[24] A Bíróság a vallási reklámok tilalmát jóváhagyó Murphy v. Írország ügyben kimondta, hogy általában szélesebb mérlegelési jogkör áll rendelkezésre, ha a véleménynyilvánítás korlátozása olyan kérdésekkel kapcsolatos, mint a személyes megítélés körébe tartozó erkölcs, illetve különösen a vallás. A Bíróság hozzátette, a mérlegelési jogkör terjedelme az, ami megkülönbözteti Murphy ügyet a VgT esettől, mivel utóbbiban úgy ítélte meg, hogy a reklám tilalma közérdekű kérdést érintett, amelyre szűkebb mérlegelést kell alkalmazni (§ 67.).

[25] A Bíróság a Murphy v. Írország ügyben a vallási, egyházi reklámok tilalmát többek között arra hivatkozva találta elfogadhatónak, hogy a vallási közösségek tagjai ne szembesüljenek más világnézetet hirdető közlésekkel a magánszférába behatolni képes médián keresztül, megsértve a hívők vallási érzékenységét. A vallási érzékenység, a reklám megosztó vagy támadó jellege miatt valóban nehéz lenne a tilalom eseti alapú alkalmazása, ami lehetővé teszi a teljes tilalmat. Ilyen érzékenység azonban a politikai reklámok esetében nem létezik. Lásd: Lewis, Tom: Reasserting the Primacy of Broadcast Political Speech after Animal Defenders International? – Rogaland Pensioners Party v Norway. Journal of Media Law, Vol. 1., 2009. p. 37–48.

[26] Polgári Eszter: Az Emberi Jogok Európai Bíróságának ítéleteiből. Fundamentum, 2009/1. p. 126–127.

[27] Animal Defenders International v. United Kingdom; 2013. április 22., Application no. 48876/08.

[28] 2007. december 31-ig a Broadcast Advertising Clearance Centre (BACC) felelt a televíziós reklámok előzetes vizsgálatáért és engedélyezéséért az elektronikus médiában.

[29] A hirdetés megtekinthető az interneten: http://www.youtube.com/watch?v=qON_IFQE4HY [2014. 01. 12.]

[30] R (Animal Defenders International) v. Secretary of State for Culture Media and Sport [2008] UKHL 15.

[31] Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland; 2012. június 21., Application no. 34124/06., § 56.

[32] Hasonló érvelés jelent meg a már említett Murphy v. Írország ügyben is. A strasbourgi Bíróság szerint a vallási reklámok korlátozásának célja többek között annak megakadályozása, hogy a nagyobb egyházak a reklámidő megfizetésével nagyobb befolyást tudjanak szerezni. Továbbá ha lehetővé tennék a vallási reklámok akár korlátozott sugárzását is, lehetetlen volna az egyes reklámok méltányos, objektív és koherens hatósági ellenőrzése (§ 77.).

[33] Fathaigh, Ronan Ó: Ban on Political Advertising Does Not Violate Article 10: Animal Defenders International v. UK. Strasbourg Observers, 2013. április 24. http://strasbourgobservers.com/2013/04/24/ban-on-political-advertising-does-not-violate-article-10/ [2014. 01. 12.]

[34] Citizens United v. Federal Election Commission, 558 U.S. 310 (2010); Unger Anna: Puha pénzek, kemény kampány és a szólásszabadság: az amerikai legfelső bíróság ítélete a kampányfinanszírozásról. Fundamentum, 2010/3. p. 63–71.; Udvary Sándor: Citizens United – Nem európainak való vidék. In Medias Res, 2012/2. p. 211–240.

[35] Rowbottom, Jacob: A surprise ruling? Strasbourg upholds the ban on paid political ads on TV and Radio. Inform's Blog, 2013. április 23. http://inforrm.wordpress.com/2013/04/23/a-surprise-ruling-strasbourg-upholds-the-ban-on-paid-political-ads-on-tv-and-radio-jacob-rowbottom/ [2014. 01. 12.]; Kóczián Sándor: Az Emberi Jogok Európai Bírósága ítéleteiből. Fundamentum, 2013/1. p. 105–109.

[36] Rowbottom, Jacob H.: Animal Defenders International: Speech, Spending and a Change of Direction in Strasbourg. Journal of Media Law, 2013., Oxford Legal Studies Research Paper No. 64/2013. p. 6. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2267411 [2014. 01. 12.]

[37] Rowbottom, Jacob H.: i. m. p. 11.

[38] Rowbottom, Jacob H.: i. m. p. 9.

[39] Fathaigh, Ronan Ó: i. m.

[40] Jones, Clifford A.: Regulating political advertising in the EU and USA: a human rights perspective. Journal of Public Affairs, Vol. 4., 2004. p. 244–255.; Rafter, Kevin: Political Advertising: The Regulatory Position & the Public View. Broadcasting Authority of Ireland, Dublin, 2009. p. 18., 20. http://www.bai.ie/wordpress/wp-content/uploads/200911_KR-PoliticalAdvertising-RegPositionPublicView_PK.pdf [2014. 01. 12.]

Szőke Gergely László

Az önszabályozás, audit és tanúsítás lehetőségei és korlátai az adatvédelem területén

1. BEVEZETŐ GONDOLATOK

Az adatvédelmi szabályozás újabb tendenciái, különösen az Európai Unió várható új adatvédelmi szabályozása, egyértelműen az önszabályozás különböző formáinak erősödése, valamint az auditálás illetve különböző címkéző-tanúsító rendszerek jelentőségének növekedése felé mutatnak. Jelen tanulmány áttekintő jelleggel mutatja be az önszabályozásban rejlő lehetőségeket és korlátokat, valamint az adatvédelmi felügyelet sajátos intézményeként felfogható adatvédelmi audit főbb jellemzőit – kitérve annak hatályos magyar szabályozására.

A szerző a PTE ÁJK Informatikai és Kommunikációs Jogi Tanszék kutatója, a PTE belső adatvédelmi felelőse.

2. ADATVÉDELEM ÉS ÖNSZABÁLYOZÁS

Európában az adatvédelmi irányelv[1] elfogadása megteremtette a többékevésbé egységes európai szabályozást, amely – úgy tűnik – kevésbé teszi szükségessé az önszabályozás különböző formáit.[2] Az Egyesült Államokban ezzel szemben – épp az egységes szövetségi szintű adatvédelmi szabályozás hiánya miatt – az iparági (adatvédelmi) önszabályozásnak komoly szerepe van. Ez azon az üzleti alapú megközelítésen alapul, amely szerint az üzleti élet szereplői képesek a fogyasztói elvárásoknak megfelelő szabályozást kialakítani[3] kivédve ezzel az állami szabályozást.[4] Az Egyesült Államok önszabályozási mechanizmusait számos kritika éri, és jelen tanulmányunkban sem ezt tartjuk követendőnek: Európában ugyanis – szemben éppen az Egyesült Államok példájával – jellemzően nem az állami szabályozást helyettesítő, sokkal inkább azt kiegészítő, pontosító, „végrehajtási sza-

bály" jellegű szerepet tölthetnek be az önszabályozás különböző formái, így (bár a tanulmányban a külföldi szóhasználathoz igazodva az önszabályozás kifejezést használjuk) valójában pontosabb e szabályozási megoldásokra társszabályozásként tekinteni.

Az önszabályozás potenciális eszközeinek
1. a magatartási kódexeket,
2. a különböző szabványokat, valamint
3. az adatkezelők szintjén elfogadott (belső) szabályozásokat
tekintjük. Az alábbiakban e területeket vizsgáljuk részletesen.

