Balogh Zsolt György – Böröcz István – Kiss Attila – Polyák Gábor – Szőke Gergely László

Az adatvédelmi hatásvizsgálat módszertana[1]

Az európai adatvédelmi reform során a technológiai forradalom által vezérelt társadalmi változásokra is reagálva olyan általános előírások fogalmazódtak meg, amelyek biztosíthatják az átlátható és arányos adatkezelést. Az új előírások között is egyre nagyobb hangsúlyt kap az angolszász jogrendszerekben a közszféra egyik kiemelkedő fontosságú – részben – önszabályozó módszere, az adatvédelmi hatásvizsgálat. A hatásvizsgálat fontos eleme lehet a személyes adatok védelmének, mivel célja az azokat érintő, a magánszférát veszélyeztető eljárások azonosítása és teljes vagy részleges kiküszöbölése. A vizsgálat céljából kiindulva annak lefolytatásában érdekelt lehet minden személyes adatot kezelő telekommunikációs cég is.

1. Bevezető: Az adatvédelmi reform

A közelmúlt társadalmi és technológiai tendenciáira válaszul az Európai Unió megkezdte a közösségi adatvédelmi szabályozás reformját.[2] A szabályozás új irányainak meghatározása során számos olyan új elv és jogintézmény gondolata jelent meg, amelynek célja egyebek között az adatkezelő felelősségének növelése, valamint egy világos és átlátható adatkezelési metodológia érvényre juttatása. A rendelettervezet holisztikus felfogásából adódóan és a technológiai forradalom által vezérelt társadalmi változásokra is reagálva olyan általános előírásokat fogalmaz meg, mint az adatkezelő felelősségre vonhatóságának szabályai, a beépített adatvédelem és az adatvédelmi hatásvizsgálat, amelyek biztosíthatják az átlátható és arányos adatkezelést (Szőke, 2013). A kitűzött célok elérése nagyban függ az új elvek megfelelő alkalmazásától, betartásától és hatékony felügyeletétől. Ebben az adatvédelmi hatásvizsgálat (Privacy Impact Assessment, PIA) nagy segítség lehet (Wright & De Hert, 2012).

E tanulmány célja az európai adatvédelmi reform során is egyre nagyobb hangsúlyt kapó, az angolszász jogrendszerekben a közszféra egyik kiemelkedő fontosságú – részben – önszabályozó módszerének, az adatvédelmi hatásvizsgálat módszertanának bemutatása. A hatásvizsgálat fontos eleme lehet a személyes adatok védelmének, mivel célja az azokat érintő, a magánszférát veszélyeztető eljárások azonosítása és teljes vagy részleges kiküszöbölése.

Az adatvédelmi hatásvizsgálat módszertanának elemzése előtt szükséges néhány terminológiai kérdés tisztázása. A jogirodalomban eleinte a privacy-hatásvizsgálat (*Privacy Impact Assessment*, PIA) kifejezés terjedt el, újabban azonban megjelent – és a rendelettervezetben is így szerepel – az adatvédelmi hatásvizsgálat, angol nyelvű szóhasználatával a *Data Protection Impact Assessment* (DPIA) kifejezés is.[3] Az elnevezésbeli különbség egyebek között az általános személyiségvédelem amerikai és európai fejlődési modelljei közötti eltérésben gyökerezik. Míg az Egyesült Államokban a személyiségi jogi védelem a magánszférához való jog *(right to privacy)* keretein belül teljesedett ki, addig Európában a titokszféra védelme, majd az adatvédelem vált annak meghatározó elemévé (Sólyom, 1983).

1 A tanulmány alapjául szolgáló kutatás az Európai Unió és Magyarország támogatásával, az Európai Szociális Alap társfinanszírozásával a TÁMOP-4.2.2.C-11/1/KONV-2012-0005 azonosító számú „Jól-lét az információs társadalomban" című kiemelt projekt keretei között valósult meg.

2 Európai Bizottság: Javaslat - Az Európai Parlament és a Tanács Rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet) Brüsszel, 2012.1.25. COM(2012) 11 végleges, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:HU:PDF (utolsó letöltés: 2013. X. 10.), a továbbiakban rendelettervezet.

3 A terminológiai különbségek oka az, hogy az angolszász jogrendszerekben valóban a magánszférára gyakorolt hatásokat vizsgálják, míg az európai adatvédelmi rezsimbe a jogintézmény szűkebb hatókörrel, a személyes adatok védelmére vonatkoztatva, adatvédelmi hatásvizsgálatként importálható.

2. Történeti visszatekintés

A PIA egy, egyebek között az OECD adatkezelési elvein[4] alapuló módszertan, amelynek célja olyan projektek, programok, termékek, szolgáltatások (továbbiakban: projekt) vizsgálata, amelyek egy meghatározott mértéken túl is hatást gyakorolnak a magánszférára.[5] A hatásvizsgálat az angolszász jogrendszerű országokban alakult ki, ahol ma is elsősorban a magánszférát érintő kormányzati és közigazgatási döntéshozatali eljárások szerves részét képezi (Simon, 2008), azonban többnek mondható egy egyszerű eszköznél. Paul De Hert definíciója szerint a PIA olyan módszer, amely felméri egy projekt, policy, program, szolgáltatás vagy más kezdeményezés (a továbbiakban e tanulmányban: projekt) magánszférára gyakorolt hatásait abban az esetben, amennyiben személyes adatok kezelésére kerül sor, valamint az érintettekkel egyeztetve a negatív hatások elkerülése vagy csökkentése érdekében ajánlásokat fogalmaz meg (Wright & De Hert, 2012).[6]

A PIA mint koncepció gyökerei Ausztráliában, Kanadában és az Egyesült Államokban találhatók; kialakulásuk az 1990-es évek derekára tehető (Wright & De Hert, 2012). A PIA Európai Uniós bevezetésének lehetőségét vetítették előre az Európai Bizottság 2010-ben kiadott állásfoglalásai az adatvédelmi reform előkészületei során.[7] Ezek egyik állomásaként, a Bizottság ajánlásával összhangban a 29. cikk szerinti munkacsoport 2011 februárjában elfogadta az RFID PIA keretszabályozást.[8] A PIA a rendelettervezetbe is bekerült, a vonatkozó rendelkezések „Az adatkezelés teljes időtartamára kiterjedő adatvédelmi irányítás" című fejezetben találhatók.

Jelenleg intézményesített adatvédelmi hatásvizsgálat az Egyesült Államokban, Kanadában, Ausztráliában, Új-Zélandon, Hong Kongban, Írországban és Nagy-Britanniában van. Habár az egyes angolszász országokban 2009 óta egyre szélesebb körben alkalmazzák, az elmúlt évek tapasztalatai és kutatásai alapján megállapítható, hogy nem létezik egységes módszertan, és az egyes országok jogi és kulturális különbségei jelentős mértékben befolyásolják a PIA karakterisztikáját. A PIA jogforrásainak szintjei között is vannak eltérések – míg egyes országok (például Kanada, Új-Zéland, Egyesült Államok) *hard law*-eszközökkel szabályozzák, máshol a *soft law*-eszközök is elegendőnek bizonyulnak (Wright et al., 2011, Böröcz, 2014).

Az 1. táblázatból látható, hogy a kialakult PIA-módszertannal rendelkező országok gyakorlata között is komoly eltérések vannak, elég kiemelni az érintettekkel való konzultáció támogatását, a hatásvizsgálat alanyi körét, vagy a független, külső felülvizsgálat intézményének támogatását.

