Boros Anita
ELTE ÁJK Polgári Jogi Tanszék
Témavezető: Balogh Zsolt György egyetemi docens, Budapesti Corvinus Egyetem, Gazdálkodástudományi Kar, Infokommunikációs Tanszék

Adatvédelmi megfelelés: privacy by design és a hatásvizsgálat mint az elszámoltathatóság eszközei

1. Bevezetés

Az új technológiai kihívások egyre tömegesebbé, gyorsabbá teszik az adatkezeléseket, ezzel párhuzamosan pedig az állampolgárok egyre nehezebben tudják ellenőrizni, nyomon követni adataik sorsát. Az európai adatvédelmi rendelet szabályai egyértelműen a kockázat alapú megközelítést hivatottak kikényszeríteni, melynek következtében az adatkezelőknek és adatfeldolgozóknak biztosítaniuk kell a személyes adatok megfelelő védelmét. A rendeletnek való megfelelés komoly kihívásnak minősülhet, hiszen a már meglévő adatkezelési szabályoknak való megfelelés mellett olyan új kötelezettségeket vezet be az adatkezelők és adatfeldolgozók számára, melyek idő- és pénzigényes folyamatok kialakítását követelik. Különösen a nagy mennyiségű személyes adatot kezelő vállalatoknak jelent ez komoly felelősséget, hiszen a megfelelés nem csak jogi kérdés, átfogóan érinti a folyamatmenedzsmentet, a kontrollkörnyezet és az üzleti folyamatokat is.

Az adatvédelmi rendelet egyik központi eleme, az elszámoltathatóság alapelve, ami nem számít újdonságnak e területen. Hiszen az adatkezelés jogszerűségéért eddig is az adatkezelő felelt, de a bizonyítás terhe csak reaktív módon, bírósági eljárás során terhelte. A jelenlegi szabályozás alapján az elszámoltathatóság magában foglalja az adatkezelő legfontosabb feladatát, akinek nem csak felelősséget kell vállalnia a rendeletben

megfogalmazott alapelvek és kötelezettségek betartásáért, de képesnek kell lennie bizonyítani is a megfelelését.

Az elszámoltathatóság elve a hatékony adatvédelem sarokkövévé és az EU adatvédelmi törvény, politika és szervezeti gyakorlat domináns trendjévé vált. Ezen alapelv betartása nélkül nem beszélhetünk adatvédelmi megfelelésről, melynek alapján egy testreszabott adatvédelmi keretrendszert szükséges kidolgozni és folyamatosan működtetni. Az adatvédelmi alapelveket mind az informatika és az üzleti folyamatok, mind a fizikai tervezés és hálózati infrastruktúra szintjén egyaránt figyelembe kell venni.

Nem kérdés tehát, hogy a beépített adatvédelem az alapvető adatvédelem elengedhetetlen alkotóeleme.[1] Ennek lényege, hogy az adatvédelmi elveket és az érintettek jogainak védelméhez szükséges garanciát már az adatkezelési eljárások kidolgozásakor és megtervezésekor figyelembe kell venni, biztosítván ezáltal az adatok maximális védelmét. A *privacy by design* olyan adatvédelmi irányzat, mely szerint az adatvédelmi szempontoknak megfelelő gyakorlat nem merülhet ki a hatályos szabályozásnak való formális megfelelésben. Az adott vállalat vagy szervezet alapvető működési struktúráját ezek maximális figyelembevételével kell kialakítania, az adatvédelmi szempontokat már az egyes működési fázisok megtervezésekor be kell építeni, így biztosítván az adatvédelem teljes körű érvényesülését.[2] Ennek egyik gyakorlati megvalósítási eszköze az adatvédelmi hatásvizsgálat. Ez adatvédelmi jogi, adatbiztonsági, és információbiztonsági kockázatelemzés, mely fontos a megfelelő technikai és szervezeti intézkedéseket kiválasztása szempontjából. Bár látszólag úgy tűnhet, hogy az előzetes hatásvizsgálat elvégzése a *privacy by design* megvalósításának első lépése, ennek ellenére a GDPR rendelkezései alapján ennek elvégzése csak bizonyos feltételek teljesülése esetén kötelező.

Az elszámoltathatóság alapelvének való megfelelés olyan adatvédelmi rendszer kialakítása iránti elkötelezettségen alapul, ahol az adatvédelem beépül az összes üzleti folyamatba. Így kijelenthető, hogy az elszámoltathatóság egyik legfontosabb eleme a beépített adatvédelemnek való megfelelés.

A tanulmány e két, az adatvédelmi megfelelés szempontjából lényeges kötelezettség közötti kapcsolatot és kölcsönhatást hivatott feltárni, amelynek

[1] Állásfoglalás a beépített adatvédelemről 2010.

[2] Nemzeti Adatvédelmi és Információszabadság Hatóság, Adatvédelmi értelmező szótár, www.naih.hu/adatvedelmi-szotar.html (letöltve: 2020.02.18.)

tisztázása kiemelkedő fontossággal bír az adatvédelmi vállalati megfelelés során. Összehasonlító, illetve leíró-kritikai elemzéssel vizsgálni fogom mindkét kötelezettség elemeit, majd kitérek a kockázatalapú megközelítés másik fontos eszközére, az adatvédelmi hatásvizsgálatra, ami szintén szoros viszonyban van e két kötelezettséggel.

