Ügyszám: 2585/H/2007-1

Állásfoglalás

Az adatvédelmi átvilágításról

I.

Az Európai Unió kísérleti projekt keretében vizsgálja egy európai szintű adatvédelmi címke létrehozásának feltételeit. Ugyan az Európai Bizottság csak 2008 második felében dönt a címkéről, fontosnak tartom az érdeklődő jogi és informatikai szakértők, valamint informatikai termékek gyártóinak, informatikai szolgáltatások nyújtóinak tájékoztatását a kezdeményezésről. A címke odaítélésének feltétele, hogy a címkére pályázó informatikai termékek gyártói vagy a szolgáltatást nyújtók egy önkéntes termék audit eljárásnak vessék alá magukat.

Az EuroPriSe kísérleti projekt célja az Európai Adatvédelmi Címke bevezetése. A címke igazolná, hogy egy informatikai termék vagy egy információ-technológián alapuló szolgáltatás elősegíti az adott terméknek vagy szolgáltatásnak az európai adatvédelmi szabályozással összhangban történő használatát. Az adatvédelmi címke tehát nem azt tanúsítaná, hogy egy termék vagy szolgáltatás konkrét alkalmazása az adatvédelmi jogszabályoknak megfelel, hanem azt, hogy használható a termék vagy szolgáltatás az adatvédelmi jogszabályoknak megfelelően. A kezdeményezésről bővebb információ a http://www.european-privacy-seal.eu/ oldalon található.

Bár a kezdeményezés csak egyes termékeket, szolgáltatásokat érint, annak egy eleme, az adatvédelmi audit szélesebb körben alkalmazható lehet.

II.

Miként korábbi Beszámolóimban olvasható, az utóbbi években nagy mértékben megnőtt a hivatalom által folytatott vizsgálatok száma. A vizsgálatok szerkezetében jelentős változás nem tapasztalható – hozzávetőleg azonos mértékben nőtt a panaszügyek és a konzultációs ügyek száma –, ugyanakkor megfigyelhető, hogy az üzleti szférát érintő ügyekben egyre gyakoribbak a nagyvállalatokkal kapcsolatos panaszok, illetve a tőlük érkező konzultációs beadványok. A beadványok kisebb része tár fel olyan jellegű jogsértést, amely mögött tudatosság ismerhető fel: sokszor inkább az okoz problémát, hogy olyan külföldi mintákat ültetnek át a hazai gyakorlatba, vagy a hatékonyabb működés érdekében olyan módszereket alkalmaznak, melyek a hazai jogi környezettel nem férnek össze. Ezen vizsgálatok azt is mutatják, hogy a legtöbb esetben a kívánt cél elérhető olyan módszerekkel is, melyek nem sértik sem a személyes adatok védelméhez való jogot, sem más személyiségi jogot, ugyanakkor kellő mértékben szolgálják az adatkezelők – többnyire pénzügyi, gazdasági – érdekeit.

Az adatkezelés sohasem önmagában jelenik meg, hanem mindig valamilyen más jogviszonyhoz, eljáráshoz kapcsolódik: ezt fejezi ki a célhoz kötöttség elve, melynek fontosságát nem csak a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban: Avtv.) emeli ki, de az Alkotmánybíróság is többször hangsúlyozta. Egy vállalat esetében az adatvédelem számos területen megjelenik. Mindenhol kiemelten fontos kérdés a munkaerő oly módon történő kiválasztása és „hasznosítása”, hogy az a leginkább megfeleljen a vállalat céljainak és érdekeinek, valamint a hatékonyság mindenhol megjelenő vezérelvének. Fontos terület emellett a vagyonvédelem, az információvédelem, az ügyfélkapcsolatok építése és megtartása. Nem véletlen, hogy az adatvédelmi biztosi intézmény fennállása óta eltelt tizenkét évben folytatott, üzleti szférát érintő vizsgálatok a vállalati tevékenységek szinte teljes spektrumát lefedték.

Nehezíti a jogkövető (vagy jogkövető szándékú) adatkezelő helyzetét az is, hogy míg mára a jogvédelem rendszere kiépült, az érintettek tisztában vannak jogaikkal és a rendelkezésükre álló hatósági, polgári jogi, büntetőjogi jogérvényesítési eszközökkel, addig a jogi környezet egyéb vonatkozásaiban távolról sem optimális. Egyes területeken a szabályozatlanság, máshol a túlszabályozottság okoz nehézséget, sokszor pedig az, hogy a merev jogi környezet nem tud lépést tartani a gazdasági, technikai fejlődés ütemével.