2.1. Ágazati magatartási kódexek

2.1.1. Az irányelv rendelkezései

Az európai adatvédelmi irányelv kifejezetten támogatja az önszabályozás bizonyos formáit: a 27. cikk kifejezetten utal magatartási kódexek (codes of conduct) elfogadásának lehetőségére, és a kódexek kidolgozói számára megteremti azt a lehetőséget is, hogy azokat véleményezés céljából a nemzeti adatvédelmi hatóság vagy a 29-es munkacsoport elé terjesszék, amelyek kötelesek a kódex és a nemzeti jog összhangját vagy annak hiányát megállapítani.[5] Európai szintű elismerésben egyelőre csak két szervezet magatartási kódexe részesült:[6] a Nemzetközi Légi Szállítási Szövetségé[7] és az Európai Direkt és Interaktív Marketing Szövetségé.[8]

Az új európai adatvédelmi szabályozásban az adatkezelők felelőssége és elszámoltathatósága (accountability) olyan új alapelvként jelenik meg, amelynek tényleges megvalósítása számos, az adatkezelők szintjén elfogadott belső szabályozókkal valósítható meg. Mind a Bizottság eredeti szövegtervezete, mind a LIBE javaslat jelentősen növeli az adatkezelők kötelezettségeit.

2.1.2. A Rendelettervezet szabályai

A Bizottság eredeti, 2012-ben kiadott rendelettervezete[9] lényegében a hatályos irányelv szabályozásához hasonlóan rendelkezett „eljárási szabályzatok" (magatartási kódexek)[10] létrehozásáról. A kódexek kidolgozói számára ez alapján is fennállna az a lehetőség, hogy azokat véleményezés céljából a nemzeti adatvédelmi hatóságok elé terjesszék, amelyek véleményt adhatnak e kódexekről.[11] Az Európai Parlament illetékes bizottsága által kidolgozott, és az Európai Parlament 2014. március 12-i plenáris ülésén óriási többséggel változtatás nélkül elfogadott ún. LIBE javaslat[12] ezen lényegében csak annyit változtat, hogy kötelezővé teszi az értékelést a nemzeti hatóságok számára (csakúgy, mint a hatályos irányelv alapján).[13]

2.2. Szabványosítási törekvések

Az önszabályozás egy másik lehetséges iránya a szabványosítás, amely lényegében abban tér el más önszabályozási formáktól, hogy valamely szabvánnyal foglalkozó szervezet keretei között dolgozzák ki.[14] A szabványosítással kapcsolatos legjelentősebb kutatások között említhető az Európai Szabványügyi Bizottság[15] Információs Társadalom Szabványosítási Rendszer[16] (CEN/ISSS) keretében 2000-ben indult, „Európai adatvédelmi szabvány kezdeményezés" elnevezésű[17] projekt, amelynek zárójelentése[18] számos releváns megállapítást tartalmaz a szabványosítás lehetőségeiről és korlátairól, az adatvédelmi auditálással kapcsolatos kérdésekről, és a magánszféravédő technológiákról.[19] A dokumentum végül arra a következtetésre jut, hogy a globális és átfogó szabvány kialakítása nem időszerű,[20] de konszenzus alakult ki arról, hogy további lépéseket kell tenni egyrészt a témát illető elemzések, másrészt önkéntes iránymutatások (guidance) kidolgozása terén. Ennek eredményeként született meg 2005-ben egy öt, majd 2010-ben egy további három dokumentumból álló informális szabványcsomag, ún. CEN Workshop Agreement.[21]

Végül érdemes megemlíteni az ISO/IEC 29100 szabványt,[22] amely azonban nem alkalmas teljes adatvédelmi kockázatelemzésre, vagy adatvédelmi irányítási rendszer kialakítására, mivel csak az adatvédelmi terminológia és adatvédelmi alapelvek egységesítésére törekszik,[23] (illetve meghatározza az adatkezelések potenciális szereplőit és feladatait).[24] Összességében tehát e szabvány csak az alapvető, definíciós kérdésekben kaphat szerepet.

2.3. Adatkezelők szintjén elfogadott szabályozások

Az önszabályozás további lehetséges – a fentieket nem kiváltó, hanem kiegészítő – iránya az adatkezelő szintjén elfogadott szabályozás (policy, szabályzat, eljárásrend stb.), amelyek hatálya nem egy-egy ágazatra/iparágra, csupán az adott szervezetre, vagy szervezetcsoportra (pl. vállalatcsoportra) terjed ki. E körben mindenképp említést érdemel a kötelező vállalati szabályok[25] térnyerése, amelyeknek az adatvédelmi szabályozásban (elsősorban harmadik országban történő adattovábbítással kapcsolatban) betöltött növekvő jelentőségét a 29-es munkacsoport BCR-rel foglalkozó dokumentumai is alátámasztják.[26] Ugyancsak megemlítendő, hogy több európai adatvédelmi törvény is kötelezően írja elő bizonyos szervezetek számára belső adatvédelmi (és adatbiztonsági) szabályzat elfogadását és/vagy belső adatvédelmi felelős kinevezését.[27] Bennett és Raab az önszabályozás egy típusának tekinti az adatvédelmi nyilatkozatokat is, amelyek mögött azonban nem feltétlenül állnak részletes belső szabályok.[28]

Az új európai adatvédelmi szabályozásban az adatkezelők felelőssége és elszámoltathatósága (accountability) olyan új alapelvként jelenik meg, amelynek tényleges megvalósítása számos, az adatkezelők szintjén elfogadott belső szabályozókkal valósítható meg. Mind a Bizottság eredeti szövegtervezete, mind a LIBE javaslat jelentősen növeli az adatkezelők kötelezettségeit.

Az adatkezelőknek mindenekelőtt kockázatértékelést kell majd végezniük, amely alapján eldönthető, hogy tevékenységük „valószínűsíthetően jelent-e sajátos kockázatokat". Amennyiben az adatkezelés jellemzői megfelelnek a javaslatban foglalt számos kritérium valamelyikének,[29] úgy az adatkezelőket további kötelezettségek terhelik: adatvédelmi hatásvizsgálat elvégzését és az adatvédelmi megfelelőség (compliance) időszakos felülvizsgálat is megköveteli majd a jogszabály. Az új rendelettervezet adatkezelőkre vonatkozó kötelezettségeinek részletes elemzése nélkül[30] is összességében megállapítható, hogy az adatkezelők szintén kialakított (irányítási) rendszer és a belső normák jelentősége az új európai adatvédelmi szabályozás során egyértelműen nőni fog.

3. ADATVÉDELMI AUDIT ÉS ADATVÉDELMI TANÚSÍTÁS

Az adatvédelmi auditálás, tanúsítás (és hozzá kapcsolódó címkézés) lényegében a fent említett különböző típusú önszabályozás/társszabályozás keretében elkészült szabályozókhoz kapcsolódó „felügyeleti" rendszerként értelmezendő.

3.1. Kiindulópontok

Mindenekelőtt érdemes áttekinteni az auditálással kapcsolatos alapfogalmakat, az audit/tanúsítás típusait, és az adatvédelmi auditálás előnyeit, hátrányait. Ezen áttekintéshez a vonatkozó – elsősorban külföldi – szakirodalmat, az ISO szabványok tanúsításával kapcsolatos forrásokat, és a már létező adatvédelmi audit módszertanokat használjuk.