3. Az adatvédelmi hatásvizsgálat előnyei, indokoltsága

Az adatvédelmi hatásvizsgálat lefolytatásának az érintett projekt tervezői számára számos funkcionális előnye van, amelyek egyebek között a következők:

- kockázatkezelés, amely magában foglalja a kockázatos elemek azonosítását és azok csökkentését/megszüntetését;
- egy sajátos figyelmeztető rendszer, amely rávilágít a magánszférát érintő problémákra;
- költséghatékony megoldások kialakítása;
- polgári jogi felelősségre vonás[9] és egyéb szankciók elkerülése;
- a privacy-tudatosság hangsúlyozása kiváló reklámlehetőség;[10]
- érintett nézőpontjának megértése (De Hert et al., 2012).

4 Az OECD 1980-ban alkotta meg a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról szóló irányelveit. Ezekről lásd bővebben: http://www.oecd.org/sti/ieconomy/15590228.pdf (utolsó letöltés: 2014. II. 15.).

5 A rendelettervezet 32a. cikke részletesen meghatározza azokat az eseteket, amelyek különös kockázatot jelentenek az érintett személyes adatainak kezelése során.

6 További információs kísérleteket lásd még Clarke (2011).

7 Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A személyes adatok Európai Unión belüli védelmének átfogó megközelítése COM(2010) 609 végleges, Brüsszel, 2010.11.04., http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf (utolsó letöltés: 2014. III. . 10.).

8 A 29. cikk szerinti adatvédelmi munkacsoport 5/2010. számú véleménye a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló ágazati javaslatról, WP 175, 2010. július 13., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_hu.pdf (utolsó letöltés: 2013. VI. 15.).

9 Jellemzően kártérítési kötelezettség.

10 Ahogy az az Egyesült Államokban bevett gyakorlat, bővebben lásd Jóri (2005).

1. táblázat.
PIA-gyakorlatok és policyk közötti hasonlóságok és különbségek
(Wright et al., 2011)

Jellemzők és sajátosságok, amelyekkel a PIA-útmutató rendelkezik	Ausztrália	Victoria	Kanada	Ontario	Alberta	Írország	Új-Zéland	Egyesült Királyság	USA OMB	USA DHS
Megjelenés éve	**2010 máj.**	**2009 ápr.**	**2002 aug.**	**2010 dec.**	**2009 jan.**	**2010 dec.**	**2002-2007 okt.**	**2009 jún.**	**2003 szept.**	**2010 jún.**
A PIA egy eljárás	✓		✓	✓		✓	✓	✓	✓	✓
Kérdéseket tartalmaz a magánszféra-invazív elemek azonosítására	✓	✓	✓	✓		✓	✓	✓		✓
Cégek és a kormány is lehet alanya	✓	✓			✓	✓	✓	✓		
A magánszféra összes típusára vonatkozik	✓	✓		✓						
A PIA-ra a kockázat-kezelés egyik fajtájaként hivatkozik	✓		✓	✓		✓		✓	✓	✓
Azonosítja a magán-szférát érintő veszélyeket	✓	✓	✓	✓		✓	✓	✓		
Stratégiát fogalmaz meg a kockázat-csökkentésre		✓					✓			
Azonosítja a PIA lefolytatásának előnyeit	✓	✓	✓			✓	✓	✓		
Támogatja a külső érintettekkel való konzultációt	✓	✓				✓		✓		
Támogatja a PIA közzétételét	✓	✓	összefogl.		összefogl.		✓	✓	✓	✓
Előzetes vizsgálat, amely meghatározza a PIA szükségességét	✓	✓	✓			✓		✓	✓	✓
Meghatározott felépítést javasol a PIA beszámolóhoz	✓	✓	✓		✓		✓	✓	✓	✓
A „projekt" fogalomba a policy és/vagy a jog-alkotás is beletartozik		✓						✓		
Folyamatosan felül kell vizsgálni a PIA-t a projekt működése során	✓	✓			✓	✓	✓	✓	✓	✓
Kijelenti, hogy a PIA nem egy „compliance-check"	✓	✓	✓	✓				✓		
A PIA policy a beszámo-lóra nézve független felülvizsgálatot biztosít			✓		✓		✓		✓	✓
A PIA alapja jog, kormányzati politika, vagy a költségvetés benyújtását kíséri			✓	✓	✓	✓		✓	✓	✓
A PIA-beszámolót a szervezet vezetőjének kell aláírnia (felelősségre vonhatóság miatt)		✓	✓	✓	✓	✓			✓	✓

Amennyiben a hatásvizsgálatot még a korai, tervezési szakaszban lefolytatják, képes kimutatni az egyes kockázatokat, amivel el lehet kerülni a projekt esetleges kudarcát, illetve a későbbi módosítási (többlet)feladatokat (Simon, 2008). Ennek jelentőségét az Adatvédelmi és Privacy Biztosok Nemzetközi Konferenciáján is kiemelték 2009-ben. A találkozó eredményeként létrejött úgynevezett Madrid Resolution 22. f) pontja kiemeli, hogy a tagállamoknak támogatniuk kell az adatvédelmi hatásvizsgálat alkalmazását az új, személyes adatokat kezelő információs rendszerek vagy információs technológiák véglegesítése előtt.[11]

A Privacy Impact Assessment módszertana Európában egyelőre kiforratlan. Az azonban látható, hogy a tagállami hatóságok egybehangzóan támogatják az intézmény bevezetését. A megfelelő gyakorlat kialakítása az Európai Adatvédelmi Testület,[12] a hatásvizsgálatot lefolytatni kívánó piaci szereplők, valamint a tagállami hatóságok feladata lesz, hiszen a rendelettervezet csupán a keretet adja meg általános előírások formájában, azokat is pontatlanul.[13] A vezető szerep e területen a piaci szereplőké lehet, a tagállami hatóságok a meglévő jelentős munkaterhük mellett (Schütz, 2012) elsősorban itt is felügyeleti szerepet vállalhatnak.

A továbbiakban egy, a különböző országok hatásvizsgálatainak legjobb gyakorlatai alapján kialakított DPIA-módszertant mutatunk be. A módszertan segítséget nyújthat olyan személyek/szervezetek számára, akik a rendelettervezet hatályba lépését követően adatvédelmi hatásvizsgálat lefolytatására kötelezettek vagy erre önként vállalkoznak.

4. A hatásvizsgálat elemei

Az egyes országok módszertanai ugyan jelentős különbségeket mutatnak, azonban mindegyikből kiemelhetők azok az elemek, amelyek együttesen egy általános, *best practice*-eken alapuló módszertant alkotnak, és kiinduló pontok lehetnek az eljárást lefolytató szervezetek számára.

Az egyes országok PIA „jó gyakorlatai" alapján egy ideális DPIA eljárás elemei az alábbiak szerint határozhatók meg:

1. A hatásvizsgálat szükségességének meghatározása;
2. Az eljárást lefolytató szerv és a hivatkozási rendszer meghatározása;
3. A projekt bemutatása;
4. Az adatmozgások és egyéb személyes adatokat érintő események vizsgálata;
5. Konzultáció az érintettekkel;
6. Kockázatkezelés;
7. Jogszerűség ellenőrzése;
8. Ajánlások megfogalmazása;
9. A beszámoló előkészítése és bemutatása;
10. Az ajánlások implementálása;
11. Megfelelőségi felülvizsgálat;
12. Lefolytatott vizsgálatok központi nyilvántartása (De Hert et al., 2012).