2. Az elszámoltathatóság elve

A sikeres adatvédelmi megfelelés megszervezése összetett vállalkozás. Az adatkezelőnek folyamatosan lépést kell tartania az értelmezési és a törvényi változásokkal, figyelnie kell mind a külső, mind a belső tényezők lehetséges veszélyeit, biztosítania kell a meglévő vagy a megfelelés során kialakult szervezeti gyakorlatok betartását, reagálnia kell az érdekelt felek kérdéseire, és mindenek felett olyan vezetői készséggel kell rendelkeznie, mely biztosítja a szervezeten belüli kellő hozzáállást. Az adatvédelmi hatóság, az ügyfelek, az alkalmazottak vagy akár üzleti partnerek egyaránt felelősségre vonhatják a szervezetet az adatvédelmi szabályok be nem tartása miatt, így egyre több vállalat kifejezett figyelmet fordít e területre.[3]

Az elszámoltathatóság fogalma

Míg az etika és a kormányzás terén az elszámoltathatóság fogalma a felelősségvállalásban és a számadási kötelezettségben merül ki, a szervezeti vezetői szerepekben az elszámoltathatóság az intézkedések, a döntések és a politikák iránti felelősség vállalása.[4] Az adatvédelem világán kívül is létezik néhány példa az elszámoltathatóság elvére. Ezek olyan megfelelési rendszerek, amelyek konkrétan meghatározzák az adatkezelőnek a jogszabályi előírások érvényesülését szolgáló politikáit és eljárásait. Ilyenek például a pénzügyi szolgáltatásokról szóló jogszabályok. Más esetekben csak ajánlott, de nem kötelező rendelkezni megfelelési programmal, mint például a versenyjog terén.[5]

[3] A 29. szerinti adatvédelmi munkacsoport 3/2010 vélemény az elszámoltathatóság elvéről, 2.
[4] Williams 2006.
[5] A 29. szerinti adatvédelmi munkacsoport 3/2010 vélemény az elszámoltathatóság elvéről, 7.

Az adatvédelmi megfelelés területén az „elszámoltathatóság” (*accountability*) mint fogalom, mely az angolszász világból származik, magában foglalja egyrészt, hogyan érvényesül az adatkezeléssel kapcsolatban az adatkezelő felelőssége, másrészt pedig, hogy ez hogyan bizonyítható. A felelősség és az elszámoltathatóság egyazon érme két oldala. Ez nem jelent mást, minthogy az adatkezelőnek az adatkezelés megtervezésétől az adatkezelés megvalósításán keresztül egészen az adatok törléséig vagy az adatkezelés megszűnéséig ügyelnie kell arra, hogy bármikor bizonyítani tudja, eleget tesz a hatályos rendelkezéseknek. Az elszámoltathatósági elv célja, hogy megerősítse és növelje az adatkezelők felelősségét a személyes adatok kezelése során. Ezért valamennyi, a rendeletben megfogalmazott kötelezettség teljesítését az elszámoltathatóság szemszögéből kell megközelíteni.[6]

Az elv bevezetését az európai adatvédelmi szabályozásba a 29. cikk szerinti adatvédelmi munkacsoport is szorgalmazta. A 3/2010 számú véleménye alapján *„az általános adatvédelmi elveket konkrét, az adatkezelő szintjén meghatározott politikákra és eljárásokra fordítaná le.”* Ezáltal az adatvédelem sokkal gyakorlatiasabban és hatékonyabban tud működni. Ugyancsak e vélemény hangsúlyozza azt is, hogy az elszámoltathatóságra vonatkozó új rendelkezés *„nem irányul arra, hogy az adatkezelőket újabb elveknek vesse alá, hanem a már létezőknek történő valós, hatékony megfelelést biztosítja.”*

Szabó Endre Győző, a Nemzeti Adatvédemi és Információszabadság Hatóság (NAIH) elnökhelyettesének megfogalmazása szerint: *„Az elszámoltathatóság elvének lényege kettős: egyrészt azt várja el az adatkezelőtől, hogy kialakítsa azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek a rendeletből fakadó kötelezettségek teljesítéséhez szükségesek, másrészt a megfelelés bemutatásának képességét várja el.”*[7]

Az elszámoltathatóság elemei

Az elszámoltathatóság elvének való megfelelés átfogó megközelítést igényel, amely egy sor kulcsfontosságú elemet magában foglal.

[6] Árvai 2018. 5-7.
[7] Szabó 2016. 4.

A megfelelés részeként az adatkezelőnek folyamatosan figyelemmel kell kísérni a vállalati tevékenységeket, hogy azok érintenek-e személyes adatokat. Ha igen, akkor megfelelő intézkedéseket kell arra rendszeresítenie, hogy az adatvédelmi megfelelést ellenőrizze és naprakészen tartsa, és nem utolsó sorban mindezeket dokumentálnia szükséges. A GDPR[8] 5. cikk (2) bekezdése értelmében tehát az elszámoltathatóság legfontosabb eleme, hogy az adatkezelő és adatfeldolgozó felelősséget vállaljon az általa végzett adatkezelésért.

A rendelet 24. cikke tovább részletezi az elszámoltathatóság kötelezettségét az adatkezelő feladatainál. Ennek megfelelően az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakészszé teszi. Ha az adatkezelési tevékenységgel arányban áll, ennek részeként az adatkezelő belső adatvédelmi szabályokat is alkalmaz.[9]

Ez azt jelenti, hogy az adatkezelő intézkedéseit a szervezete konkrét sajátosságaihoz és a kérdéses adatkezelési műveletekhez kell igazítani. Az elszámoltathatóság elve alapján megkövetelt technikai és szervezeti intézkedéseknek a 24. cikkben meghatározott két tényezőre, nevezetesen az adatfeldolgozás jellegére, valamint a kockázat valószínűségére és súlyosságára tekintettel kell megfelelőnek lenniük. Ilyen kockázatok a GDPR 75. preambulum bekezdése alapján származhatnak:

1. olyan személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélküli feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat;

[8] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (továbbiakban: GDPR)

[9] Árvai 2018. 7.