3.1.1. Adatvédelmi audit és tanúsítás fogalma

Bár a jogirodalomban, illetve több különböző, adatvédelmi auditra vonatkozó módszertanban közvetlenül is szerepel az adatvédelmi audit fogalma, érdemes megnézni mindenekelőtt az ISO szabványcsalád – meglehetősen semleges – audit fogalmát. Eszerint: „az audit auditbizonyítékok nyerésére és ezek objektív kiértékelésére irányuló módszeres, független és dokumentált folyamat annak meghatározására, hogy az auditkritériumok milyen mértékben teljesülnek."[31]

Az adatvédelmi audit meghatározásakor CEN Workshop Agreement egyik dokumentumára támaszkodunk. Eszerint az adatvédelmi audit egy módszeres és független vizsgálat annak meghatározására, hogy az adatkezeléssel kapcsolatos tevékenységek összhangban vannak-e a szervezet adatvédelmi szabályaival (policyvel) és az EU adatvédelmi irányelvének követelményeivel.[32]

E két meghatározás segítségével megkísérlünk egy harmadik, mindkét fogalom alapvető elemeit felhasználó definíciót alkotni. Eszerint az adatvédelmi audit egy független, auditbizonyítékok[33] gyűjtésén és objektív értékelésén alapuló, módszeres és dokumentált vizsgálat annak meghatározására,

hogy egy szervezet adatkezelési tevékenysége[34] megfelel-e az e tevékenységre irányadó szabályoknak.[35]

Az auditálást rendszerint (de nem szükségszerűen) tanúsítás is követi, amely lényegében a pozitív auditjelentésen alapuló, meghatározott időszakra szóló tanúsítvány kiadását jelenti. A tanúsítást tehát mindenképp meg kell, hogy előzze az audit folyamata.

3.1.2. Az audit/tanúsítás típusai

3.1.2.1. Eszköz-audit és rendszer-audit

Mind a minőségirányítási rendszerekkel, mind az adatvédelmi auditálással foglalkozó szakirodalom megkülönbözteti a különböző eszközök, termékek auditálását (vagy másként: terméktanúsítás) az adatvédelemre vonatkozó rendszer-auditálásától (rendszer-audit vagy rendszertanúsítás).

Valamely eszköz (termék) tanúsítása biztosítékot jelent arra, hogy a termék megfelel a vonatkozó jogszabályoknak, az előírt szabványoknak és egyéb dokumentumoknak (szerződésben előírt követelményeknek).[36] Az adatvédelmi eszköz-audit tulajdonképpen az adatfeldolgozási hardver- és szoftver-termékek adatvédelmi és adatbiztonsági megbízhatóságának auditálására és adott esetben tanúsítására irányuló egyszeri eljárás, amely jelentősen megkönnyítheti az adatvédelmi szempontból megbízható eszközök kiválasztását is.[37]

A rendszer-audit célja, hogy – a fenti definícióval összhangban – egy szervezet adatkezelésekkel kapcsolatos tevékenységét értékelje. A rendszer-auditként értelmezett adatvédelmi audit feltételezi egy olyan adatvédelmi irányítási rendszer kialakítását, amely integrálja és konkretizálja az adatkezelővel szemben a szabályozás alapján fennálló kötelezettségeket.[38] Jelen tanulmányban az adatvédelmi audit alatt kizárólag rendszer-auditot értünk.

3.1.2.2. Belső, beszállítói és külső audit

Az auditot végző személy/szervezet alapján megkülönböztethető belső, beszállítói és külső audit.

A belső audit során az adott adatkezelő szervezet maga végzi el a vizsgálatot és az értékelést, amelyről dokumentációt készít.[39] Ha egy szervezet rendelkezik belső adatvédelmi felelőssel vagy más adatvédelemért felelős szervezeti egységgel, akkor a belső audit gyakran e személy vagy szervezeti egység feladata. A belső audit jellemzően nem jár együtt külön tanúsítvány kibocsátásával, de előfordul, hogy valamely tanúsítvány több éven keresztül történő használatához előfeltétel a meghatározott időszakonként lefolytatott belső audit.

Az ún. beszállítói auditra rendszerint akkor kerül sor, ha egy szervezet kiszervezi az adatkezelés tevékenységét, és szeretne meggyőződni a partner adatvédelmi rendszerének megfelelőségéről.[40]

Végül a külső audit során a szervtől elkülönült, független szerv végzi el az auditot: ez lehet az adott állam adatvédelmi hatósága (Magyarország mellett néhány európai országban is találunk erre példát) vagy piaci szereplő. Előfordul, hogy az adatvédelmi auditálásban érdekelt szervezetek valamely más, például informatikai biztonsági vagy minőségirányítási rendszerek tanúsításával kapcsolják össze az adatvédelmi tanúsítás szolgáltatás igénybevételét is.[41]

3.1.2.3. Alkalmassági audit (adequacy audit) és megfelelőségi audit (compliance audit)

Az ICO adatvédelmi audit kézikönyve, és az azt elemző magyar kutatás alapján megkülönböztethető ún. alkalmassági audit (adequacy audit) és megfelelőségi audit (compliance audit).

Az alkalmassági audit annak megállapítására irányul, hogy az adatkezelő szervezetnél található különböző dokumentumok: szabályzatok, policy-k, gyakorlati útmutatások stb. megfelelnek-e a központi adatvédelmi jogszabályok előírásainak. Az auditálás ezen szakasza nem feltétlen igényel helyszíni vizsgálatot, csupán az iratok áttekintésével jár.

A megfelelőségi audit célja annak megállapítása, hogy az adatkezelő szervezet tényleges működése (adatkezelési gyakorlata) megfelel a dokumentált szabályzatainak és a jogszabályoknak. Ezen eljárás megköveteli helyszíni vizsgálatok elvégzését, és rendszerint a munkatársaktól való információgyűjtést is.[42]

Nyilvánvaló, hogy lényegesen alaposabb a megfelelőségi audit, mivel az a tényleges helyzet feltárására és értékelésére irányul, nem csak a dokumentáció törvényességének vizsgálatára.

Megjegyezzük, hogy hasonló szempontrendszer szerint három típusba is sorolható az megfelelőség-értékelés. Bennett és Raab nevesíti a „policy-megfelelést" (compliance of policy), amely lényegében egyet jelent az alkalmassági audit eredményeként fennálló megfeleléssel. Az „eljárások megfelelősége" (compliance of procedure) a szerzők szerint azt igazolja, hogy az adott szervezet megfelelő eljárásokkal implementálja és végrehajtja a szabályzatait, míg a harmadik típus, a „gyakorlat megfelelősége" (compliance of practice), azt igazolja, hogy az adott szervezet tényleges tevékenysége megfelel a rá vonatkozó szabályzatoknak.[43] Utóbbi lényegében megegyezik a megfelelőségi audittal.

3.1.3. Az adatvédelmi tanúsítás előnyei, hátrányai – az érintett szervezetek motivációja

Első ránézésre is egyértelmű, hogy az adatvédelmi tanúsításhoz szükséges auditálásra való felkészülés azt feltételezi, hogy az adott szervezet alaposan megvizsgálja az adatkezeléssel kapcsolatos dokumentumait és gyakorlatát, így az adatvédelmi audit intézménye nagyban hozzájárul az adatkezelők adatvédelmi tudatosságának, érzékenységének erősítéséhez. Az auditálás feltételezi az adatvédelmi elképzelések, célkitűzések rendszerezett rögzítését, és a megvalósítás eszközrendszerének előzetes felvázolását is. Ellenérvként felhozható, hogy az önkéntes audit nem alkalmas az adatvédelmi színvonal általános, széles körű javítására, mivel abban valószínűleg azok az adatkezelők vesznek részt, akik korábban is magas színvonalú védelmet biztosítottak, és kimaradnak belőle azok, akik az adatvédelmi követelményekre kisebb hangsúlyt helyeznek.[44]

Emellett jelentős motivációs tényező lehet az adatkezelők számára, hogy a sikeres auditáláshoz kapcsolódó tanúsítvány megfelelő kommunikációja alkalmas az ügyfelek illetve az állampolgárok adott szervezet felé megnyilvánuló bizalmának növelésére is.[45] Az adatvédelmi erőfeszítések tehát potenciális versenyelőnyt is jelenthetnek.[46]

További motivációként értékelhető a jogellenes adatkezelésből eredő hátrányok, elsősorban a hatósági bírság elkerülése. Az egyre komplexebbé váló adatkezelések áttekintése növekvő kihívást jelent az adatkezelő szervezetek számára, márpedig alapos vizsgálat és értékelés nélkül az adott szerv egyszerűen nem lehet biztos benne, hogy valamennyi adatkezelése valóban jogszerű. Megjegyezzük, hogy az európai adatvédelmi jog fejlődése is egyértelműen abba az irányba mutat, amely feltételezi az adatkezelők saját adatkezelési rendszerükhöz való eddigieknél sokkal tudatosabb hozzáállását.