A rendelettervezet is meghatározza az adatvédelmi hatásvizsgálat főbb elemeit, azonban ezek egy része inkább az adatkezelés katalogizálásáról szól (amit az adatkezelőnek egyébként is meg kellene tennie), más részük azonban valóban segíti az adatkezelés kockázatainak felméréséhez szükséges kritériumok meghatározását.[14] Az ugyanakkor nehezen érthető, hogy a rendelettervezet – több más jogszabályhellyel szemben – miért nem rendelkezik a további, akár a Bizottság, akár a leendő Európai Adatvédelmi Testület által kidolgozandó részletszabályokról.

11 Adatvédelmi és Privacy Biztosok Nemzetközi Konferenciája, Madrid, 2009, Privacy: *Today is Tomorrow – International Standards on the Protection of Personal Data and Privacy*, p. 24, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf (utolsó letöltés: 2014. IX. 9.).

12 Rendelettervezet 64 cikk.

13 Erről bővebben lásd: 5. fejezet.

14 A DPIA keretében végzett kockázatelemzés nem azonos a rendelettervezet 32a pontjában foglalt kockázatértékeléssel, amelynek célja annak megállapítása, hogy az adatkezelés beleesik-e a tervezet által „valószínűsíthetően különleges kockázattal járó" adatkezelési körök valamelyikébe.

4.1. A hatásvizsgálat szükségességének meghatározása

Egy személyes adatokat érintő projekt tervezése során általánosan elvárható, hogy meghatározzák, kategorizálják a kezelendő adatok körét (például a jogszabályi követelményeknek való megfelelés ellenőrzése okán).

A 29. cikk szerinti munkacsoport 5/2010. számú véleményében[15] kiemelte: „...az adatvédelmi hatásvizsgálatnak segítenie kell az adatkezelőket abban, hogy átfogóan kezeljék a magánélet- és adatvédelmi kockázatokat."[16] A munkacsoport olyan eszközként utal rá, amely segít a magánélet-védelmi kockázatok értékelésében és azon megoldások megtalálásában, amelyek képesek garantálni a személyes adatok védelmét, csökkentve így a jogbizonytalanságot és a felhasználók bizalomvesztését.

Az eljárás szükségességének megállapításához egy kérdéssor nyújthat segítséget, amelyet az adatkezelést végző személynek/szervezetnek kell kitöltenie.[17] A kérdőív egyes részei megfelelnek a Rendelettervezet 32a. cikk (1) bekezdésében foglalt „kockázatelemzés" fogalmi ismérveinek. Ez alapján az adatkezelőnek a projekt tervezési szakaszában el kell végeznie a jövőbeni adatkezelésnek az érintett jogaira és szabadságaira gyakorolt lehetséges hatásainak kockázatelemzését, amelynek során vizsgálni kell, hogy az adatkezelés jelent-e különleges kockázatot. Amennyiben igen, a hatásvizsgálatot le kell folytatni,[18] és a kockázatelemzést egy éven belül, illetve – ha az adatkezelési műveletek jellege, alkalmazási köre vagy rendeltetése jelentős mértékben megváltozik, – azonnal felül kell vizsgálni, függetlenül attól, hogy készül-e adatvédelmi hatásvizsgálat vagy sem.[19]

A kockázatelemzést (jelen módszertan alapján a kitöltött kérdőívet) minden esetben dokumentálni kell – ha azonban szükség van hatásvizsgálat lefolytatására, akkor ez a vizsgálat dokumentációjának részét képezi.

4.2. Az eljárást lefolytató szervezet és a hivatkozási rendszer meghatározása

Amennyiben a projektet tervező szervezet nem rendelkezik belső adatvédelmi felelőssel vagy a személyes adatok védelméért felelős szervezeti egységgel, úgy célszerű, ha a hatásvizsgálatot külső személy/szervezet végzi. Ellenkező esetben a vizsgálat hasznossága, értéke és hitelessége jelentős mértékben csökkenhet. Várhatóan elsősorban ügyvédi irodák, tanácsadó cégek fogják ellátni e feladatokat.

Egyes országokban a tagállami adatvédelmi hatóság által lefolytatott hatásvizsgálat is elfogadott. A hatósági hatásvizsgálat lefolytatásával kapcsolatban hasonló aggályok merülhetnek fel, mint a hatóság által végzett auditálással kapcsolatban:[20] előfordulhat, hogy a hatóságnak a saját maga által kialakított adatvédelmi kereteket kell felügyelnie és nem megfelelő adatkezelés esetén szankcionálnia, ami nem példa nélküli,[21] de a „tanácsadás" tartalmáért viselt felelősséget mindenképp célszerű tisztázni.

A hivatkozási rendszert tekintve a jogszabályi háttér főszabály szerint a tagállami joganyag. Ebben az esetben azonban felmerülhet kérdésként a más tagállamban lefolytatott DPIA érvényessége, másik országban történő megfeleltetése. Ehhez esetenként vizsgálni kell a két országban használatos szabályozási és módszertani különbségeket. A rendelettervezet elfogadása jelentősen csökkentheti a tagállami jogi környezet különbségeit, a hatóságok közötti kommunikáció és együttműködés elősegítése pedig a létrehozni kívánt Európai Adatvédelmi Testület egyik fontos feladata lesz „a felügyelő hatóságok közötti együttműködés és a hatékony két- vagy többoldalú információcsere és gyakorlatok cseréjének előmozdítása, beleértve a közös műveletek és más közös tevékenységek koordinálását, amennyiben egy vagy több felügyelő hatóság kérésére így dönt".[22]

---

15 A 29. cikk szerinti adatvédelmi munkacsoport 5/2010. számú véleménye a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló ágazati javaslatról, 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_hu.pdf (utolsó letöltés: 2014. IX. 9.).

16 A 29. cikk szerinti adatvédelmi munkacsoport 5/2010. számú véleménye a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló ágazati javaslatról, WP 175, 2010. július 13., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_hu.pdf, p. 6. (utolsó letöltés: 2014. IX. 9.).

17 Lásd Melléklet. Kérdőív az adatvédelmi hatásvizsgálathoz.

18 Rendelettervezet 32a. cikk (3) c) pont.

19 Rendelettervezet 32a. cikk (4)

20 Erről lásd részletesen Polyák & Szőke (2011).

21 Több európai állam joga is ismeri a hatóság által végzet adatvédelmi audit jogintézményét, illetve hasonló helyzet felmerülhet az irányelv előzetes ellenőrzéssel kapcsolatos szabályainak alkalmazása kapcsán is.

22 Rendelettervezet 66. cikk (1) bekezdés e) pont

4.3. A projekt bemutatása és a hatásvizsgálat hatókörének megállapítása

A projekt bemutatásának két eleme a projekt általános leírása, valamint a felek közötti információcsere formájának és gyakoriságának meghatározása. A projekt tervezője és a hatásvizsgálatot végző szerv között különösen fontos a kommunikáció. Az eljárás csak akkor folytatható le eredményesen, ha a projekt, valamint a hatásvizsgálat minden eleme ismert a felek számára. Ehhez az szükséges, hogy a projekt vezetője részletesen ismertesse a szolgáltatás működési elveit, a személyes adatokat bármilyen formában érintő elemeket, valamint az egyes részelemek alkalmazásának indokoltságát. Mindkét fél érdeke a teljeskörű, az eljárás teljes időtartamára kiterjedő informáltság.

