-1587701-p180200777 (utolsó letöltés: 2019. október 1.)
5. Comission Nationale de l'Informatique et des Libertés (CNIL) (2012): Methodology for Privacy Risk Managment. Translation of June 2012 edition. Elérhetőség: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf (utolsó letöltés: 2019. október 1.)
6. Commission Nationale de l'Informatique et des Libertés (CNIL) (2015): Privacy Impact Assessment: Methodology (how to carry out a PIA). Elérhetőség: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (utolsó letöltés: 2019. október 1.)
7. Európai Uniós Hálózati- és Információbiztonsági Ügynökség (ENISA) (2013): Ajánlás az adatvédelmi incidensek súlyosságának felmérésére szolgáló módszerről. Elérhetőség: https://www.enisa.europa.eu/publications/dbn-severity (utolsó letöltés: 2019. október 1.)
8. Information Commissioner's Office (ICO) (2014): Conducting Privacy Impact Assessments Code of Practice. ICO. Elérhetőség: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (utolsó letöltés: 2019. október 1.)
9. Péterfalvi Attila – Révész Balázs – Buzás Péter (szerk.) (2018): Magyarázat a GDPR-ról. Wolters Kluwer Hungary Kft., Budapest.
10. Szabó Endre Győző (2016): 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: 2019. október 1.)
11. Wright, David – De Hert, Paul (2012): Privacy Impact Assessment. Springer Science and Business Media B.V., Springer Dordrecht, Heidelberg–London–New York.

A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert rektorhelyettes

Címe:
1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Császár-Biró Anna

Tördelőszerkesztő:
Friebert Máté

ISBN 978-963-498-235-7 (elektronikus)