Emellett az auditálásból következő előny lehet a szervezeten belüli folyamatok ellenőrizhetőbbé válása is,[47] azaz az adatkezelési folyamatok „rendbetétele" jól illeszkedhet az adott szervezet általános irányítási rendszerének fejlesztéséhez is.

Az informatikai biztonsággal foglalkozó iparág folyamatosan fejlődése is együtt járhat az adatvédelmi (jogi) kérdések előtérbe kerülésével. Az informatikai biztonsági szabványok ugyanis több esetben előírják a különböző jogi követelményeknek való megfelelést is, így az adatvédelmi kérdések kisebb-nagyobb mélységben való vizsgálata nem megkerülhető az informatikai biztonsági irányítási rendszerek auditálása során sem.

Végül megjegyezzük, hogy az adatvédelmi audit jogszabályi szintű elismerése önmagában jelentősen növelheti a jogintézmény iránti bizalmat illetve annak népszerűségét.

3.1.4. Adatvédelmi audit és adatbiztonság

Az adatvédelmi audit szempontjainak meghatározásában is fontos elem az adatbiztonság. Ezzel kapcsolatban az új adatvédelmi törvény a korábbinál részletesebb követelményeket határoz meg. Mindenekelőtt általános alapelvként írja elő, hogy az adatkezelő az adatkezelési műveleteket köteles úgy megtervezni és végrehajtani, hogy az adatvédelmi törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét (ez lényegében a jogirodalomban igen népszerűnek számító Privacy by Design elvének jogszabályba iktatása). Az adatkezelőnek és az adatfeldolgozónak ugyanakkor az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére, de több lehetséges adatkezelési megol-

dás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja – kivéve, ha ez aránytalan nehézséget jelentene az adatkezelőnek.[48] „E rendelkezések az adatvédelmi szabályozás egészében meghonosítják az adatvédelemnek azt az elektronikus hírközlés és az elektronikus kereskedelem területén már korábban megjelent szemléletét,[49] amely az adatvédelmi garanciák érvényesülését kifejezetten az adatkezelő megfelelő biztonsági, szervezeti, eljárási rendjéhez kapcsolja. Ez a szemlélet az adatbiztonsági követelmények felértékelését hozza, és annak felismerésen alapul, hogy megfelelő adatbiztonság nélkül az adatvédelem jogszabályi feltételei sem teljesülhetnek."[50] A törvény ezen túlmenően a jogosulatlan adatbevitel megakadályozásától az adatfeldolgozó rendszerhez való hozzáférés ellenőrizhetőségén át az üzemzavar helyreállíthatóságáig meghatároz néhány konkrét adatbiztonsági elvárást,[51] amelyhez az adatkezelőnek és az adatfeldolgozónak igazodnia kell, és amelyek egy auditálási szempontrendszerben is helyet kaphatnak.

Mindenképpen pozitívum, hogy az új szabályozásban legalább utalás szintjén megjelenik a kockázatarányos biztonság elve, de még így is jelentős jogi megfelelőségi kockázatot jelent, hogy az adatbiztonság tényleges szintjéről a jogalkotó alig ad támpontot. Ezzel kapcsolatban a különböző informatikai biztonsági és minőségirányítási szabványok adhatnak eligazítást.

A fentiekből az is következik, hogy az – akár a hatóság, akár piaci szereplő által végzett – adatvédelmi auditálásnak és tanúsításnak ki kell terjednie valamilyen szinten az adatbiztonsági követelményekre is. Tekintettel arra, hogy az adatbiztonsági szabványok tanúsítása egyébként bevett szolgáltatásnak minősül, ezért célszerűnek tűnik az e tanúsítások során alkalmazott auditálási-tanúsítási módszereket az adatvédelmi auditálás módszertanának kidolgozásakor hangsúlyosan figyelembe venni.

3.2. Az adatvédelmi audit szabályozása

3.2.1. Adatvédelmi audit a Rendelettervezetben

Újdonságként került be a 2012-es bizottsági szövegtervezetbe egy adatvédelmi tanúsítással és címkézéssel kapcsolatos cikk, amely szerint (meglehetősen soft law jellegű megfogalmazással) a tagállamok, valamint a Bizottság – különösen európai szinten – ösztönznék olyan adatvédelmi tanúsítási mechanizmusok és adatvédelmi címkék és jelzők létrehozását, amelyek segítségével az érintettek gyorsan fel tudják mérni az adatkezelő és az adatfeldolgozó által biztosított adatvédelem szintjét.[52] Ugyanakkor e „szándéknyilatkozat" komolyságát mutatta, hogy a Bizottság felhatalmazást kapott volna az adatvédelmi tanúsítási mechanizmusokra vonatkozó szempontok és követelmények meghatározása érdekében további jogi aktusok elfogadására.[53]

A LIBE javaslat azonban ennél lényegesen továbbmegy. Az új 39. cikk szerint bármely adatkezelő vagy adatfeldolgozó ésszerű, az adminisztratív költségeket figyelembe vevő díj ellenében bármely uniós felügyelő hatóságot felkérheti annak tanúsítására, hogy a személyes adatok feldolgozása megfelel e rendeletnek, (különösen az adatkezelő és az adatfeldolgozó kötelezettségeire és az érintettek jogaira vonatkozó szabályoknak). A tanúsításnak önkéntesnek, megfizethetőnek, valamint hozzáférhetőnek kell lennie.[54]

Ezek a rendelkezések tehát kötelezik a tagállami hatóságokat arra, hogy audit-szolgáltatást nyújtsanak az adatkezelők számára, ráadásul rögtön „versenyhelyzetbe" is hozva őket, mivel az adatkezelők bármely tagállam hatóságához fordulhatnak (ennek legfeljebb a nyelvi korlátok szabhatnak határt egyes adatkezelőknél).

A versenyhelyzetet enyhítendő a tervezet együttműködést és az eljárási díjak harmonizálását írja elő,[55] ami ugyanakkor egyes kevésbé fejlett EU tagállamokban akár irreálisan magas díjakat is eredményezhet. Mindegyik tagállami hatóság azonos feltételek teljesítését tanusító, egységesen „európai adatvédelmi címke" elnevezésű tanúsítványt és címkét bocsát ki. A tanúsítvány addig érvényes, amíg a tanúsított adatkezelő vagy adatfeldolgozó adatfeldolgozási műveletei maradéktalanul megfelelnek a rendeletnek, legfeljebb azonban öt évig. Az érvényes és érvénytelen tanúsítványok nyilvános elektronikus nyilvántartásban bárki számára hozzáférhetőek.[56]

A rendelettervet gondol a hatósági kapacitások szűkösségére is, ezért lehetővé teszi számukra, hogy harmadik félként eljáró, akkreditált ellenőröket (lényegében piaci szereplőket) vegyen igénybe az auditálás során. A rendelettervezet előír néhány általános jellegű minimumfeltételt, miszerint e szereplőknek megfelelő képzettséggel kell rendelkezniük és pártatlannak (összeférhetetlenségtől mentesnek) kell lenniük. A piaci szereplők közreműködése mellett a „végleges tanúsítást" és a tanúsítvány kibocsátását a hatóság végzi el.[57]

Végül az új szövegváltozat is felhatalmazást ad a Bizottságnak további jogi aktusok elfogadására, valamint az Európai Adatvédelmi Testületnek arra, hogy valamely műszaki szabvány rendelettel való összhangját megállapítsa.[58]

Meg kell jegyezni, hogy a tervezett Rendelet elfogadása a Európai Parlament márciusi döntése ellenére igen lassan halad, és jelentős módosítások várhatóak, ugyanakkor a változások iránya egyértelmű: az új európai adatvédelmi szabályozási keretek között az adatvédelmi auditnak és tanúsításnak a korábbinál lényegesen nagyobb szerepe lehet. A jelenlegi szövegtervezet egy sajátos, a hatósági tanúsítási modell és a piaci szereplők által végzett tanúsítási modell között „félúton" elhelyezkedő, hibrid megoldásra tesz javaslatot. Ennek értékelésére a magyar szabályozás elemzése kapcsán kitérünk.