Roger Clarke kritériumai alapján a hatásvizsgálatot megfelelő dokumentumok előkészítésével kell megalapozni, amelyeknek egyebek között a következő tartalmi elemekkel kell rendelkezniük:

- a környezet bemutatása, amelyben a dokumentumok előterjesztése történik (beleértve a szociális, a gazdasági, és a technológiai körülményeket), valamint a projekt céljainak és az azt motiváló elemeknek a leírása;
- a tervezett hatásvizsgálat céljainak kijelölése;
- a vizsgálat alá vont rendszer működésének felvázolása;
- a hatásvizsgálat menetének, illetve további fejlesztési lehetőségek meghatározása (Clarke, 1998);

Jelentős mértékben növeli a vizsgálat hatékonyságát, ha a hatásvizsgálatba bevont érintettek is megértik a projektben felhasznált technológiák működését. Ehhez a dokumentáció, illetve egy részletes leírás hozzáférhetővé tétele szükséges.

A kölcsönös információnyújtás során tisztázni kell továbbá:

- a projekt felelősét,
- a megjelenés/elindítás dátumát,
- a projekt/szolgáltatás célközönségét,
- a szükséges mérföldköveket, úgy, mint a projekt felépítését is érintő döntések (De Hert et al., 2012).

Az információcsere során behatárolhatóvá válik egyebek között az érintett és az adatkezelő közötti kapcsolat, az érintett és a szervezet közötti kapcsolat természete, valamint a személyeket érintő döntések indoka.[23]

Az adatvédelmi hatásvizsgálatot lefolytató szervezet első fontos feladata az immár ismert információk alapján a DPIA hatókörének felmérése, ami alapján reálisan megbecsülhetővé válik a szükséges munkaerő, illetve munkaidő. A vizsgálat terjedelmének egyenes arányban kell állnia az adatvédelemmel kapcsolatos közvetlen kockázatok mértékével. Amennyiben az előzetes felmérések alapján a személyes adatokat érintő intézkedések jelentéktelenek/jelentősek, a hatásvizsgálat terjedelme ennek megfelelően csökkenthető/növelhető. A vizsgált projekt költségvetésének nagysága azonban önmagában nem mérvadó, nem értékelhető magánszférát érintő tényezőként. A vizsgálatnak ki kell terjednie az adatokon végzett bármely műveletre (De Hert et al., 2012).

4.5. Konzultáció az érintett szereplőkkel

A projekt fejlesztőjének azonosítania kell az érintett szereplők *(stakeholders)* lehetséges körét, majd megfelelő mértékben tájékoztatnia kell őket az eljárásról. A tájékoztatás célja – a visszajelzések útján – a negatív hatások csökkentése, illetve a figyelem felhívása a jogorvoslati lehetőségre. A tájékoztatás során ki kell térni az eljárás menetére, idejére, várt eredményére. Az esetleges konzultációt már a tervezési/fejlesztési szakaszban célszerű elvégezni, hogy az érintettek észrevételeit, ajánlásait esetlegesen implementálni lehessen, jelentős többletköltség nélkül. Az érintetti kör nincs korlátozva – a projekt tárgyát tekintve érintett lehet állami és civil szervezet, támogató, szolgáltató, fejlesztő és az adatkezelés adatalanyai egyaránt.

23 Information Commissioner's Office (ICO): Conducting privacy impact assessments code of practice, 2014, http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf, p. 13. (utolsó letöltés: 2014. VIII. 8.).

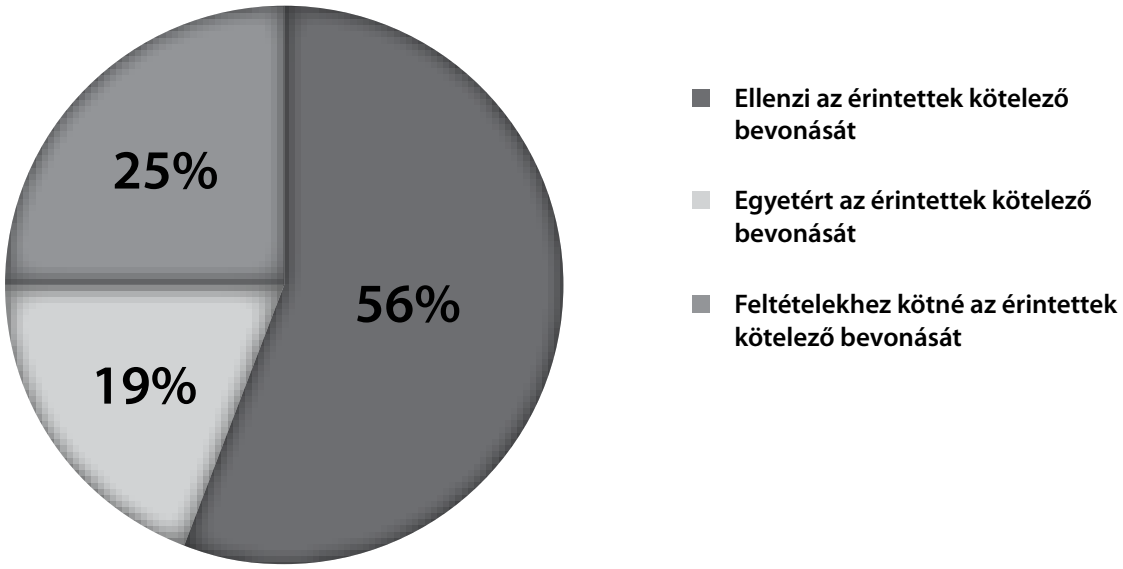
Az érintettek hatásvizsgálatba való bevonására számos lehetőség van:

- az egyes érintetti kategóriák meghatározása és párbeszéd folytatása az egyes kategóriák képviselőivel;
- konzultációs eljárások biztosítása, hogy az érintetteknek lehetőségük legyen álláspontjaik kifejtésére;
- a DPIA tervezetének érintettek számára történő hozzáférhetővé tétele.

A konzultáció formája többféle lehet: interjú, közvélemény-kutatás, meghallgatás, *workshop*, online konzultáció. A tervezett projekt negatív hatásainak csökkentése vagy kiküszöbölése érdekében célszerű a visszajelzéseket dokumentálni és a projekt megvalósítása során figyelembe venni (Clarke, 2011).

Az Uniós tagállamok véleménye megoszlik az érintettek bevonásának szükségességéről. A tagállami adatvédelmi hatóságok többsége nem támogatja az érintettek bevonásának kötelezővé tételét (lásd az 1. ábrát), elkerülhető adminisztrációs teherként hivatkoznak rá, továbbá a döntési jogkört az adott projekt tervezőjének kezében hagynák. Ezt a tendenciát igazolja a rendelettervezet szövegének Állampolgári Jogi, Bel- és Igazságügyi Bizottság (továbbiakban: LIBE – Bizottság) általi, 2013. októberi felülvizsgálata. A normaszövegből kikerült az érintettek vagy képviselőik véleményének kikérése a tervezett adatfeldolgozással kapcsolatban.[24] A vélemény kikérését a LIBE – Bizottság az adatkezelőkre nézve aránytalan teherként értékelte.[25]

1. ábra
Forrás: Hosein & Davies (2012: 16)



24 Rendelettervezet 33. cikk (4) bekezdés

25 Állampolgári Jogi, Bel- és Igazságügyi Bizottság jelentése a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendeletre (általános adatvédelmi rendelet) irányuló javaslatról (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 2013., http://www.tisztessegesadatkezeles.hu/letoltes/tkMQJ7RbxxzG0E2B1tz0rOu2UZX [2014.07.10.]