A gyakorlat azt is megmutatta, hogy az adatvédelmet már a tervezés szintjén sem lehet figyelmen kívül hagyni. Számos összetett tevékenység épül adatkezelésre, melynek elégtelensége sikertelenséget eredményezhet, jogellenessége pedig a megvalósítás gátja. Nem megoldás az, ha felmerülő adatvédelmi kérdések akkor kerülnek elő, amikor felépülnek a bonyolult informatikai rendszerek, beindulnak az adatáramlási csatornák. Éppen ezért fontos, hogy az adatkezelés – amely, mint az fentebb olvasható, sohasem önálló, hanem mindig járulékos, valamilyen célt szolgál – jogi szempontból megfelelő legyen.

Ezt észlelték az adatkezelők is, így mára visszatérő jelenség, hogy az adatvédelmi biztostól nem csupán egy-egy kérdésben, hanem átfogó tervek, bonyolult üzleti folyamatok, összetett belső szabályozások kialakításához kérnek véleményt. Az adatvédelmi biztos feladatait azonban az Avtv. kötelező jelleggel határozza meg, és a rendelkezésre álló anyagi és szervezeti források ezt a munkát nem teszik lehetővé. Az adatvédelmi átvilágítás, másképpen – angol eredetű, de mára hazánkban is elterjedt szóhasználattal – az adatvédelmi audit ugyanakkor megoldást jelenthet.

A személyes adatok védelméhez való jog érvényesítése az Alkotmányból fakadó kötelezettség, és bár az Avtv. minden más érdeket mögé helyez (4. §), nem tartható az a szemlélet, amely az adatvédelmet egyedül helyezi középpontba. Ez a fajta megközelítés nem csupán figyelmen kívül hagyja a gazdasági élet sajátosságait, törvényszerűségeit, de konfliktusokat is szül, ezáltal akár azt is eredményezheti, hogy az érintett jogai nagyobb mértékben sérülnek. A hatékony adatvédelem is kívánja a konstruktív megközelítést, azt, hogy ne csupán a személyes adatok védelméhez való jog legyen középpontban, hanem az adatvédelem és az adatkezeléshez fűződő egyéb érdekek összhangban legyenek. E kijelentés helyességét egyértelműen bizonyítják azok a – többnyire gyors, hatékony, és minden érintett fél számára kielégítően záruló – vizsgálatok, konzultációk, melyek során nem csupán a jogellenes adatkezelés megszüntetésére, megakadályozására törekedtünk, hanem az adatkezelőnek segítséget nyújtottunk a céljainak megfelelő, egyúttal jogszerű adatkezelési rend kialakításában.

III.

Az adatvédelmi audit, mint tevékenység széles körben elterjedt, nem csak az Európai Unióban, de azon kívül is. Hangsúlyosabb szerepe ugyanakkor kétségkívül az Unióban van, tekintettel arra, hogy az adatvédelem valamennyi tagállamban kiemelt szerephez jut. Ennek jogi háttere az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK Irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az Irányelv igen szigorú követelményrendszert állít fel, melynek valamennyi tagállam köteles megfelelni, belső jogalkotás útján. Valamennyi tagállam elfogadta a maga adatvédelmi szabályozását, többnyire az Irányelv rendelkezéseivel összhangban, kötelező szabályokat állítva fel mind az állami, mind az üzleti szféra vonatkozásában. Miután az adatvédelem nem csak érvényesíthető joggá, és betartandó kötelezettséggé vált, hanem egyfajta értékké is, melynek a különböző vállalati politikák („Policy”-k) is teret adtak, megjelent az igény a minőségbiztosításra, arra, hogy létre jöjjön egy egységes követelményszint, együtt a megfelelési kritériumokkal, és az azokat érvényesítő önszabályozással. Ez megfelel az Irányelv preambulumának is, mely szerint: *„… a tagállamoknak és a Bizottságnak, saját hatáskörükön belül, ösztönözniük kell az érintett szakmai szövetségeket és más érintett érdekképviseleti szervezeteket arra, hogy etikai szabályzatokat hozzanak létre az irányelv alkalmazásának megkönnyítésére, figyelembe véve az egyes ágazatokban végzett adatfeldolgozás speciális jellemzőit, és tiszteletben tartva az annak végrehajtása érdekében elfogadott nemzeti rendelkezéseket…”.*

Az adatvédelmi audit csak hazánkban kevéssé ismert, más európai országokban kialakult gyakorlata, intézményrendszere van. Egyes államokban – pl. Németország – törvény rendelkezik róla, több helyen az adatvédelmi hatóság tevékeny részvételével valósul meg. Ez megjelenhet abban, hogy az adatvédelmi hatóság módszertant, keretrendszert dolgoz ki, segítséget nyújt a lebonyolításban, az értékelésben. Több országban az adatvédelmi hatóságok kiemelt tevékenysége az adatvédelmi audit, amely egyben jelentős bevételi forrás is.