3.2.2. Kitekintés egyes tagállami szabályozásokra

Az adatvédelmi hatóság által végzett adatvédelmi auditálás nem példanélküli Európában. Az Egyesült Királyságban az információs biztos végez auditálási tevékenységet, amelyet – hasonlóan a LIBE javaslathoz – külső szakember bevonásával is gyakorolhatja. A biztos az adatkezelő hozzájárulásával a helyes adatvédelmi gyakorlat érvényesülését értékeli. Az angol adatvédelmi törvény szerint a személyes adatok kezelése során helyesnek tekinthető az a gyakorlat, amely a biztos szerint kívánatos az adatalany és mások érdekeire tekintettel, és megfelel az adatvédelmi törvény követelményeinek.[59] A biztos e jog gyakorlásához kidolgozta és 2001-ben kiadta az adatvédelmi audit módszertani kézikönyvét,[60] amelyet 2012-ben egy új iránymutatás (guide)[61] váltott.[62] Az auditálás célja a törvényi előírásoknak és a szervezet saját adatvédelmi rendszerének való megfelelés vizsgálata, a hiányosságok és gyengeségek feltárása, valamint információ szolgáltatása az adatvédelmi rendszer felülvizsgálatához. A saját adatvédelmi rendszer a törvényi előírásoknál szigorúbb követelményeket is megfogalmazhat. Az önkéntes auditálás végeredménye az adatkezelő, illetve a biztos tájékoztatása, iránymutatás kibocsátása az adatkezelési gyakorlat előmozdítása végett, szankció alkalmazására természetesen nem kerül sor.[63]

Emellett pl. Németországban Schleswig-Holstein tartomány adatvédelem hatósága is végez adatvédelmi auditálást az ebben önként résztvevő közjogi adatkezelőre vonatkozóan. Az eljárás célja annak vizsgálata, hogy az adatkezelő által önként meghatározott adatvédelmi célkitűzések az azokhoz rendelt intézkedésekkel megvalósíthatók-e. Az eljárás eredményeként a hatóság tanúsítványt bocsát ki, amely az állampolgár számára garancia arra vonatkozóan, hogy az adott közigazgatási szerv tudatos adatvédelmi tevékenységet végez.[64] Ez az eljárás összességében határozottan elválik az adatkezelés jogszerűségének hatósági ellenőrzésétől, alapvető célja a szervezeten belüli adatvédelmi tevékenység tudatosságának növelése, valamint az adatvédelemnek a törvényi garanciákat meghaladó színvonalú biztosítása.[65]

A LIBE javaslat 39. cikke szerint bármely adatkezelő vagy adatfeldolgozó ésszerű, az adminisztratív költségeket figyelembe vevő díj ellenében bármely uniós felügyelő hatóságot felkérheti annak tanúsítására, hogy a személyes adatok feldolgozása megfelel e rendeletnek. Ezek a rendelkezések tehát kötelezik a tagállami hatóságokat arra, hogy audit-szolgáltatást nyújtsanak az adatkezelők számára, ráadásul rögtön „versenyhelyzetbe" is hozva őket, mivel az adatkezelők bármely tagállam hatóságához fordulhatnak.

3.2.3. Az adatvédelmi audit szabályozása Magyarországon

A hazai adatvédelmi szakirodalomnak is évek óta tárgya az adatvédelmi auditálás intézményének bevezetése.[66] Az új adatvédelmi törvény egyik jelentős újdonsága, hogy rendelkezik e jogintézményről. Az auditálásra vonatkozó szakaszok az Infotv. első hatálybalépését követő egy évvel, 2013. január 1-jén léptek hatályba – időt adva a NAIH számára a felkészülésre. A törvényi szabályozás összességében igen szűkszavú, az audit céljainak, módszerének, eljárásának részletes meghatározását az adatvédelmi hatóságra

hagyja. Ennek megfelelően 2013 legelején a Hatóság közzétette az adatvédelmi audit szolgáltatásával kapcsolatos szempontrendszerét,[67] amely a törvényszöveg által okozott bizonytalanságok egy részét rendezi. Az alábbiakban a jogszabályi környezetet és ezzel összhangban a hatóság által kibocsátott szempontrendszert együttesen elemezzük.

Az Infotv. szerint az adatvédelmi audit az adatvédelmi hatóság által, az adatkezelő kérelmére nyújtott szolgáltatás, amelynek célja a végzett vagy tervezett adatkezelési műveleteknek a hatóság által meghatározott és közzétett szakmai szempontok szerinti értékelésén keresztül a magas szintű adatvédelem és adatbiztonság megvalósítása.[68] A törvény egyértelművé teszi, hogy az auditálást a hatóság nem közigazgatási hatáskörben, hanem szolgáltatásként végzi, annak eredménye tehát nem lehet közigazgatási határozat. Az audit szempontrendszer kimondja, hogy a Hatóság az adatvédelmi audit keretében „csak" külső alkalmassági auditot végez, azaz az audit célja az adatkezelő adatvédelmi dokumentációjának a törvényhez mérése, és nem az adatkezelés tényleges gyakorlatának feltárása (megfelelőségi audit).[69]

Az audit, mint szolgáltatásnyújtás jelenlegi szabályozása azt is jelenti, hogy az adatkezelő oldalán nem keletkezik olyan jog, amely alapján egy adatkezelő valamely adatkezelését a Hatóság köteles adatvédelmi audit alá vonni[70] (szemben a LIBE javaslat szövegtervezetével, amely az adatkezelők jogává tenné, hogy adatvédelmi tanúsítványt kérjenek valamely tagállami hatóságtól).

A hatóság az audit eredményét az auditról készített értékelésben rögzíti, amelyben javaslatokat fogalmazhat meg az adatkezelő számára.[71] Az értékelés tehát sem az adatkezelőre, sem a hatóságra nézve nem kötelező. Önmagában az értékelésben foglaltak nem teljesítése jogkövetkezményt nem von maga után, de a javaslatok megvalósítása a jogszerű működésnek sem garanciája. A törvény nem rendelkezik arról, hogy az adatvédelmi hatóság ad-e ki olyan tanúsítványt, amely szerint az adatkezelő, illetve az adott adatkezelés jogszerű. A Hatóság audit szempontrendszere erről szintén hallgat, de részletezi az értékelés elkészítésének menetét,[72] így összességében egyértelművé válik, hogy tanúsításra (tanúsítvány kiadására) nem kerül sor.

A hatóság az audit eredményét az auditról készített értékelésben rögzíti, amelyben javaslatokat fogalmazhat meg az adatkezelő számára. A törvény nem rendelkezik arról, hogy az adatvédelmi hatóság ad-e ki olyan tanúsítványt, amely szerint az adatkezelő, illetve az adott adatkezelés jogszerű. A Hatóság audit szempontrendszere alapján azonban egyértelművé válik, hogy tanúsításra (tanúsítvány kiadására) nem kerül sor.