4.6. Kockázatkezelés

A DPIA központi eleme kétségkívül a kockázatelemzés, amely régóta működő megközelítési mód a legkülönfélébb területeken. Az adatvédelmi hatásvizsgálat módszertana során így célszerű lehet a kockázatelemzésre más területeken kialakított, sokszor szabványként is megjelenő módszerekből kiindulni (De Hert et al., 2012).[26]

A kérdőívek kitöltése, valamint az egymással, illetve az érintettekkel történő konzultáció után a hatásvizsgálatot lefolytató szerv a projekt minden releváns részelemének ismeretében elvégzi a kockázatkezelést, amelynek elemei az alábbiak:

1) a lehetséges kockázati tényezők azonosítása,
2) a kockázati tényezők értékelése,
3) a kockázati tényezők csökkentésére, megszüntetésére irányuló javaslatok megfogalmazása.

A kockázatkezelés sikeressége függ az azt megalapozó módszertan kidolgozottságától, valamint a hatásvizsgálatot végző személy(ek) szakértelmétől. A kockázati tényezők azonosításában nagy szerepe van továbbá az érintettekkel való konzultációnak.

A lehetséges kockázatok az ICO kézikönyve alapján három csoportra oszthatók:

1. Személyeket érintő kockázatok:
   - az adatok nem megfelelő nyilvánosságra hozatala növeli annak esélyét, hogy olyan adatokat is megosztanak, amelyeket jogszerűen nem lehetne;
   - az adatkezelés célja megváltozhat, így az idő múlásával a tárolt adatokat másra használják fel az érintett tudta nélkül;
   - adatbázisok összefésülése, amelynek köszönhetően olyan felhasználói profilok hozhatók létre, amelyekből új információk nyerhetők ki.[27]
   - azonosítók összekapcsolása, amely meggátolja az anonim felhasználást.
2. Szervezeteket érintő kockázatok:
   - adatvédelmi hatóság álláspontjába vagy olyan jogszabályi előírásba való ütközés, amelynek következményeként bírság vagy más szankciók is kiszabhatók;
   - olyan problémák felmerülése, amelyekre csupán a projekt elindítását követően derül fény, és a kijavításuk rendkívül költségigényes;
   - az adatminimalizálás elvébe ütköző felesleges, készletező, esetleg többszöri adatgyűjtés, amely így csökkentheti a projekt hatékonyságát;
   - a bizonytalan és nem megfelelő adatkezelés a társadalomban bizalomvesztést eredményezhet, amely bevételcsökkenés formájában jelenhet meg.
   - adatvesztés, amely az érintettek számára kárt okoz, valamint az érintettek részéről kártérítési igényt generál.
3. *Compliance*-kockázatok:
   - az adatkezelés nem felel meg a tagállami hatóság állásfoglalásaiban foglaltaknak;
   - az ágazat-specifikus előírásoknak; vagy
   - az alkotmányjogi előírásoknak.[28]

A példálózó jellegű felsorolással kapcsolatban fontos megjegyezni, hogy az európai szabályozás – így természetesen a magyar – több veszélyforrást is kifejezetten megtilt, például a készletező adatkezelést vagy a hozzájárulás nélküli adattovábbítást.

26 Wright, David & Wadhwa, Kush & Lagazio, Monica & Raab, Charles & Charikane, Eric: Privacy impact assessment and risk management. Report for the Information Commissioner's Office, prepared by Trilateral Research & Consulting, 2013, http://ico.org.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf pp. 21-22 (utolsó letöltés: 2014. II. 20.).

27 A profilalkotás adatvédelmi aggályairól lásd bővebben: Hildebrand & Gutwirth (2010).

28 ICO-kézikönyv, 24–25. o.

Az elemzés az azonosított kockázatok értékelésével folytatódik. A magánszférára gyakorolt hatásuk mértéke alapján megkülönböztethető:

- alacsony (esély van a kockázat megjelenésére, de vannak enyhítő körülmények);
- közepes (valószínű, hogy megjelenik a kockázat, ha nem történik korrekció);
- magas (megjelenik a kockázat, ha nem történik korrekció) szintű kockázat.

Az azonosított kockázati tényezők kategorizálása után a következő lépés a kockázatokat csökkentő eljárások megfogalmazása, amelyek az implementálást követően csökkentik vagy megszüntetik az adott kockázati tényezőt. A kockázatcsökkentő javaslatok előtt a hatásvizsgálat lefolytatója jellemzően költség/haszon-elemzést is végez, amely kizárólag a szervezet szemszögéből történik, nem foglalkozik külső tényezőkkel, például az ügyfelek érdekeivel. A DPIA jelentősége éppen abban áll, hogy ezt kiegészítve több szempont és álláspontot megjelenítését teszi lehetővé, figyelembe véve így az érintettek érdekeit is (Clarke, 2011).

4.7. A jogszerűség ellenőrzése

A hatásvizsgálatot lefolytató szervezet az ajánlások megfogalmazásával párhuzamosan köteles ellenőrizni, hogy a projekt az esetleges módosítások implementálása után is megfelel a jogszabályi előírásoknak *(compliance check)*. Az ellenőrzés során figyelembe kell venni a jogi kötőerővel nem bíró állásfoglalásokat, iránymutatásokat is.[29]

4.8. Ajánlások megfogalmazása és implementálása

A kockázatelemzés eredményeként a hatásvizsgálatot elvégző szervezet ajánlásokat, javaslatokat fogalmaz meg, valamint készít egy akciótervet a szolgáltatás fejlesztője számára a módosítások implementálására. A rendelettervezet 33. cikk (3b) bekezdése alapján a záró beszámolónak tartalmaznia kell az ajánlások implementálásának menetét, illetve annak határidejét is.

Az ICO-kézikönyv szerint a szervezetnek számos lehetősége van a kritikus elemek csökkentésére, például:

- a szervezet úgy dönt, hogy nem gyűjt, illetve nem tárol meghatározott típusú adatot;
- olyan adatmegőrzési stratégia kidolgozása, amely alapján az adat csak a szükséges ideig lesz megőrizve, valamint biztonságos adatmegsemmisítési módszerek kidolgozása;
- megfelelő szintű adatbiztonsági rendszerek felállítása;[30]
- a projektben foglalkoztatottak adatvédelmi központú ismereteinek bővítése, tréningek, továbbképzések szervezése;[31]
- anonimizálási folyamatok beiktatása, ahol lehetséges és indokolt;
- munkavállalók számára útmutató készítése az új rendszerek használatával kapcsolatban;
- olyan rendszerek kidolgozása, amelyek segítik az érintetteket adataik ellenőrzésében, valamint adatigényléseik teljesítésében;
- megkülönböztetett figyelem fordítása az érintettek tájékoztatására;
- megfelelően kvalifikált adatfeldolgozó(k) alkalmazása.[32]

29 Például az Európai Bizottság 29. cikk szerinti adatvédelmi munkacsoport ajánlásai, mint például a DPIA-ról és Smart Grid/Smart Meteringről szóló 07/2013-as és 04/2013-as ajánlása, a rendelettervezetről szóló 01/2012-es véleménye.

30 E megoldás korántsem olyan egyszerű, mint annak látszik, különálló diszciplína foglalkozik a területtel. Erről bővebben lásd Szádeczky (2013).

31 A munkavállalók továbbképzése közvetve csökkenti a kockázti elemeket. A jogszabályi követelményeknek való megfelelés, a vásárlói/fogyasztói elégedettség és bizalom, egy pozitív kimenetelű átvilágítás, a szervezet jóhírnevének növelése vagy az elszámoltathatóság mind eredménye az adatvédelem központú tréningeknek, és előrevetíti az adatkezelés jogszerűségét. Az információbiztonsági és adatvédelmi központú tréning-programokról bővebben lásd Herold (2011).