IV.

Az adatvédelmi audit nem idegen az Avtv. rendelkezéseitől sem. A törvény az adatbiztonság körében előírja, hogy az adatkezelő köteles *„megtenni azokat a technikai és szervezési intézkedéseket,*

kialakítani azokat az eljárási szabályokat”, melyek a szabályozási háttér által támasztott követelményeknek megfelelnek (Avtv. 10. § (1) bek.). Emellett egyes adatkezelők számára kötelezővé teszi a belső adatvédelmi felelős kinevezését – meghatározott feladatkörrel –, továbbá adatvédelmi és adatbiztonsági szabályzat készítését (Avtv. 31/A. §). Egyértelmű, hogy a törvény alapján kötelező szabályzat megalkotását nagyobb adatkezelőknél megelőzi valamilyen felmérés, és a szabályzat egyszerre szolgálja az adatvédelem és az adatkezelő érdekeit.

Bár az adatvédelem minden gazdálkodó szervezetnél szerepet kap, nem mindenhol indokolt az, hogy nagy ráfordítással komplex auditra kerüljön sor. Ez leginkább akkor fontos, ha az adott szervezet tevékenysége döntően valamilyen adatkezelésen alapul, de indokolhatja az auditot az érintettek nagy száma, az adatkezelés mérete is. Az Avtv. 31/A. §-ában meghatározott adatkezelői kör (az üzleti szférában: pénzügyi szervezetek, távközlési és közüzemi szolgáltatók) ebbe a körbe tartoznak. A lefolytatott vizsgálatok, a panaszügyek, és külföldi tapasztalatok alapján meghatározható az a tágabb kör, ahol az audit indokolt lehet.

Elsősorban azon vállalatok tartoznak ide, melyek szolgáltatóként számos érintett (ügyfél) adatát kezelik. Az auditot indokoltabbá teszi az, ha nem csupán az érintettek száma nagy, de a kezelt adatkör is igen széles, esetleg változó. Egyszerűbb a helyzet egy közüzemi szolgáltató esetében, ahol az adatkör viszonylag szűk. Bonyolultabb az adatkezelés – ezt a vizsgálataink is egyértelműen alátámasztják – elektronikus hírközlési szolgáltatók, hitelintézetek, pénzügyi vállalkozások, biztosítók esetében. Itt nehézséget okoz az, hogy az egyes célok eltérő adatkört indokolnak, és az adatkezelő vállalat érdekei ütköznek az érintettek azon törekvésével, hogy minél kevesebb adatot adjanak át. Egyes tevékenységek különösen „érzékeny” adatkezelést eredményeznek, ilyenek például a hitelezési kockázat vizsgálata, a biztosítási kockázat vizsgálata.

A másik fontos adatkezelési terület a munkaviszonyhoz kapcsolódik. Minden évben nagy arányt képviselnek vizsgálataink közt a munkáltatókat érintő panaszok, konzultációk. Itt a fő nehézséget az jelenti, hogy míg a jogi szabályozás meglehetősen hiányos, a munkáltatói érdekek igen változatosak. A különböző kiválasztási módszerek, alkalmassági vizsgálatok, ellenőrzési és minősítési rendszerek, adatfeldolgozási mechanizmusok bonyolult adatkezelést eredményeznek, melyekhez hozzáadódnak a jogszabályok által részletesen szabályozott adminisztratív adatkezelések. Ezen a területen további nehézséget okoz az, hogy a munkáltatói és munkavállalói érdekek sokszor ütköznek, és a jogviszony alanyai között csak formális a mellérendelt viszony, a munkavállaló valójában egzisztenciálisan kiszolgáltatott. A vállalatcsoportok esetében az egységes munkaerő-gazdálkodás is számos kérdést felvet.