A törvényszöveg alapján nem lenne világos, hogy az auditálás során figyelembe vett értékelési szempontok mennyiben haladhatják meg a törvényi követelményeket.[73] E tekintetben az audit szempontrendszer közvetve eligazítást ad: a Hatóság csak alkalmassági auditot végez, így a belső szabályzatokat „méri" az Infotv. rendelkezéseihez – a törvényi előírásnál magasabb mércét viszont éppen a belső szabályzatok írhatnának elő, az ezeknek való megfelelés pedig csak megfelelőségi audit keretében lenne mérhető.

A hatósági audit szabályozásával kapcsolatban a legérzékenyebb kérdés az audit és más hatósági eljárások viszonya. Felmerül például a kérdés, hogy mi történik akkor, ha az adatvédelmi audit során a Hatóság jogellenes adatkezelést tár fel, illetve az, hogy miként biztosítható a különböző típusú eljárások egymástól való elválasztása.

A törvény kifejezetten rögzíti, hogy az adatvédelmi audit a hatóság egyéb hatásköreinek gyakorlását nem korlátozza. Így elvi szinten az sem kizárt, hogy az auditról készített értékelés nincs összhangban egy későbbi közigazgatási határozattal. A Hatóság audit módszertana igyekszik e kérdést rendezni, és kifejti, hogy az „auditra az adatkezelő számára nyújtott segítségként érdemes tekinteni", és „az a célja, hogy elősegítse az adatkezelő számára az adatvédelmi előírásoknak történő minél teljesebb megfelelést",[74] és a Hatóság az auditot nem bírságolást elősegítő eszköznek, hanem „figyelemfelkeltő, tudatosságot erősítő, mediáló" eszköznek tekinti. Amennyiben az adatvédelmi audit során jogellenes adatkezelésre derül fény a Hatóság a végleges értékelés kibocsátása előtt megfelelő határidő tűzésével felszólítja az adatkezelőt a jogellenesség orvoslására. Ugyanakkor, ha az adatkezelő ennek nem tesz eleget, akkor a Hatóság fenntartja a jogot arra, hogy az audit keretein kívüli eszközzel kényszerítse ki a jogellenesség megszüntetését. Emellett ha a Hatóság az adatvédelmi audit keretében bűncselekményt észlel, vagy olyan információkat talál, amelyek alapján kötelező az adatvédelmi hatósági eljárást megindítani, akkor a Hatóság az adatkezelő értesítése mellett a szükséges intézkedéseket megteszi. Az audit szempontrendszer rögzíti ugyanakkor, hogy a Hatóság adatvédelmi auditban résztvevő munkatársai az adatkezelővel szemben indított adatvédelmi hatósági eljárásában nem vehetnek részt.[75]

Álláspontunk szerint a különböző eljárások közötti „átjárhatóság" kezelése korántsem megnyugtató, ez a probléma azonban elsősorban a törvényi szabályozásból következik. Jelenleg úgy tűnik, hogy a jogintézmény kockázata éppen az, hogy a hatósági és nem hatósági jogköröket a jogalkotó nem tudta következetesen szétválasztani, és az adatkezelő kénytelen annak kockázatát vállalni, hogy a Hatóság jogellenes adatkezelést tár fel, és ezért végső soron akár bírsággal is sújtja az adatkezelőt. Erre a gyakorlatban viszonylag kicsi az esély, elsősorban azért, mert a Hatóság jelenleg csak alkalmassági auditot végez, azaz az adatkezelő ténylegesen megvalósuló gyakorlatát nem vizsgálja.

Más jogterületeken[76] az auditálást rendszerint nem valamely hatóság végzi, hanem szakmai, gazdasági szervezetek, és legfeljebb e szervezet ellenőrzését, regisztrációját látja el az ágazati hatóság. Az auditálás eredménye általában egy olyan tanúsítvány, amely valamely minőségi követelményrendszernek való megfelelést igazol. A tanúsítvány feltétele lehet bizonyos tevékenység végzésének, de adott esetben kizárólag valamely feltételezett piaci előny kapcsolódik hozzá. Az auditálás intézmények törvénybe foglalása ugyanakkor nem zárja ki a piaci alapon működő adatvédelmi auditálás és tanúsítás lehetőségét, amelynek jelentős előnye lehet például a tanúsító szerv általi felelősségvállalás, amely kiterjedhet – a tanúsítás által meghatározott területen – a tanúsított szerv által esetlegesen okozott kárért, vagy a szervezetet ért adatvédelmi bírságokért való helytállásért is.

A létező európai példák, és a LIBE javaslat „hibrid" megoldása mellett is azt gondoljuk, hogy az adatvédelmi auditálást elsősorban piaci szereplők által szerencsés végezni. Ez esetben mindenképpen biztosítható az auditált vállalkozás adatainak bizalmas kezelése, a hatósági ellenőrzéstől teljes mértékben elkülönült auditálási és tanúsítási folyamat, valamint – a polgári jogi szabályok alapján – egyértelművé tehetők a tanúsítvány kibocsátásával vállalt felelősségi kérdések. Az adatvédelmi auditálás és tanúsítás jól illeszthető a már létező informatikai biztonsági szabványokkal kapcsolatban kialakult gyakorlatba, az ezeknél alkalmazott módszerek nagyrészt az adatvédelmi jogi auditnál is alkalmazhatók. Véleményünk szerint szerencsésebb lett volna a hatályos szabályozás helyett a piaci szereplők által végzett adatvédelmi tanúsítás feltételeit törvényben rögzíteni. Ilyen feltételek lehetnek a tanúsítást végző szervek nyilvántartásba vételi kötelezettsége, az auditorrá válás meghatározott feltételekhez kötése, a felelősségi kérdések szabályozása stb. Ennek hiányában az piaci alapú adatvédelmi audit jelenleg a polgári jog általános szabályai szerint végzett tanácsadási tevékenység keretében folytatható.

Ugyanakkor a jelenlegi magyar törvényi szabályozás az adatkezelők kifejezett kérésére történő hatósági auditról rendelkezik, így megfér egymás mellett a hatóság által végzett és a piaci alapon végzett auditálás intézménye. Az adatkezelők az egyes eljárások előnyeit és hátrányait (ideértve az audit és a hatósági eljárások egymáshoz való viszonyából eredő kockázatot is) egyaránt mérlegelve eldönthetik, hogy számukra melyik auditáló szervezet kívánatos. A hatóság eljárása elsősorban az állami, önkormányzati szervek számára lehet vonzó (egyes külföldi szabályozási minták kizárólag állami szervek számára teszik lehetővé a hatósági által végzett auditálást), amelyeknek üzleti titkaik nincsenek, és forrásaik szűkössége miatt a piaci alapon végzett auditálás nem feltétlenül elérhető számukra.

4. KONKLÚZIÓ

A tanulmányban bemutattuk az önszabályozás (pontosan: társszabályozás) különböző formáit a személyes adatok védelme területén, és részletesen elemeztük ezekhez kapcsolódóan az adatvédelmi audit és tanúsítás elméleti hátterét és a tételes jogban megjelenő szabályait.

Rámutattunk, hogy ezek jelentősége, ideértve különösen az adatkezelők szintjén elfogadott intézkedéseket, a közeljövőben várhatóan nőni fognak. Az új rendelettervezet sorsa ugyan egyelőre bizonytalan, de az adatkezelők elszámoltathatóságát (accountability) erősítő tendencia egyértelmű, és vélhetően akkor is nagy szerepet kap a jövőbeli európai szabályozásban, ha a

jelenlegi szövegtervezetet az európai jogalkotó szervek esetleg jelentősen átdolgozzák.

Meglátásunk szerint ezért az adatvédelem területén olyan új szemléletre van szükség, amellyel az adatkezelők képesek mind a központi jogszabályoknak, mind a különböző önszabályozási formákban foglalt normáknak megfelelni, és az adatkezelők szintjén szükségszerűen megjelenő belső szabályozókat is egységes szemlélettel kezelni.