32 ICO-kézikönyv, 28. o.

E példálózó felsoroláson túl természetesen számos további intézkedés is elképzelhető. A projekt fejlesztőinek minden ajánlás esetén állást kell foglalniuk arról, hogy implementálják-e az adott módosítási javaslatot vagy sem. Nem szükséges természetesen az összes javaslattal egyetérteniük, de a döntés során jelezniük kell, hogy mely módosításokat eszközölték már korábban vagy fogják a későbbiekben, illetve melyeket nem szándékozzák és miért.

Az implementálás a projekt működésébe integrált technikai és szervezeti lépésekkel történhet. Amennyiben lehetséges, célszerű valamely kérdés kapcsán több lehetséges megoldást is felkínálni a szervezet számára, hogy dönthessen, melyik a legjobb a számára. A javaslatok implementálása után ugyan maradhatnak még kockázati tényezők, ezek azonban – a költség/haszon-elemzés tükrében – az elért előnyökkel szemben nem tekintendők relevánsnak.

4.9. A beszámoló elkészítése és nyilvánossága

A hatásvizsgálat zárásaként beszámoló készül, amely többek között tartalmazza a személyes adatok védelmének elveire és hatásaira vonatkozó megállapításokat, a kezelt személyes adatok körét, azt, hogy a projekt milyen hatást gyakorol a személyes adatok védelmére, továbbá a kockázatelemzést és a kockázatcsökkentési javaslatokat (Simon, 2008).

Érdekes kérdés lehet a beszámoló nyilvánossága, illetve ezzel összefüggésben az elvégzett hatásvizsgálatok nyilvántartása. A piaci szféra és a szakértők számára is iránymutató lehetne egy központi adatbázis, amely a lefolytatott eljárások eredményét tartalmazza, könnyen hozzáférhető módon. A nyilvántartás egyfajta tudásbázisként funkcionálna jogszerű projektek létrehozására. Az elgondolás kapcsán azonban felmerül néhány kérdés; például az, hogy a regiszter működtetése kinek a feladata legyen (ideális megoldás lehet a nemzeti hatóság), vagy az, hogy a vizsgálati eredmények milyen mélységben legyenek megosztva (szükséges-e a teljes dokumentáció, vagy elég egy megfelelő szintű összefoglaló is) (De Hert et al., 2012). A hatásvizsgálat részleteinek feltárása ugyanakkor számos szereplő üzleti érdekeit sértheti, a részletes leírások üzleti titoknak minősülhetnek, így a nyilvánossággal kapcsolatos esetleges jogi szabályozás megalkotása során a kellő körültekintéssel kell eljárni.

4.10. Megfelelőségi felülvizsgálat

Az adatvédelmi hatásvizsgálatot célszerű lehet meghatározott időközönként felülvizsgálni. A rendelettervezet 33a. cikke szerint a megfelelőségi felülvizsgálatot legfeljebb két évvel a hatásvizsgálat lefolytatása után az adatkezelőnek el kell végeznie. A felülvizsgálat célja az, hogy igazolja az adatvédelmi hatásvizsgálatnak megfelelő adatkezelést. Amennyiben az adatkezelésben változás következik be, a felülvizsgálatot újra el kell végezni. A hatásvizsgálathoz hasonlóan a felülvizsgálatot is dokumentálni kell. Könnyebbség az adatkezelő számára a felülvizsgálat során, hogy az adatkezelőnek (akár saját magának, akár harmadik személynek) nem kell újra elvégeznie a teljes hatásvizsgálatot; elég a beszámolót az azóta bekövetkezett esetleges változásokkal összevetnie. Rendszertanilag vizsgálva a megfelelőségi felülvizsgálat lényegében egy belső auditnak is tekintehető.

5. Összegzés

Az adatvédelmi hatásvizsgálat egyes elemei nem teljesen ismeretlenek az európai adatvédelmi szabályozásban: elég kiemelni az adatvédelmi irányelv 20. cikkét, amely meghatározza az előzetes ellenőrzés követelményét, vagy a jogszerűség és transzparencia egyik garanciális elemeként aposztrofált, a 21. cikkben szabályozott nyilvánosság biztosítását. A PIA és a magyar szabályozás között is azonosíthatók hasonló elemek, ezeket Simon Éva tárgyalja részletesen tanulmányában (Simon, 2008).

E tanulmányban bemutattuk az adatvédelmi hatásvizsgálat főbb elemeit, az eljárás lefolytatásának menetét. A tanulmányban ismertetett menetrend elsősorban a több, mint egy évtizedes gyakorlattal rendelkező amerikai,

kanadai és ausztrál hatásvizsgálatok elemeit tartalmazza, utalva a várható uniós adatvédelmi rendelettervezet előírásaira. Egy sikeres adatvédelmi hatásvizsgálathoz azonban nem feltétlenül van szükség az összes részelem alkalmazására, azok szűkebb körű felhasználása esetén is elérhető a hatásvizsgálat célja. A létező angolszász minták és joggyakorlat – az adatvédelmi szabályozás különbözőségeinek ellenére – az európai rezsimben is hasznosíthatóak. Az adatvédelmi hatásvizsgálat ugyanis (jelen állás szerint) hamarosan az európai adatvédelmi jog részévé is válhat. A Rendelettervezet kifejezetten rendelkezik az adatvédelmi hatásvizsgálatról, amelynek tartalma szerint azonban „a tervezett adatfeldolgozási műveleteknek az érintettek jogai és szabadságai, különösen a személyes adatok védelméhez való joguk tekintetében várható hatásának vizsgálatát" jelenti. Ez furcsa módon még a privacy-hatásvizsgálatnál is szélesebb vizsgálódási kört ölel fel, és ebben a formában kissé parttalan. A jogintézmény gyakorlatba való átültetése számos olyan elvi és gyakorlati kérdést vet fel, amelynek megválaszolása az Európai Unió és a tagállamok jogalkalmazó szerveinek (különösen az adatvédelmi hatóságoknak) a feladata lesz.

Melléklet: Kérdőív az adatvédelmi hatásvizsgálathoz

A kérdéssor összeállításához az ausztrál,[33] valamint az amerikai igazságügyi minisztérium PIA minta-kérdéssora[34] szolgált alapul. A Rendelettervezet által különösen fontosnak tartott elemeket érintő kérdéseket dőlt betűvel jelöltük. Az esetleges gyakorlati tapasztalatok során derülhet ki, hogy a magyar jogi környezetben a kérdéssor mennyiben releváns, milyen mértékben szükséges a kérdések hazai jogszabályhoz történő további igazítása.

A kérdőív első részében szereplő kérdésekre elegendő igennel vagy nemmel válaszolni. A kérdőív második részét csak abban az esetben kell kitölteni, ha szükséges a vizsgálat lefolytatása: amennyiben az 5–11. kérdések közül bármelyikre „igen" a válasz, a hatásvizsgálat lefolytatása kötelező. A második részben az egyes kérdések részletes kifejtése szükséges. A harmadik részt csak abban az esetben kell kitölteni, amennyiben arra a hatásvizsgálatot lefolytató szerv szerint szükség van.

Első rész: Szükséges-e a hatásvizsgálat lefolytatása?