A harmadik fontos terület egyes marketing tevékenységekhez kapcsolódik. Napjainkra a hagyományos postai úton bonyolódó direkt marketing háttérbe szorult, helyette a telemarketing, az e-mail marketing jut fontos szerephez, az Internet terjedése pedig újabb módszerek kialakulását eredményezi – elegendő itt a személyre szabott hirdetésekre gondolni. A marketing célú adatkezelések sajátossága, hogy nincs közvetlen kapcsolat az érintett és az adatkezelő között, az utóbbi sokszor az érintett tudta nélkül jut az adatokhoz.

Más jellegű adatvédelmi auditot indokol az, ha az adatkezelő tevékenységéből adódóan az információk biztonságának, a hálózatvédelemnek, a „technikai” adatbiztonságnak tulajdonít jelentőséget. Általában elmondható, hogy az Avtv. 10. §-ából eredő, a személyes adatok biztonságával kapcsolatos kötelezettség nagyobb részben technikai jellegű. Az adatbiztonságra, informatikai biztonságra vonatkozó egyes normák változatos képet mutatnak mind a lefedett területek, mind a szabályozás hierarchiája tekintetében. A jogi szabályozás mellett nagy szerephez jutnak az egyes ajánlások és úgynevezett „legjobb gyakorlatok”, melyek gyakran egymással versengve igyekeznek mérvadó előírásokat megfogalmazni az informatikai rendszerek biztonságával és védelmével kapcsolatban. Az informatikai biztonság emellett túlnő a személyes adatok védelmén, hiszen ebbe a körbe beletartozik például az általános hálózatbiztonság, az informatikai eszközök működtetése.

V.

Az adatvédelmi audit célja kettős: egyaránt irányulhat a jogszabályoknak való megfelelés, illetve az adatbiztonság technikai követelményeinek való megfelelés biztosítására.

Az adatbiztonság, informatikai biztonság az Avtv. alapján is követelmény, és az érintetteknek is vitathatatlan érdeke fűződik hozzá – nem csupán azért, hogy illetéktelenek ne szerezzenek tudomást az adatokról, komoly jog- és érdeksérelemmel járhat az adatok megsemmisülése, károsodása is. Az adatkezelőknek jelentős érdekük fűződik az informatikai biztonsághoz, részben az üzleti titkok védelme miatt, másrészt azért, mert a biztonságos adatkezelés az alaptevékenységükhöz is elengedhetetlen. Mindezek okán az adatkezelő – főként gazdasági – érdekei és az érintettek érdekei, valamint az adatvédelmi követelmények sokszor egybeesnek, és az adatkezelők saját elhatározásukból is törekednek a lehető legnagyobb informatikai biztonság kialakítására, és az adatbiztonság egyéb elemeinek érvényre juttatására. Az adatbiztonság elsősorban technikai kérdés, vizsgálata, elemzése különleges szaktudást igényel, amely egy gyorsan fejlődő tudományhoz kapcsolódik. Az alkalmazott módszerek is sokfélék lehetnek, a „piacon" ugyanakkor számos szolgáltatás igénybe vehető e cél érdekében.

A jogszabályoknak való megfelelés vizsgálata a legtöbb esetben célok és érdekek vizsgálatát, elemzését is magában foglalja. Az adatkezelés, mint arról már volt szó, nem öncél, hanem más célokat szolgál, és ezek a célok az adatkezelő alaptevékenységével függnek össze. Ezen célok mögött végső soron gazdasági érdekek húzódnak, melyek teljes körű érvényesítése, illetve az erre való törekvés okozza az érintettek jogainak és érdekeinek sérelmét. Az adatvédelmi átvilágítás célja a jogkövetés kötelezettségének és az érdekek érvényesítésének összhangjára irányul: végső soron egy olyan adatkezelési rend kialakítására, amely tiszteletben tartja az érintettek jogait, megfelel a jogszabályoknak, és kellő alapot biztosít az adatkezelő tevékenységének, érdekei érvényesítésének. Nem utolsó sorban fontos szempont, hogy a kialakított adatkezelés áttekinthető, adott esetben rugalmas is legyen.

Összefoglalva a fentieket: az eredményes audit bizonyosságot teremt azzal kapcsolatban, hogy az adatkezelés megfelel a személyes adatok védelmét biztosító jogszabályoknak, egyéb normáknak, és biztosítja a jövőre nézve is az adatkezelő tevékenységének hatékonysága és az adatvédelem, adatbiztonság közötti összhangot.