Ezen új szemlélet lényege, hogy az adatkezelőknek ún. adatvédelmi irányítási rendszer kialakítására kell törekedni. Az adatvédelmi irányítási rendszer e kutatásban nem valamely technikai rendszerre vonatkozó követelményt jelent; fogalma a minőségirányítási- és informatikai biztonsági irányítási rendszerek mintájára adható meg. Az irányítási rendszer (management system) egy rendszer politika és célok megfogalmazásához, valamint célok eléréséhez.[77] A minőségirányítási rendszer (quality management system) irányítási rendszer egy szervezet vezetésére és szabályozására, a minőség szempontjából.[78] Az adatvédelmi irányítási rendszer fogalma ez alapján megalkotható egy szó lecserélésével: irányítási rendszer egy szervezet vezetésére és szabályozására, a személyesadat-védelem szempontjából. Az adatvédelmi irányítási rendszer fogalmilag tehát nem tér el jelentősen a többi irányítási rendszertől, de a területre nem műszaki, hanem jogi követelmények vonatkoznak. A kialakítandó adatvédelmi irányítási rendszer kiépítésének főbb lépései 1) az adott szervezetre vonatkozó kötelező szabályok összegyűjtése; 2) a megfelelő belső dokumentáció elkészítése; és a 3) szervezet tényleges működtetésének dokumentációhoz történő hozzáigazítása.

Jelen tanulmányban e definíciós kísérletnél többre nem vállalkozunk. További kutatások szükségesek ahhoz, hogy az adatvédelmi irányítási rendszer kialakításának korántsem triviális lépéseit, módszertanát kidolgozzuk. Ennek során a már létező adatvédelmi auditálásra vonatkozó módszertanokat, valamint a legújabb külföldi kutatásokban megjelenő, adatvédelmi hatásvizsgálatra (data protection impact assessment) vonatkozó módszertanokat érdemes alapul venni – így, vagy úgy ugyanis mindegyiknek közös célja az adatkezelő által végzett adatkezelések (akár a kockázatok elemzése, akár az adatkezelések értékelése céljából történő) szisztematikus feltárása.

Jegyzetek

1 95/46/EK irányelv a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (95/46/EK irányelv)

2 Ld. erről Bennett, Colin J. – Raab, Charles D.: The Governance of Privacy. Policy Instruments in Global Perspective, 2006, pp. 155–159., Robinson, Neil – Graux, Hans – Botterman, Maarten – Valeri, Lorenzo: Review of the European Data Protection Directive, Rand Corporation, 2009, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf [2012. 10. 18.] pp. 9-10., és Nouwt Sjaak: Towards a Common European Approach to Data Protection: A Critical Analysis of Data Protection Perspectives of the Council of Europe and the European Union, 2010, pp. 284–285. In: Gutwirth, Serge – Poullet, Yves – De Hert, Paul – De Terwangne, Cécile – Nouwt, Sjaak (eds.): Reinventing Data Protection? Springer, pp. 275–292. Az iparági önszabályozási törekvések megbukhatnak az érintettek „adatvédelmi igényeinek" hiányán és ezzel összefüggésben piaci szereplők „üzleti" logikáján, is. Előbbin az adatvédelmi tudatosság növelésével lehetne javítani. Ilten, Carla – Guagnin, Daniel – Hempel, Leon: Privacy Self-regulation Throug Awareness? A Critical Investigation into the Market Structure of the Security Field, 2012, pp. 240–241., 246. In: Gutwirth, Serge – Leenes, Ronald – De Hert, Paul – Poullet, Yves (eds.): European Data Protection: In Good Health? Springer, pp. 233–247.

3 Ruiter, Joep – Warnier, Martijn: Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice, 2011, p. 364. In: Gutwirth, Serge – Poullet, Yves – De Hert, Paul – Leenes, Ronald (eds.): Computers, Privacy and Data Protection: an Element of Choice, Springer, pp. 36–376.

4 Jóri András: Adatvédelmi kézikönyv, Osiris, 2005, p. 53.

5 95/46/EK Irányelv, 27. cikk

6 2009-es adat, ld. Robinson, Neil – Graux, Hans – Botterman, Maarten – Valeri, Lorenzo i. m. p. 9. Egy későbbi másik forrás szerint csak egy elismert magatartási kódex van: a FEDMA-é, ld. Nouwt , Sjaak i. m. p. 284.

7 International Air Transportation Association (IATA)

8 Federation of European Direct and Interactive Marketing (FEDMA)

9 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 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:HU:PDF [2013. 10. 10.], a továbbiakban Rendelettervezet

10 Az angol szöveg „Code of Conduct" kifejezésének sokkal inkább megfelel magyar fordításként a „magatartási kódex" kifejezés így a továbbiakban ezt használjuk.

11 Jelenleg az ún. 29-es munkacsoport elé lehet e kódexek tervezetét terjeszteni, ez a feladat tehát átkerülne a Bizottsághoz.

12 Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs Rapporteur: Jan Philipp Albrecht http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN [2013.12.10.], a továbbiakban LIBE Javaslat

13 Adatvédelmi rendelet tervezete, 38. cikk. (1)–(3) bekezdés.

14 Dumortier, Jos – Goemans, Caroline: Data Privacy and Standardization. Discusssion Paper prepared for the CEN/ISSS Open Seminar on Data Protection, K.U. Leuven, ICRI, 2000, p. 29. https://www.law.kuleuven.be/icri/publications/90CEN-Paper.pdf [2012. 10. 20.]

15 European Committee of Standardization (CEN)

16 Information Society Standardization System (ISSS)

17 Initiative on Privacy Standardization in Europe (IPSE)

18 Initiative on Privacy Standardization in Europe, Final Report CEN/ISSS Secretariat, Brussels, 2002. http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/ipsefinalreportwebversion.pdf [2012. 10. 20.]

19 Privacy Enhancing Technology (PET)

20 A jelentés összefoglalását ld. Jóri András: Az adatvédelmi jog generációi és egy második generációs szabályozás részletes elemzése, PhD thesis, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar Doktori Iskola, 2009, p. 289–295.

21 Winn, J. K.: Technical Standard sas Data Protection Regulation, 2010, pp. 198-199. In.: Gutwirth, Serge – Poullet, Yves – De Hert, Paul – De Terwangne, Cécile – Nouwt, Sjaak (eds.): Reinventing Data Protection? Springer, pp. 191-206., A szabványosítás szerepéről ld. még Bennett, Colin J. – Raab, Charles D. i. m. pp. 159–164.

22 ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework

23 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, 4 May 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 [2014. 02. 20.], p. 134.

24 A szabvány rövid leírását ld: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123 [2014. 02. 20.]

25 Binding Corporate Rules (BCR)

26 Ld. többek között: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (WP133) Working Document setting up a framework for the structure of Binding Corporate Rules Choose translations of the previous link (WP 154), és Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP195)

27 Ld. például Magyarországon az Infotv. 24. §-át, amely szerint belső adatvédelmi felelőst kell kinevezni és adatvédelmi és adatbiztonsági szabályzatot kell elfogadni az országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő adatkezelőnél, a pénzügyi szervezeteknél, és az elektronikus hírközlési és közüzemi szolgáltatóknál; ill. Németországban a BDSG. 4f-4g pontjait a belső adatvédelmi felelősről.

28 Bennett, Colin J. – Raab, Charles D. i. m. pp. 153–154.

29 A teljesség igénye nélkül ilyen kritérium például az, hogy az adatkezelés több, mint 5000 érintettre vonatkozik, az adatkezelés különleges adatot érint, az adatkezelés eredménye joghatással is járó egyéni profilalkotás, az adatkezelés nyilvánosan hozzáférhető területek megfigyelésére szolgál (pl. CCTV rendszer üzemeltetése) stb.