1. Használ vagy fejleszt-e olyan informatikai rendszert, amely személyes adatokat kezel?
   Igen ❑ Nem ❑

2. Szükséges-e személyes adatokat gyűjteni a szolgáltatás működtetéséhez?
   Igen ❑ Nem ❑

3. Megvalósul-e a korábbiaktól eltérő célú adatkezelés már meglévő személyes adatokkal kapcsolatban?
   Igen ❑ Nem ❑

   a) Alkalmaz új adatköröket gyűjtő technológiát, amely jelentős mértékben megváltoztatja az adatkezelést?
   Igen ❑ Nem ❑

   b) Amennyiben releváns szervezeti változás következik be:
   • az egyesülés, beolvadás vagy egyéb szervezeti átalakulás hatással van-e az adatbázisokra?
   Igen ❑ Nem ❑

   • ez a változás eredményezi új adatok kezelését vagy új nyilvánosságra hozatali eljárásokat?
   Igen ❑ Nem ❑

33 PIAF D3 p. 25.

34 Department of Justice: Privacy Impact Assessment (PIA) Template, http://www.justice.gov/sites/default/files/jmd/legacy/2014/04/08/preliminary_pia.pdf (utolsó letöltés: 2014. V. 5.).

c) Amennyiben ez az információ már korábban be lett gyűjtve:

• érint-e új vagy nagy létszámú érintetti csoportot?

Igen ❑ Nem ❑

• rögzít-e ezen felül további személyes adatot?

Igen ❑ Nem ❑

4. A szolgáltatás korlátozza-e az érintettek személyes adataikhoz való hozzáféréséhez fűződő jogait?
   Igen ❑ Nem ❑

5. Tervezi-e egymást követő 12 hónapból álló időszak során 5000-nél több érintett személyes adatainak kezelését?[35]
   Igen ❑ Nem ❑
6. Megvalósul-e különleges adatok, tartózkodási helyre utaló adatok, illetve gyermekekre vagy munkavállalókra vonatkozó, széleskörű nyilvántartási rendszerekben tárolt adatok kezelése?[36]
   Igen ❑ Nem ❑

7. Megvalósul-e profilalkotás, amelyre az érintett személy tekintetében joghatással bíró vagy az egyént hasonlóan jelentős mértékben érintő intézkedések épülnek?[37]
   Igen ❑ Nem ❑

8. Megvalósul-e egészségügyi ellátás nyújtására, járványügyi kutatásokra, mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatok kezelése, amennyiben az adatok feldolgozására meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor?[38]
   Igen ❑ Nem ❑

9. Megvalósul-e nyilvánosság számára hozzáférhető területek (közterületek) nagyarányú, automatizált nyomon követése?[39]
   Igen ❑ Nem ❑

10. Megvalósul-e olyan adatkezelés, amely során a személyes adatok megsértése várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét?[40]
    Igen ❑ Nem ❑

11. Az adatkezelő vagy adatfeldolgozó fő tevékenységei olyan eljárásokat foglalnak-e magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerű megfigyelését igénylik?[41]
    Igen ❑ Nem ❑

12. A személyes adatokat olyan jelentős számú személy számára teszi-e hozzáférhetővé, amely ésszerűen elvárható módon nem korlátozható?[42]
    Igen ❑ Nem ❑

35 Rendelettervezet 32a. cikk (2) a) pont.

36 Rendelettervezet 32a. cikk (2) b) pont. A kérdésben különleges adatnak tekintendők a 9. cikk (1) bekezdésben meghatározott különleges adatkategóriák.

37 Rendelettervezet 32a. cikk (2) c) pont.

38 Rendelettervezet 32a. cikk (2) d) pont.

39 Rendelettervezet 32a. cikk (2) e) pont.

40 Rendelettervezet 32a. cikk (2) g) pont.

41 Rendelettervezet 32a. cikk (2) h) pont.

42 Rendelettervezet 32a. cikk (2) i) pont.

13. Létrejön-e új azonosító vagy hozzáférési jogosultságot ellenőrző rendszer, például biometrikus azonosítás?
    Igen ❑ Nem ❑

14. Megfigyelés alatt állnak-e az érintettek helyváltoztatás, másokkal való kommunikáció vagy egyéb magatartás tanúsítása közben?
    Igen ❑ Nem ❑

15. Megvalósul-e automatizált adatfeldolgozás?
    Igen ❑ Nem ❑

16. Személyes adatok védelmének növelése érdekében előír-e (ha volt ilyen) a korábbinál magasabb szintű adatbiztonsági követelményeket?
    Igen ❑ Nem ❑

17. Személyes adatokkal való visszaélés megelőzése érdekében bevezetésre kerülnek-e új vagy módosított előírások?
    Igen ❑ Nem ❑

18. Személyes adatok tárolásával kapcsolatban bevezetésre kerülnek-e új vagy módosított előírások?
    Igen ❑ Nem ❑

19. Megvalósul-e tudományos kutatási vagy statisztikai célból történő adatkezelés?
    Igen ❑ Nem ❑

20. Az adatkezelés kiterjed-e különleges adatokra?
    Igen ❑ Nem ❑

21. Megvalósul-e bármilyen más, magánszférát érintő magatartás?
    Igen ❑ Nem ❑

22. Végeztek-e már korábban hatásvizsgálatot? Amennyiben a válasz igen, csatolja a dokumentumot!
    Igen ❑ Nem ❑

Második rész: Előzetes hatásvizsgálat

1. Ki a tájékoztatásra kötelezett személy (név, telefonszám, emailcím)? (Ha van belső adatvédelmi felelős, akkor az ő adatai).
2. Mutassa be a szolgáltatás működését, felépítését!
3. Ki az adatkezelő (név, telefonszám, emailcím, postai cím)?
4. Mi az adatkezelés pontos címe/helye/webhelye? (Csak akkor töltse ki, ha az eltér az adatkezelő címétől!)
5. Mi az adatkezelés célja, módja és jogalapja?
6. Mi az adatkezelés időtartama?
7. Kíván-e adatfeldolgozót igénybe venni? Ha igen, mutassa be részletesen az adatfeldolgozó személyét (kapcsolattartó, adatkezeléssel összefüggő tevékenység, adatfeldolgozó címe, adatfeldolgozás helye, technológiája stb.)!
8. Melyek a kezelni kívánt adatkörök?
9. Határozza meg a gyűjteni kívánt adatok mennyiségét, illetve az érintett személyek számát (hozzávetőlegesen)!
10. Melyek az adatfelvétel formái? Megvalósulhat az adatgyűjtés személy azonosítására alkalmas igazolvány segítségével is? Ha igen, fejtse ki!

11. Az adatszolgáltatás önkéntes? Ha igen, az érintettek megfelelő mértékben tájékoztatva vannak-e a kezelt adatok köréről, illetve jogaikról?
12. Az érintetteknek van-e lehetőségük arra, hogy adataik kizárólag meghatározott célokra történő felhasználásához nyújtsanak hozzájárulást? Ha igen, hogyan?
13. Megvalósul-e harmadik országba irányuló adattovábbítás? Ha igen, írja le a továbbítandó adatok fajtáit, a továbbítás címzettjének adatait, valamint az adattovábbítás jogalapját!
14. Fejtse ki, milyen lépéseket tesz az adatok biztonságának megőrzése érdekében!
15. Amennyiben megfelelő szintűnek vélt az adatok biztonsága, milyen eszközök óvják az azonosítatlan hozzáféréstől?
16. A megfelelő védelmi eszközöket használja azonosítatlan hozzáférés megakadályozása érdekében? Fejtse ki álláspontját!
17. Van egyéb közlendő információja?