VI.

Az adatvédelmi audit menetére jelen állásfoglalás nem próbál egységes módszertant adni. Az auditnak különböző módjai léteznek, melyek többnyire részletesen kidolgozott elméleti alapokon és gyakorlati tapasztalatokon nyugszanak. Iránymutatásul szolgálhat az Európai Unió Szabványosítási Bizottsága (European Committee for Standardization, Comité Européen de Normalisation – CEN) által kiadott adatvédelmi audit keretrendszer (Personal Data Protection Audit Framework (EU Directive EC 95/46), CWA 15499-1:2006). Általánosságban felvázolható egy audit menete, és meghatározhatóak az adatbiztonság kapcsán vizsgálandó főbb területek.

1. Az audit céljának meghatározása:

Az audit egyik célja annak biztosítása, hogy az adatkezelés a jogszabályoknak megfeleljen, a cél meghatározása azonban ennél bonyolultabb. Ebben a szakaszban kell pontosan körülírni az adatkezelő azon tevékenységét, amelyhez szükséges az adatok kezelése, azon jogviszonyokat, melyekhez adatkezelés kapcsolódik. Elkerülhetetlen azon érdekek nevesítése, melyeket érvényesíteni kell. Ennek tükrében határozható meg az audit általános célja: olyan adatkezelési rend kialakítása, amely a jogok gyakorlását, a kötelezettségek teljesítését, az egyes – akár egymással szemben álló – érdekeket egyaránt szolgálja. Ebben a szakaszban kell meghatározni az audit irányát, mélységét, azt, hogy csak egyes adatkezelésekre, vagy a teljes adatkezelési rendszerre irányuljon; a meglévő adatkezelések jogszerűségének biztosítása legyen a középpontban, vagy egy, a jövőbeni céloknak is megfelelő rendszer kialakítása.

2. Az auditot lefolytató személy kiválasztása:

Az audit lehet belső és külső. A belső audit mellett szól egyszerűsége és olcsósága, kérdéses azonban az, hogy a szükséges szaktudás és tapasztalat rendelkezésre áll-e. A belső audit ellen szól az is, hogy az auditot lebonyolító személy (vagy szervezeti egység) munkáját nehezítik a szervezeten belüli függőségi viszonyok, és eredményét megkérdőjelezheti az, hogy az auditot végzőnek milyen érdekei fűződnek az eredményhez. A külső auditot független személy végzi, akinek munkáját

függőségi viszonyok nem befolyásolják, a végeredményhez pedig nem fűződik érdeke. A külső audit esetén ugyanakkor kiemelt figyelmet kell fordítani a megfelelő személy kiválasztására.

3. Az audit módszerének kiválasztása:

Miként az fent olvasható, az auditnak többféle módszere lehet. Elterjedt a „kérdőíves" módszer, de fontos lehet az alkalmazott eljárások, technológiák, belső szabályzatok áttekintése is.

4. A vizsgált területek, kérdések részletes áttekintése:

Meg kell határozni a szervezet által kezelt adatok közül a személyes adatok körét, fel kell mérni az adatkezelések mögött álló célt. Vizsgálni kell a megfelelő jogalap létét, az érintettek jogainak érvényesülését, az erre vonatkozó eljárások szabályozottságát. A technikai-informatikai biztonság körében vizsgálni kell személyi, eljárási és technikai feltételeket. Ki kell térni arra a kérdésre, hogy az adatkezelő miképpen szabályozza a szervezeti és működési szabályzat, valamint a belső utasítások szintjén az adatbiztonság személyi, szervezeti és technikai követelményeit. Nem elhanyagolható szempont az sem, hogy a biztonságra törekvés jegyében bevezetett intézkedések hogyan hatnak az érintettek – pl. munkavállalók, ügyfelek – jogaira.

5. Az audit eredménye:

A „végeredmény" nagymértékben függ attól, hogy mi volt az audit célja. Ennek tükrében az eredmény lehet egy jelentés, amely a visszásságokat feltárja, és javaslatot ad azok kiküszöbölésére. Összetettebb audit végeredménye egy átfogó adatvédelmi, adatkezelési szabályzat, amely a meglévő szervezeti és tevékenységi struktúrához, esetleg a jövőbeni célokhoz igazodva határozza meg az adatkezelés kereteit.