30 Ld. erről részletesen Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése, Infokommunikáció és jog 2013/3. A kötelezettségek elemzése a Bizottság 2012-es szövegtervezetén alapulnak, mivel a kézirat leadásakor a LIBE Javaslat változtatásai még nem voltak elérhetőek).

31 Az MSZ ISO 19011 szabvány definícióját hivatkozza: Berényi, László – Szintay, István – Tóthné Kiss, Anett (2011): Minőségügy alapjai, Miskolci Egyetem, Vezetéstudományi Intézet, http://www.szervez.uni-miskolc.hu/blaci/minmen/index.html [2012. 10. 28.]

32 CEN, CWA 15262-2005 p. 8. Az Egyesült Királyság Információs Biztosa által kiadott kézikönyv lényegében ezzel azonos fogalmat alkalmaz, ld. ICO: Data Protection Audit Manual, UK Information Commissioner's Office, p. 1.4 http://www.privacylaws.com/documents/external/data_protection_complete_audit_guide.pdf [2012. 10. 11.]

33 Ilyen auditbizonyíték lehetnek például a szabályzatok, eljárásrendek, utasítások, tájékoztatók, szerződések adatvédelmi rendelkezései, személyes adatokat érintő panaszok, jegyzőkönyvek, szóbeli interjún alapuló információk stb.

34 A „tevékenység" kifejezést a lehető legtágabban értve ide értjük az adatkezelésre vonatkozó dokumentumok meglétét, a tényleges adatkezelési műveleteket, a rendszer fejlesztésével kapcsolatos terveket, stb.

35 A „tevékenységre irányadó szabályokat" szintén tágan értve ide tartozik minden olyan dokumentum, amely az adatkezeléssel kapcsolatos szabályt állapít meg: törvények és más jogszabályok, policy-k, szabályzatok, szerződési feltételek, stb.

36 Szigeti, Ferenc – Végső, Károly – Kiss, István: Minőségirányítási ismeretek, Nyíregyházi Főiskola, 2003, 6.2. http://mmfk.nyf.hu/min/index.htm [2012. 10. 28.]

37 Balogh, Zsolt György – Jóri, András – Polyák, Gábor: Adatvédelmi „legjobb gyakorlat" kialakítása az elektronikus közigazgatásban, Kézirat, Pécsi Tudományegyetem, Állam és Jogtudományi Kar, Pécs, 2002, p. 390.

38 Az adatvédelmi audit, mint rendszeraudit, és ezzel összefüggésben Roßnagel audit-koncepciójának részletes elemzését ld. Balogh, Zsolt György – Jóri, András – Polyák, Gábor i. m. pp. 334–340.

39 ICO: Data Protection Audit Manual, p. 1.5 Az ICO dokumentuma ezt „First Party Audit"-nak nevezi.

40 ICO: Data Protection Audit Manual, p. 1.5. Az ICO „Second Party Audit" vagy „Supplier Audit" elnevezést használ.

41 ICO: Data Protection Audit Manual, pp. 1.5-1.6. Az ICO „Third Party Audit" elnevezést használ. Az egyes audit-típusok ICO dokumentumon alapuló magyar nyelvű összefoglalását ld. még Balogh, Zsolt György – Jóri, András – Polyák, Gábor i. m. pp. 382–383.

42 ICO: Data Protection Audit Manual, pp. 2.2-2.3., Balogh, Zsolt György – Jóri, András – Polyák, Gábor im. pp. 384–385., NAIH: szakmai szempontok az adatvédelmi audit végzéséhez 2013, http://naih.hu/files/AdatvedelmiAuditSzakmaiSzempontokVegleges.pdf (Továbbiakban: NAIH audit szempontrendszer), p. 4.

43 Bennett, Colin J. – Raab, Charles D. i. m. p. 259.

44 Alexander Roßnagel, koncepcióját és annak Hans-Ludwig Drews *és* Hans Jürgen Kranz általi kritikáját idézi: Balogh, Zsolt György – Jóri, András – Polyák, Gábor i. m. p. 329.

45 A fogyasztói bizalomnak igen nagy jelentősége van olyan speciális területeken, mint például az elektronikus kereskedelem (ideértve a legkülönbözőbb online szolgáltatásokat).

46 Balogh, Zsolt György – Jóri, András – Polyák, Gábor i. m. pp. 330–331.

47 Thomas Königshofen gondolatait idézi Balogh, Zsolt György – Jóri, András – Polyák, Gábor i. m. p. 331.

48 Infotv. 7. § (1), (6)

49 Ld. 2003. évi C. törvény az elektronikus hírközlésről 154. § (4); 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről 13/A. § (3)

50 Polyák, Gábor – Szőke, Gergely László: Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései, In.: Drinóczi, Tímea (ed.): Magyarország új alkotmányossága, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs, pp. 15–177., 2011, p. 175–176.

51 Infotv. 7. § (5)

52 Adatvédelmi rendelet tervezete, 39. cikk. (1) bekezdés

53 Adatvédelmi rendelet tervezete, 39. cikk. (2) bekezdés

54 LIBE javaslat, 39. cikk (1a)–(1b)

55 LIBE javaslat, 39. cikk (1c)

56 LIBE javaslat, 39. cikk (1e)–(1h)

57 LIBE javaslat, 39. cikk (1d)

58 LIBE javaslat, 39. cikk (1i)-(2)

59 Data Protection Act 1998 Art. 51

60 ICO: Data Protection Audit Manual

61 ICO: Auditing data protection. A guide to ICO data protection audits. UK Information Commissioner's Office, 2012 http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/guide_to_ico_data_protection_audits_v2.ashx [2012. 11. 20.]

62 A 2001-ben kiadott Adatvédelmi Audit Kézikönyv formálisan ugyan visszavonásra is került (ld. Morgan/Boardman, 2012, p. 58.), mivel azonban az újabb iránymutatásnál lényegesen részletesebb, fontos, e tanulmányban is többször hivatkozott jogirodalmi forrásként tekintünk rá.

63 Polyák, Gábor – Szőke, Gergely László i. m. p. 175.

64 Polyák, Gábor – Szőke, Gergely László i. m. p. 174.

65 Ld. az Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein honlapját, https://www.datenschutzzentrum.de/index.htm [2012. 10. 25.]

66 Ld. ugyane témát: Polyák, Gábor – Szőke, Gergely László i. m.

67 NAIH: szakmai szempontok az adatvédelmi audit végzéséhez 2013, http://naih.hu/files/AdatvedelmiAuditSzakmaiSzempontokVegleges.pdf (Továbbiakban: NAIH audit szempontrendszer)

68 Infotv. 69. § (1)

69 A megfelelőségi és alkalmassági auditról ld. NAIH, 2013, p. 4.

70 NAIH audit szempontrendszer, p. 11.

71 Infotv. 69. § (4)

72 NAIH audit szempontrendszer, p. 13.

73 A külföldi példák arra mutatnak rá, hogy az adatvédelmi hatóság által végzett auditálás is legalább részben az adatvédelem törvényi előírásait meghaladó, az adatkezelő önkéntes vállalásain alapuló adatvédelmi követelmények teljesítésének minősítésére irányul.

74 NAIH audit szempontrendszer, p. 5.

75 NAIH audit szempontrendszer, p. 16.

76 Ld. például 2009. évi CXXXIII. törvény a megfelelőségértékelő szervezetek tevékenységéről; 2001. évi XXXV. törvény az elektronikus aláírásról

77 MSZ EN ISO 9000:2005 3.2.2. Minőségirányítási rendszerek. Alapok és szótár

78 MSZ EN ISO 9000:2005 3.2.3. Minőségirányítási rendszerek. Alapok és szótár