2. az olyan adatkezelésekből, amelyek következtében az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett;
3. olyan személyes adatok kezeléséből, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre, vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, a büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak;
4. az olyan adatkezelésekből melyek során személyes jellemzők értékelésére – így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére – kerül sor személyes profil létrehozása vagy felhasználása céljából;
5. ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy
6. ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

A kockázat valószínűségét és súlyosságát minden esetben az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni. A kockázatot felmérése mindig objektív értékelés alapján történik, amelynek során szükséges megállapítani, hogy az adatkezelési műveletek kockázattal, illetve nagy kockázattal járnak-e.[10]

A „megfelelő” szó az elszámoltathatóság skálázhatóságára utal, ami lehetővé teszi az adatkezelő számára, hogy – figyelembe véve többek között a szervezet típusát, legyen az nagy vagy kicsi, valamint a személyes adatok típusát, jellegét és összességét – ő maga döntse el, hogy éppen milyen intézkedések alkalmazása szükség.[11]

A szervezeti intézkedések közé tartozik egyrészt az adatvédelmi megfelelést igazoló dokumentáció fenntartása. A rendelet számos ilyen dokumentáció fenntartásáról tesz említést, ilyen például adatkezelési műveletek nyilvántartása, az adatvédelmi incidensek nyilvántartása vagy az adatvédelmi hatásvizsgálat dokumentálása. Dokumentáció szempontjából

[10] GDPR (76) preambulumbekezdés
[11] Kuner 2020. 562.

szintén fontos az adatkezelési tájékoztatók elkészítése, a belső adatkezelési szabályzatok, az adatfeldolgozói szerződésnek az adatvédelmi kitételei vagy mellékletei, és mint az adattovábbításokkal kapcsolatos adatvédelmi garanciák, a szerződéses kikötések beiktatása is. Ugyancsak a dokumentálási követelményekhez tartozik érdekmérlegelési tesztek eredményeinek rögzítése, a megfelelő belső szabályzatok elkészítése, amelyek a fent említetteken túl szólhatnak a megőrzési szabályokról vagy az informatikai biztonságról. Ugyancsak dokumentálandók az adatkezelőhöz érkezett érintetti megkeresések, az arra adott válaszok, a munkahelyi eszközök használata, a személyzet megfigyelésének szabályozása és az adatkezelő belső adatvédelmi tréningjei.[12]

A dokumentáció elkészítése mellett szervezeti intézkedések végrehajtása is szükséges. Ilyen például: az adatvédelmi projekt vezetése és felügyelete; adatvédelmi tisztviselő kinevezése; kockázatfelmérés (beleértve a hatásvizsgálatot); adatfeldolgozók gondos kiválasztása; átláthatóság biztosítása; képzés és tudatosság növelése a szervezeten belül; ellenőrzés; válaszadás, panaszkezelés és végrehajtás. Ezek olyan intézkedések, amelyeket vagy a törvény, vagy egy adott tanúsítvány, vagy magatartási kódex szabályai írhatnak elő, vagy a szervezet hatékonyabb működése céljából szükségesek. De mindegyik esetben átfogó adatvédelmi vállalatirányítási rendszert képeznek, amely nem csak a legalapvetőbb szinten biztosítja a vonatkozó szabályok betartását, de széles körű további előnyökkel is járhat a szervezet és más érdekelt felek számára is, különösen akkor, ha az elszámoltathatósági intézkedések túllépnek a törvényben előírt minimális kereteken.[13]

Az elszámoltathatóság előnyei

Az első és legfontosabb előny az elszámoltathatóság elismerése az adatvédelmi bírságok kiszabása esetén. Alapvetően a rendelet nem tesz különbséget multinacionális vállalatok, KKV-k, intézmények vagy szervezetek, sőt magánszemélyek között, így az egyéni vállalkozókat is ugyanazok a kötelezettségek terhelik, mint a nagyobb adatkezelőket. Sőt mi több, a felügyeleti hatóságok különböző szankciókat alkalmazhatnak a

[12] Kuner 2020. 563.
[13] Heyder-Grogan 2018.

jogszabály rendelkezéseinek nem megfelelő betartásával szemben, és bírságot is kiszabhatnak rájuk. Ennek mértéke szintén nem az adatkezelő vagy adatfeldolgozó méreteitől vagy az adatkezelés mértékétől függ. A 29. cikk alapján létrehozott adatvédelmi munkacsoport 2017. október 3-án iránymutatást adott ki a bírság alkalmazásáról[14]. Ez a felügyeleti hatóságok számára ad iránymutatást a bírság kiszabásával kapcsolatban. A felügyeleti hatóságnak egyenként kell azonosítania és értékelnie a jogsértéseket, és a leginkább megfelelő korrekciós intézkedést (szankciót) kell alkalmaznia, figyelembe véve – többek között – az adatkezelő vagy az adatfeldolgozó felelősségének mértékét, tekintettel az általa foganatosított technikai és szervezési intézkedésekre.[15] E véleményből kitűnik, hogy az elszámoltathatóság elvének való megfelelés enyhítő körülménynek tekinthető egy esetleges bírság kiszabása esetén.

További előnyt jelenthet multinacionális cégeknél az elszámoltathatóság magas szintjének biztosítása, mely lehetővé teszi továbbá a vállalaton belüli globális harmonizáció előmozdítását és az interoperabilitás és a globális adatáramlás megkönnyítését is.

Nem elhanyagolható következmény az sem, hogy a megfelelő adatvédelmi vállalatirányítási rendszer kialakítása hasznos eszközként szolgál az adatvédelmi szempontból biztonságos adatfeldolgozók kiválasztásakor.