Harmadik rész: További analízis

18. Hogyan biztosítja az érintettek jogainak érvényesítését?
19. Fejtse ki azokat az Ön által is ismert, alternatív megoldásokat, amelyek az eredeti eljáráshoz képest a cél elérése mellett kisebb mértékben érintenék a magánszférát!
20. Milyen módszerekkel kívánja csökkenteni az azonosított kockázati tényezőket?
21. Hogyan ellenőrzi az adatok teljességét?
22. Megfelelően naprakészek-e a gyűjtött adatok? Amennyiben igen, támassza alá válaszát!
23. Kifejtett és részletezett az adatok természete?
24. Kinek van hozzáférési joga (lehetősége) a személyes adatokhoz?
25. Mi alapján kerülnek kiválasztásra azok a személyek, akik rendelkeznek ezzel a joggal?
26. A személyes adatokhoz való hozzáférés feltételei, módja, korlátai rögzítve vannak?
27. Milyen eszközök biztosítják az adatkezelés céljától eltérő felhasználás megakadályozását?
28. Hozzáférhet-e más rendszer a saját rendszerben kezelt adatokhoz? Ha igen, fejtse ki!
29. Az adatkezelés idejének lejárta után milyen módon kerülnek törlésre az adatok? Hogyan lesz dokumentálva az adattörlés?

Irodalom

Online források

A 29. cikk szerinti adatvédelmi munkacsoport 5/2010. számú véleménye a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló ágazati javaslatról, WP 175, 2010. július 13., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_hu.pdf (utolsó letöltés: 2013. VI. 15.).

Adatvédelmi és Privacy Biztosok Nemzetközi Konferenciája, Madrid, 2009, Privacy: Today is Tomorrow – International Standards on the Protection of Personal Data and Privacy, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf (utolsó letöltés: 2014. IX. 9.).

Állampolgári Jogi, Bel- és Igazságügyi Bizottság jelentése a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló európai parlamenti és tanácsi rendeletre (általános adatvédelmi rendelet) irányuló javaslatról (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 2013, http://www.tisztessegesadatkezeles.hu/letoltes/tkMQJ7RbxxzG0E2B1tz0rOu2UZX (utolsó letöltés: 2014. VII. 10.).

Clarke, Roger: An evaluation of privacy impact assessment guidance documents, In: *International Data Privacy Law*, 2011, vol. 1, http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.full.pdf (utolsó letöltés: 2014. IX. 10.).

Clarke, Roger: Privacy Impact Assessment Guidelines, 1998, http://www.xamax.com.au/DV/PIA.html (utolsó letöltés: 2014. III. 16.).

De Hert, Paul & Kloza, Dariusz, Wright, David: Recommendations for a Privacy Impact Assessment Framework for the European Union, Privacy Impact Assessment Framework Deliverable D3, 2012, http://www.piafproject.eu/ref/PIAF_D3_final.pdf (utolsó letöltés: 2014. VIII. 3.).

Department of Justice: Privacy Impact Assessment (PIA) Template, http://www.justice.gov/sites/default/files/jmd/legacy/2014/04/08/preliminary_pia.pdf (utolsó letöltés: 2014. V. 5.).

Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, a Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A személyes adatok Európai Unión belüli védelmének átfogó megközelítése COM(2010) 609 végleges, Brüsszel, 2010.11.04., http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_hu.pdf (utolsó letöltés: 2014. III. 10.).

Európai Bizottság: Javaslat – Az Európai Parlament és a Tanács Rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet), Brüsszel, 2012. I. 25. COM(2012) 11 végleges, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:HU:PDF (utolsó letöltés: 2013. X. 10.).

Hosein, Gus & Davies, Simon: Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the European Union, A Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D2, 2012, http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf (utolsó letöltés: 2014. IX. 8.).

Information Commissioner's Office (ICO): Conducting privacy impact assessments code of practice, 2014, http://ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf (utolsó letöltés: 2014. VIII. 8.).

PIAF Empirical research of contextual factors, http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf, 2014 (utolsó letöltés: 2014. VI. 6.).

Wright, David & Wadhwa, Kush & De Hert, Paul & Kloza, Dariusz: A Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1 – Revision of existing PIAs, 2011, http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf (utolsó letöltés: 2013. XI. 11.).

Wright, David & Wadhwa, Kush & Lagazio, Monica & Raab, Charles & Charikane, Eric: Privacy impact assessment and risk management. Report for the Information Commissioner's Office, prepared by Trilateral Research & Consulting, 2013., http://ico.org.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf (utolsó letöltés: 2014. II. 20.).

Offline források

Böröcz István (2014): A Privacy Impact Assessment forrásai. In: *Infokommunikáció és jog*, 3. sz. (megjelenés alatt).

Herold, Rebecca (2011): *Managing an Information Security and Privacy Awareness and Training Program.* CRC Press.

Hildebrand, Mireille & Gutwirth, Serge, eds. (2010): *Profiling the European Citizen*. Springer.

Jóri András (2005): *Adatvédelmi kézikönyv*. Budapest: Osiris Kiadó.

Polyák Gábor & Szőke Gergely László (2011): Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései. In: Drinóczi Tímea (szerk.): *Magyarország új alkotmányossága*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 155–177. o.

Schütz, Philip (2012): The Set Up of Data Protection Authorities as a New Regulatory Approach. In: Gutwirth, Serge & Leenes, Ronald & De Hert, Paul & Poullet, Yves (eds.): *European Data Protection: In Good Health?* Springer, pp. 125–142.

Simon Éva (2008): Az adatvédelmi hatásvizsgálat bevezetésének lehetősége Magyarországon. In: Székely Iván & Szabó Máté Dániel (szerk.): *Szabad adatok, védett adatok 2*. Információs Társadalomért Alapítvány, 199–213. o.

Sólyom László (1983): *A személyiségi jogok elmélete.* Budapest: Közgazdasági és Jogi Könyvkiadó (http://www.oecd.org/sti/ieconomy/15590228.pdf (utolsó letöltés: 2014. II. 15.).

Szádeczky Tamás (2013): Az IT biztonság szabályozásának konfliktusa. In: *Infokommunikáció és jog,* 56. szám, 149–153. o.

Szőke Gergely László (2013): Az adatvédelem szabályozásának történeti áttekintése. In *Infokommunikáció és jog*, 56. szám, 107–112. o.

Wright, David & De Hert, Paul (2012): *Privacy Impact Assessment*. Springer.

Balogh Zsolt György a Budapesti Corvinus Egyetem Gazdálkodástudományi Karának tudományos főmunkatársa. Kutatási területe az elektronikus kereskedelmi szolgáltatások szabályozása, valamint az online szerencsejáték.

Böröcz István a Pécsi Tudományegyetem Állam- és Jogtudományi Karának PhD-hallgatója. Kutatási területe a Big Data-jelenség, valamint a profilalkotás adatvédelmi jogi vonatkozásai.

Kiss Attila a Nemzeti Közszolgálati Egyetem tanársegédje. Kutatási területe a közterületi térfigyelő rendszerek szabályozásának kérdései, valamint a képmáshoz fűződő jogok védelme.

Polyák Gábor a Pécsi Tudományegyetem Állam- és Jogtudományi Karának docense. Kutatási területe a médiaszabályozás műszaki, gazdasági és társadalomtudományi összefüggései és piacszabályozási vonatkozásai.

Szőke Gergely László a Pécsi Tudományegyetem Állam- és Jogtudományi Karának tudományos segédmunkatársa, a Pécsi Tudományegyetem belső adatvédelmi felelőse. Kutatási területe az adatvédelmi jog, a szerzői jog, az elektronikus kereskedelem joga.