6. Nyomon követés

Az eredményes audit többnyire adott időponthoz kötődik, ehhez képest akár a jogszabályi környezet, akár az adatkezelés mögötti érdekek változhatnak. Ennek következtében elengedhetetlen a tényleges adatkezelések, a célok, illetve az esetlegesen megalkotott szabályzatok felülvizsgálata bizonyos időközönként.

Ez a folyamat azonban inkább tekinthető vázlatnak, mintsem egy audit forgatókönyvének. Ennek elsődleges oka az, hogy a keretrendszer kiindulópontja az általános európai gyakorlat, ugyanakkor a hazai adatvédelmi szabályozás speciálisnak tekinthető: az adatvédelmi törvény szigorúbb, mint a az Európai Unió többi tagállamának hasonló jogszabálya. Ez az egyes területeket szabályozó, úgynevezett szektorális jogalkotásra, illetve a gyakorlatra is rányomja bélyegét. Ilyenformán egy hazai auditor szűkebb keretek között mozog, egyszersmind nehezebb is a feladata, mint külföldi kollégájának.

A másik fontos tényező, amelynek okán a fenti vázlat csak nagyvonalú iránymutatás: minden adatkezelés különbözik. Ennek okán a keretrendszer nem helyettesítheti az adatvédelemben jártas szakember közreműködését.

VII.

Míg külföldön, elsősorban Nyugat-Európában az adatvédelmi auditnak kialakult intézményei vannak – auditot végeznek szolgáltatásként gazdálkodó szervezetek, tanácsadó vállalkozások, illetve adatvédelmi hatóságok akár törvény alapján, esetleg díj ellenében, akár üzleti alapon –, hazánkban ez hiányzik. Az informatikai biztonság vizsgálatával számos vállalkozás foglalkozik, többnyire csak technikai szempontból, vagyis egyfajta szemléletváltás szükséges. A jogi, szervezeti oldalról „közelítő" audit lefolytatására azonban nehezebb megfelelő személyt találni. Egyes tanácsadással foglalkozó vállalkozások már felismerték a kérdés fontosságát, így tevékenységi körük része az adatvédelmi szempontú átvilágítás és tanácsadás. Emellett – az adatkezelésekre vonatkozó szabályozás bonyolulttá válása és a hatékony jogérvényesítés intézményrendszerének kialakulása következtében – egyre több ügyvéd szakosodott kisebb-nagyobb mértékben adatvédelemmel kapcsolatos ügyekre.

Valódi megoldást azonban a inkább a jövőben várható. Egyre gyakoribbak az olyan konferenciák, továbbképzések, melyeken nem csupán egy-egy előadás terjedelemben kap teret az adatvédelem, hanem teljes egészében e területtel foglalkoznak – erre igény van, amit neves képzés-szervező, konferenciaszervező cégek kínálata is mutat. Egyes felsőoktatási intézményekben – különösen a jogi, gazdasági, illetve számítástechnikai irányokon – is megjelent az adatvédelem, több helyen nem csupán egy nagyobb tananyag részeként, hanem választható, esetleg kötelező kurzusként. Amennyiben a piac igényli, kétségtelen, hogy az oktatás „kitermeli" a megfelelően felkészült szakembereket.

VIII.

Nem vonható kétségbe az, hogy a leghatékonyabb jogvédelem az adatvédelem területén sem az egysíkú, szigorú szemléletben, hanem valamennyi jogos, méltányolható érdeket figyelembe vevő megközelítés útján biztosítható. Az állampolgárok érdekeit is jobban szolgálja az, ha adataik kezelésre – akár munkaviszonyban, akár ügyfélkapcsolatban – egy kellően megalapozott, jogszabályoknak megfelelő rendszerben kerül sor, és nem utólag okoz nehézséget jogaik érvényesítése. Az adatvédelmi audit iránt az igény megfigyelhető, elegendő az Adatvédelmi Biztos Irodájához érkező kéréseket tekinteni. Ezen kérések teljesítését azonban a törvényi háttér, illetve az intézményi struktúra nem teszi lehetővé. Nem feltétlenül kell ugyanakkor kizárni annak lehetőségét, hogy az adatvédelmi biztos az auditálással foglalkozók módszertanát átvizsgálja, arról általánosságban véleményt mondjon; esetleg – akár egy nyilvános „szaknévsor" publikálásával – közreműködjön abban, hogy a szolgáltatók és a szolgáltatást igénybe vevők közötti kapcsolatfelvétel megvalósulhasson.

Budapest, 2007. december 11.

Dr. Péterfalvi Attila