Nem utolsó sorban az elszámoltathatóság végrehajtása nemcsak a vállalatok, hanem az érintett magánszemélyek javát is szolgálja, hiszen biztonságossá és ellenőrizhetővé válik a személyes adataik kezelése, így az adatkezelőkkel és adatfeldolgozókkal szemben megnő a vevői, fogyasztói bizalom, ugyanis ezen intézkedések betartása garantálja, hogy a vállalkozás nem él vissza a személyes adataikkal.[16]

Láthatjuk tehát, hogy az elszámoltathatóság elvének való magas szintű megfelelés számos előnnyel járhat bármely vállalkozás számára, de ennek költségei egyáltalán nem elhanyagolható mértékűek. Így nem meglepő, hogy a kis- és középvállalkozások többsége a törvényben meghatározott minimális követelményeknek igyekszik eleget tenni.

A fenti elemzés alapján az elszámoltathatóság elvének tehát három fő eleme van:

[14] A 29. szerinti adatvédelmi munkacsoport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához

[15] Heyder - Grogan 2018.

[16] Center for Information Policy Leadership 2018.

1. megfelelő dokumentáció elkészítése, annak folyamatos felülvizsgálata (a szabályzatok elszámoltathatósága);
2. adatvédelmi irányítási keretrendszer kialakítása (az eljárások elszámoltathatósága); és
3. e kettő gyakorlatba ültetésének bizonyítása (a gyakorlati elszámoltathatóság).

A beépített adatvédelem az adatvédelmi irányítási rendszerek fejlesztésében válik kritikusan fontossá. A rendelet szellemiségét tekintve kiemelkedően fontos, hogy a megfelelési folyamat nem merül ki formális dokumentum alapú megfelelésben. A technikai és szervezeti intézkedések meghozatala önmagában nem juttatja érvényre az elszámoltathatóság elvét . A reputációs veszteség és a megfelelési kockázatok minimalizálása érdekében a vállalatnak már a folyamatok megtervezése előtt figyelembe kell vennie az adatvédelmi elveket.

3. A privacy by design elve

A *privacy by design* fogalmát elsőként Ann Cavoukian, a kanadai Ontario állam adatvédelmi biztosa határozta meg a 90-es években. Eszerint az adatvédelmi szabályozás elveit be kell építeni az adatkezelési technológiákba mind a tervezés, mind a működtetés során. Ez az elv kezdetlegesen az infokommunikációs technológia kapcsán jelent meg, majd kiterjedt az üzleti folyamatokra is. [17] Az általa megfogalmazott filozófiára jellemző hét alapelv[18] fontos kiindulópont e fogalom megértéséhez és gyakorlatba ültetéséhez. Ezek a következők:

1. Reakció helyett proaktivitás, utólagos orvoslás helyett megelőzés. A káros hatások orvoslása helyett a jogsértés bekövetkezését kell megakadályozni.

2. Alapértelmezett adatvédelem, mely a maximális védelmet az egyén számára különös lépés megtétele nélkül, automatikusan garantálja.

3. A harmadik alapelvhez szorosan kötődik a másodikhoz, miszerint az alapértelmezett adatvédelmet már a tervezési folyamat során

[17] Balogh 2014. 39.
[18] Cavoukian 2013.

figyelembe kell venni, és részévé kell tenni bármilyen eszköz/szolgáltatás fejlesztési folyamatának.

4. Teljes működőképesség, vagyis olyan megoldások kivitelezése, amelyek integrálják az összes érintett jogos érdeket és célt, majd ez pozitív végeredményt vált ki.

5. Teljes életciklusra kiterjedő védelem, mely szerint a hatékony biztonsági előírások az adatkezelés teljes ciklusát átfogják a kezdettől a végig.

6. Láthatóság és átláthatóság, mely biztosítja, hogy az adatkezelések az érintettek számára is követhetőek legyenek.

7. Felhasználó magánszférájának tisztelete, mely megköveteli, az érintett érdekeinek szem előtt tartását, egyértelmű tájékoztatás és felhasználóbarát megoldások használata révén.

Privacy by design az 95/46/EK irányelvben

Európában a beépített adatvédelem – a szabályozás szintjén – elsőként a 95/46/EK irányelvben jelenik meg. Noha konkrétan maga a fogalom nem található meg a szabályozás szövegében, a (46) preambulum bekezdése rámutat, hogy *"az érintettek jogainak és szabadságainak védelme […] megkívánja, hogy megfelelő műszaki és szervezeti intézkedéseket hozzanak mind az adatfeldolgozó rendszer megtervezésekor, mind az adatfeldolgozás időpontjában."*[19] Emellett az irányelv 17. cikke szintén hangsúlyozza a megfelelő technikai intézkedéseket szükségességét: *„a tagállamoknak rendelkezniük kell arról, hogy az adatkezelő végrehajtsa a megfelelő technikai és szervezési intézkedéseket a személyes adatok véletlen vagy jogellenes megsemmisülése, véletlen elvesztése, megváltoztatása, jogosulatlan nyilvánosságra hozatala vagy hozzáférése elleni védelme érdekében […]."*[20]

Ezt figyelembe véve, az új adatvédelmi rendeletben már konkrétan megfogalmazott 25. cikk szerinti elvek (beépített és alapértelmezett adatvédelem) nem járnak új kötelezettségek bevezetésével, sokkal inkább

[19] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, HL 281/31, 1995.11.23 (a továbbiakban: 95/46/EK irányelv)

[20] 95/46/EK irányelv

annak értelmezésére szolgálnak, meghatározván, milyen módon kell az egyébként már létező kötelezettségeket végrehajtani.[21]

Privacy by design az általános adatvédelmi rendeletben

25. cikk szerint megfogalmazott *privacy by design* elv alapján: *„Az adatkezelő […] mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, […] másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába."*

Fontos kiemelni először is, hogy e megfogalmazás szerint a beépített adatvédelem pozitív kötelezettség, mely az adatkezelő aktív cselekvését követeli technikai és szervezési intézkedések végrehajtása révén. Másodsorban megfigyelhető a kockázatalapú megközelítés, mely intézkedések végrehajtása során az adatkezelőnek mindenképp figyelembe kell vennie a következő tényezőket:

- a tudomány és technológia állását (state of the art);
- a megvalósítás költségeit;
- az adatkezelés jellegét, hatókörét, körülményeit és céljait; illetve
- a természetes személyek jogaira és szabadságaira jelentett kockázatokat.[22]

A (78) preambulumbekezdés konkrét javaslatokat tartalmaz, ami e szervezeti intézkedéseket érinti: *„az említett intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat."*

Fontos megjegyezni, hogy a jogalkotó választási lehetőséget biztosít az adatkezelő számára, hiszen mind a 25. cikkben megjelent álnevesítés, mind a preambulumbekezdésben található idézett felsorolás ajánló jelleggel bír,

[21] Szabó 2016. 4.
[22] GDPR 25. cikk

meghagyva a lehetőséget bármi olyan technikai és szervezeti intézkedés használatára, mely a beépített adatvédelem céljai elérésére megfelelhet.[23]

A rendeletben fellelhető néhány ilyen intézkedés mellett gyakorlati szempontból az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (ENISA) ajánlása is segítséget nyújthat, felsorolva néhány adatvédelmi tervezési stratégiát. Az első négy stratégia magára az adatkezelésre, adattárolásra vonatkozik, majd a következő négy általános alapelveket fogalmaz meg:

1. Adatminimalizáció

Az adatminimalizáció szorosan összefügg az adattakarékosság elvével, mely szerint a kezelt adatok csak a célhoz szükséges megfelelő, releváns és korlátozott mértékben gyűjthetők. Esetenként egyéni vizsgálatra van szükség, és ennek alapján állapíthatómeg, mely adatok szükségesek feltétlenül a cél teljesítése érdekében.

2. Titkosítás

A titkosítás az egyik legmegbízhatóbb adatvédelmi módszer, különösen bizalmas vagy kényes adatok esetén, melyet a GDPR 32. cikk (1) bekezdésének a) pontja is megemlít. Ez a stratégia magába foglalja mind az információ átvitelekor történő titkosítási eljárásokat (kódolt üzenetek, titkos nyelvezet használata stb.), mind az anonimizálás és álnevesítés eszközeinek használatát. Fontos szempont és elvárás az anonimizáció során, hogy a kapcsolat ne legyen többé helyreállítható. Ez elsőre talán egyszerűnek tűnik, viszont a fejlődő technológiának köszönhetően nem könnyű feladat az adat és a természetes személy közötti kapcsolat végérvényesen megszüntetése.

3. Szétválasztás

A harmadik tervezési stratégia a szétválasztás, melynek lényege, hogy a gyűjtött személyes adatokat különálló részekre kell tagolni és ezeket, amikor csak lehetséges, külön adatbázisokban kell tárolni. Ezáltal kiküszöbölhető a profilalkotás lehetősége.[24]

4. Összesített, aggregált adatok használata

Az aggregáció esetén olyan egymástól különálló adatelemek vagy részek csoportosítása vagy összekapcsolása történik, amelyek önmagukban nem képesek az egyén azonosítására, viszont a kívánt cél eléréséhez (többnyire statisztikai elemzések végrehajtásához) elegendő információt nyújtanak. A

[23] Zanfir 2018. 174.
[24] European Union Agency for Network and Information Security (ENISA) 2014. 18-22.

rendelet szerint *" a statisztikai célú adatkezelés eredménye nem személyes adat, hanem összesített [aggregált] adat, ha ezt az eredményt vagy a személyes adatokat nem használják fel konkrét természetes személyekre vonatkozó intézkedések vagy döntések alátámasztására."*[25]

5. Tájékoztatás

Bármely adatkezelési művelet során fontos figyelembe venni a transzparencia elvét és biztosítani az érintettek megfelelő tájékoztatását. A 12. cikk szerinti tájékoztatás követelményei a következőek: tömör, átlátható, érthető és könnyen hozzáférhető forma tiszteletben tartása. Figyelni kell, hogy a közölni kívánt információ eredményesen célba érjen. Éppen ezért a tájékoztatónak minden más általános szerződési feltételtől vagy bármilyen más információtól különállónak kell lennie.[26]

6. Átláthatóság

Biztosítani kell továbbá, hogy az érintettek rendelkezhessenek az adataik felett, mely stratégia nagymértékben összefügg az átláthatóság elvével és a tájékoztatási kötelezettséggel. Az adatok feletti rendelkezés biztosítása a rendeletben feltüntetett érintetti jogok[27] tiszteletben tartásán is túlmutat, hiszen az azt is jelenti, hogy a felhasználók eldönthetik, hogy egy bizonyos rendszert használnak-e, ha igen a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogyan tekintenek bele vagy milyen egyéb módon kezelik, azt milyen adatokat és milyen céllal gyűjtik.[28]

7-8. Végrehajtás és elszámoltathatóság

Végezetül a 7. és 8. stratégia szorosan kapcsolódik egymáshoz és a beépített adatvédelem alapját képezi. Ezek a végrehajtás és az elszámoltathatóság, melyek megkövetelik olyan technikai és szervezeti politikák implementálását amelyek egyaránt tiszteletben tartják a rendelet alapelveit és az érintettek adatkezeléssel kapcsolatos jogait.

Ahhoz, hogy a vállalatok/szervezetek eleget tudjanak tenni mind a *privacy by design*, mind az elszámoltathatóság elvének, meg kell találniuk az adott helyzetben legmegfelelőbb technikai vagy szervezeti intézkedést. Ez gyakorta komoly fejtörést okoz, hiszen számtalan különféle szituáció állhat elő az adatkezelés jellegétől vagy a vállalat/szervezet fő tevékenységétől függően.

[25] GDPR (162) preambulumbekezdés
[26] GDPR 12. cikk
[27] GDPR 15-22. cikk
[28] GDPR (39) preambulumbekezdés

Fontos kiemelni, hogy a rendelet nem határozza meg pontosan a bizonyítás eszközeit. Legtöbb esetben ennek kiválasztást az adatkezelőre bízza. Ugyanakkor mintegy ajánlásként a rendeletben több helyen is megjelenik a jóváhagyott magatartási kódexekhez vagy jóváhagyott tanúsítási mechanizmushoz való csatlakozás a bizonyítás eszközeként. Ilyen például a 24 cikk (3) bekezdése, mely szerint a 40. cikk szerinti jóváhagyott magatartási kódexekhez, vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítási részeként, hogy az adatkezelő teljesíti kötelezettségeit. A 32. cikk (3) bekezdése alapján a tanúsítási mechanizmusokhoz való csatlakozás révén az adatbiztonsági kötelezettségek betartását is bizonyítani lehet. A 25 cikk (3) bekezdése alapján a 42. cikk szerinti, jóváhagyott tanúsítási mechanizmus szintén felhasználható annak bizonyítása részeként, hogy az adatkezelő a beépített és alapértelmezett adatvédelem követelményeinek eleget tesz.

A (77) preambulumbekezdés megemlíti ugyanakkor, hogy *„a megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához, továbbá a kockázat mérséklésével kapcsolatos bevált gyakorlatoknak az azonosításához útmutatással szolgálhatnak különösen a jóváhagyott magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Testület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások.”*

A gyakorlatban a megfelelés bizonyítására szolgáló eszköz mindig az adatkezelés jellegétől fog függeni.

Az előzetes hatásvizsgálat elvégzése az adatkezeléssel kapcsolatos döntések meghozatalát segítő fontos lépés. A 29. cikk alapján létrehozott adatvédelmi munkacsoport véleménye szerint a beépített adatvédelem elve összhangban van az adatvédelmi hatásvizsgálattal, hiszen a hatásvizsgálatot minden esetben „az adatkezelést megelőzően” kell elvégezni. Nem elhanyagolható tény viszont, hogy az előzetes hatásvizsgálat elvégzése csak bizonyos esetekre terjed ki, amely kijelentés nem vonatkozik a beépített adatvédelem elvének való megfelelésre.

4. Az adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálat kockázatalapú megközelítés, melynek célja a magánszférát veszélyeztető eljárások azonosítása és teljes vagy részleges kiküszöbölése,[29] és amely az adatvédelmi megfelelés bizonyítására is szolgálhat.

A 35. cikk szerinti adatvédelmi hatásvizsgálat célja az adatkezelés kockázatainak feltárása, a szükségesség és arányosság vizsgálata, valamint az esetleges kockázatok és korlátozások felismerése, orvoslása vagy kezelése.[30] Ennek elvégzése nagymértékben segítheti az adatkezelőket abban, hogy átfogóan kezeljék az adatvédelmi kockázatokat.[31]

A hatásvizsgálat szükségessége

Amennyiben az adatkezelés magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl. profilalkotáson alapuló döntéshozatal, különleges adatok nagyszámú kezelése), akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot köteles végeznie arra vonatkozóan, hogyan érintik a tervezett adatkezelési műveletek a személyes adatok védelmét. A hatásvizsgálat célja tehát nem más, mint az adatkezelés kockázatainak feltárása, a szükségesség és arányosság vizsgálata, illetve a kockázatok felismerése és esetleges kezelése.[32] A rendelet szerint magas kockázatúnak kell tekinteni az automatizált adatkezeléseket (ideértve a profilalkotást is), a személyes adatok különleges kategóriáinak vagy büntetőjogi felelősség megállapítására vonatkozó személyes adatoknak a tömeges kezelését, valamint a nyilvános helyek nagymértékű, módszeres megfigyelését is. [33]

A szabályozás szövegében fellelhető „különösen”[34] szó jelzi azonban, hogy a felsorolás nem kimerítő jellegű. Előfordulhatnak olyan „magas kockázatú” adatkezelési műveletek, amelyek ugyan nem szerepelnek a felsorolásban, mégis hasonlóan szükségessé teszik a szóban forgó hatásvizsgálat

[29] Bygrave 2017. 106.
[30] Jóri 2018. 349.
[31] A 29. cikk szerinti adatvédelmi munkacsoport 5/2010. számú véleménye a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló ágazati javaslatról.
[32] Jóri 2018. 350.
[33] GDPR 35. cikk
[34] GDPR 35. cikk (3) bekezdés

elvégzését. Mivel a meghatározás nem konkrét, így az adatkezelő felelőssége marad megvizsgálni a feltételek fennállását, és eldönteni a hatásvizsgálat szükségességét.

Valószínűsíthetően magas kockázat

A hatásvizsgálat szükségességének egyik feltétele a valószínűsíthetően magas kockázat megléte az érintett jogaira és szabadságaira nézve. A 29. cikk szerinti adatvédelmi munkacsoport véleménye alapján 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."* Önmagában a kockázat megléte nem elegendő, ennek valószínűsíthetően magasnak kell lennie, melynek felismerése szintén az adatkezelőt terheli. Ez különösen jellemző lehet az új adatkezelési technológiák bevezetésének alkalmazásakor, hiszen ezekben az esetekben nem ismert, hogy ezek milyen hatással lehetnek az érintettek jogaira és szabadságaira. Amennyiben az adatkezelő nem képes eldönteni a valószínűsíthetően magas kockázat jelenlétét, a munkacsoport ajánlása alapján érdemes elvégezni a hatásvizsgálatot, ami mindenképpen segítséget nyújt a megfelelésben.[35]

A hatásvizsgálat tartalmi követelményei

Míg a hatásvizsgálat szükségessége esetről esetre változik, ennek tartalmát a rendelet pontosan meghatározza. Eszerint a hatásvizsgálatnak ki kell terjednie legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és

[35] Jóri 2018. 353.

- a kockázatok kezelését célzó intézkedések bemutatására, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákra, biztonsági intézkedésekre és mechanizmusokra.

Amennyiben az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére, akkor kötelező konzultálni a hatáskörrel rendelkező felügyeleti hatósággal.[36]

A *privacy by design* elvéhez hasonlóan itt is megjelenik az azonosított kockázatok orvoslására szükséges biztonsági intézkedések és mechanizmusok bevezetése.

A privacy by design és a hatásvizsgálat közötti kapcsolat

A két fogalom közötti kapcsolat vizsgálatát, a *privacy by design* proaktív tulajdonságánál érdemes kezdeni, miszerint az adatvédelmi kérdésekre már az adatkezelési folyamatok tervezési fázisában figyelni kell, megelőzve ezáltal a probléma keletkezését. A stratégiai gondolkodás kiemelten fontos szerepet tölt be, amennyiben olyan adatkezelési folyamatok kidolgozására törekszünk, amelyek tiszteletben tartják az adatvédelmi alapelveket. A vállalati szférában gyakori jelenség, hogy az adatvédelmi kérdésekkel kapcsolatban mindig adott probléma kezelésére a cél. Ennek megoldása azonban nem jelenti az alapelveknek való teljes körű megfelelést, hiszen a *privacy by design* elv e magatartás pontos ellentétét követeli.

A megelőzés gondolata olyannyira fontos, hogy a 46. preambulumbekezdés a szolgáltatások és alkalmazások előállítóját is be kívánja vonni az elv betartásába. Eszerint: *„az olyan alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek, a termékek, szolgáltatások és alkalmazások előállítóit arra kell ösztönözni, hogy e termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védelméhez való jogot, és a tudomány és technológia állását kellően figyelembe véve gondoskodjanak*

[36] Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e (továbbiakban: WP29 iránymutatás hatásvizsgálatról)

arról, hogy az adatkezelők és az adatfeldolgozók adatvédelmi kötelezettségeiknek eleget tegyenek."

Ez nem jelent mást, minthogy a beépített adatvédelem elvének betartása nem a már meglévő kockázatok elemzését vagy kiküszöbölését hivatott kezelni, sokkal inkább az adatvédelmi alapelvek vállalati kultúrába való bevezetését jelenti. Ezáltal bármely termék szolgáltatás vagy folyamat fejlesztésekor vagy bevezetésekor az érintettek jogainak és szabadságainak tiszteletben tartása elsődleges szemponttá válik.[37] Ezzel ellentétben az adatvédelmi hatásvizsgálat legtöbb esetben reaktív, mintsem proaktív jellegű. Elsősorban azért, mert a hatásvizsgálat szükségességének megállapításakor már egy megtervezett adatkezelési folyamatot vizsgálunk meg, hiszen – ahogy azt fentebb említettük – ez kifejezetten meghatározott esetekben szükséges.[38] Másodsorban a hatásvizsgálat célja végső soron a megfelelés, nem pedig az alapvető adatvédelmi garanciáknak a technológiai tervezésbe történő beépítése.

Mindezek ellenére az adatvédelmi hatásvizsgálat elvégzése és felülvizsgálata nemcsak a folyamatos fejlődés szempontjából hasznos, de az idővel változó környezetben az adatvédelem szintjének fenntartásához is elengedhetetlen. Akkor is szükségessé válhat, 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.[39]

A megfelelő technikai és szervezeti intézkedések nemcsak a beépített adatvédelem meghatározásában (*„mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket*"[40]), hanem az adatvédelmi hatásvizsgálat tartalmi követelményeiről szóló rendelkezésekben is fellelhető: *„hatásvizsgálat kiterjed legalább […] a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más*

[37] Fazlioglu 2018.

[38] International Association of Privacy Professionals 'CHECK OR MATE? Strategic Privacy by Design' dataprotection.industries/wp-content/uploads/2017/10/strategic-privacy-by-design.pdf *(*letöltve: 2020.02.15.)

[39] A 29. cikk alapján létrehozott adatvédelmi munkacsoport iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e, 16.

[40] GDPR 25. cikk

személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat."[41]

Bár mindkét esetben az említett technikai intézkedések és mechanizmusok fogalma ugyanazokat a kivitelezési módokat takarja (álnevesítés, szétválasztás, összesített adatok, tájékoztatás stb.), tovább elemezve fontos különbséget észlelhetünk. A rendelet 36. cikke szerint ugyanis, amennyiben a hatásvizsgálat megállapítja, hogy az adatkezelés a kockázat mérsékelése céljából teendő adatkezelői intézkedések hiányában valószínűleg magas kockázattal jár, az adatkezelő köteles konzultálni a felügyeleti hatósággal, mely köteles írásban tanácsot adni. Ennek alapján akár az adatkezelő által választott technikai intézkedések megváltoztatatásra vagy a szóban forgó adatkezelés teljes kiküszöbölésére is sor kerülhet. A beépített adatvédelem alkalmazása során választott és használt intézkedéseknek ilyen formai követelményeknek nem kell eleget tenniük. Ebből is pontosan látszik, hogy a hatásvizsgálat elvégzése nem tekinthető a beépített adatvédelemnek való megfelelés lépésének, két különböző helyzet és kötelezettségnek való megfelelésről lévén szó.

5. Következtetések

A fenti elemzés alapján kijelenthető, hogy az elszámoltathatóság elvének való megfelelés részeként az adatvédelmi szabályozás elveit be kell építeni az adatkezelési technológiákba, mind a tervezés, mind a működtetés során. A technológiát úgy kell megtervezni és megvalósítani, hogy egész életciklusát a demokratikus társadalmainkat meghatározó alapvető jogokkal és értékekkel kompatibilis módon lehessen működtetni. Ugyanakkor a hatásvizsgálat elvégzése – mint ahogy a beépített adatvédelem vállalati kultúrába való bevezetése sem – nem tekinthető standard, minden vállalat szempontjából ugyanolyan formában teljesíthető kötelezettségnek. Az adatkezelőknek esetről esetre kell dönteniük a megfelelő szervezeti és technikai intézkedések alkalmazásáról, mely függhet a vállalat/szervezet méretétől, célcsoportjától vagy akár főtevékenységétől. A beépített adatvédelem stratégia, a hosszú távú tervezés alapköve, mely megköveteli az adatvédelmi alapelvek és az érintettek jogainak és szabadságainak tiszteletben tartását már az első lépéstől kezdve, bármilyen üzleti

[41] GDPR 35. cikk. (7) bekezdés

folyamatról legyen szó. Mindez lehetetlen az adatvédelmi tudatosság fejlesztése nélkül, melyet a munkavállalóknak és a vezetőknek is szükséges elsajátítani. Figyelemmel tehát a beépített adatvédelem elveire, a megfelelő adatvédelmi irányítási keretrendszer bevezetése az adatvédelmi elszámoltathatóság követelményét operacionalizálja. Egy keretrendszer ugyanis igazolhatóvá teszi az adatvédelmi kontrollok bevezetését és azok alkalmazását, a kockázatcsökkentő intézkedések dokumentáltságát és ezek belső vagy külső ellenőrzését.

Felhasznált irodalom

A 29. cikk alapján létrehozott adatvédelmi munkacsoport iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e WP 248 rev.01. 2017.04.04.

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

A 29. cikk szerinti adatvédelmi munkacsorport iránymutatása az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához, WP251 rev.01, 2018.02.06

A 29. szerinti adatvédelmi munkacsoport 3/2010 vélemény az elszámoltathatóság elvéről, WP 173, 2010.07.13.

Állásfoglalás a beépített adatvédelemről, elfogadta az adatvédelmi biztosok 32. nemzetközi konferenciája, Jeruzsálem, 2010.10.27.–29, https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf (letöltve: 2020.02.25.)

Ann CAVOUKIAN: *Privacy and Security by Design: An Enterprise Architecture Approach.* Oracle, Ontario, Canada 2013.

ÁRVAI Viktor György [et al.]: *Az elszámoltathatóság alapelve és az adatkezelő kötelezettségei.* NKE, Budapest 2018.

BALOGH Zsolt [et al.]: Technológia a jog szolgálatában? – Kísérletek az adatvédelem területén adatvédelem és technológia – privát szférát erősítő

technológiák – beépített adatvédelem elve – Privacy by Design'. *Pro Futuro* 2014/1.

Center for Information Policy Leadership, The Central Role of Organisational Accountability in Data Protection Discussion Paper 2 (of 2), Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf (letöltve: 2020.01.26.)

Christopher KUNER [et al.]: *The EU General Data Protection Regulation (GDPR), A commentary.* Oxford University Press, United Kingdom 2020

Christopher WILLIAMS: *Leadership accountability in a globalizing world.* Palgrave Macmillan, London 2006.

European Union Agency for Network and Information Security (ENISA), Privacy and Data Protection by Design– from policy to engineering, 2014, 18-22. forrás: www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport , (letöltve: 2020.01.05.)

Gabriella ZANFIR-FORTUNA [et al.]: Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR. *European Data Protection Law Review,* EDPL 2018.

International Association of Privacy Professionals: CHECK OR MATE? Strategic Privacy by Design. 2018 dataprotection.industries/wp-content/uploads/2017/10/strategic-privacy-by-design.pdf (letöltve: 2020.02.15.)

Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e, WP 248 rev.01, 2017.10.4.

JÓRI András [et al.]: *A GDPR magyarázata.* HVG-ORAC, Budapest 2018.

Lee A. BYGRAVE: Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review,* 2017.

Markus HEYDER - Sam GROGAN: The role of DPAs in incentivizing accountability. 2018.07.30, www.iapp.org/news/a/the-role-of-dpas-in-

incentivizing-accountability/?fbclid=IwAR1FrLNz7Rv9Te-MRFFXSZvy-vJf9hiE_vtxCSzLwcoXPAt554rslOr0evs ,(letöltve: 2020.02.14.)

Müge FAZLIOGLU: 10 Operational Responses to the GDPR – Part 4: Data protection impact assessments and data protection by default and by design. iapp.org/news/a/top-10-operational-responses-to-the-gdpr-part-4-data-protection-impact-assessments-and-data-protection-by-default-and-by-design/ (letöltve 2020.03.05)

Nemzeti Adatvédelmi és Információszabadság Hatóság, Adatvédelmi értelmező szótár, www.naih.hu/adatvedelmi-szotar.html (letöltve: 2020.02.18.)

SZABÓ Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II. *Pázmány Law Working Papers*, 2016/27.

***

Data protection compliance: privacy by design and impact assessment as a tool for accountability
Summary

Accountability represents a comprehensive approach to data protection where the data controller must be able to demonstrate that he has taken appropriate and effective organizational and technical measures for the protection of personal data. The key elements covering all aspects of a solid data protection and management program are: leadership and oversight; risk assessment (including DPIAs); policies and procedures relating to data processing; transparency; training and awareness; monitoring, verification and response; complaint-handling and enforcement. The essential elements make it clear that accountability comes from privacy protections based on commitment to a program where privacy is built into all business processes, where privacy by design is a process map for putting the essential elements of accountability into effect.