AZ ELEKTRONIKUS SZEMÉLYAZONOSÍTÁS ADATVÉDELMI KÖVETELMÉNYEI

Készítette az

a Nemzeti Fejlesztési Ügynökség megrendelésére
2007-ben

Szerzők:

dr. Majtényi László, jogász, az Eötvös Károly Közpolitikai Intézet elnöke, a Magyar Köztársaság első adatvédelmi biztosa, a Pécsi Tudományegyetem docense

dr. Simon Éva, jogász, adatvédelmi szakértő, a Magyarországi Tartalomszolgáltatók Egyesületének munkatársa

dr. Székely Iván, társadalmi informatikus, adatvédelmi szakértő, a Nyílt Társadalom Archívum főtanácsadója, a Budapesti Műszaki Egyetem docense

dr. Szabó Máté Dániel, jogász, adatvédelmi szakértő, az Eötvös Károly Közpolitikai Intézet munkatársa

Tartalomjegyzék

Bevezető

Ez a tanulmány a Nemzeti Fejlesztési Ügynökség megbízásából, az Eötvös Károly Közpolitikai Intézet vezetésével, az Intézet munkatársai és külső szakértők közreműködésével készült, 2007. júliusa és szeptembere közötti időszakban. Célja, hogy adatvédelmi szempontból értékelje a közigazgatás informatizálásával kapcsolatos terveket, koncepciókat, megvalósítási tanulmányokat, kiemelten az elektronikus ügyfélazonosítás modelljeit és az ehhez a problémakörhöz kapcsolódó személyesadat-kezelési megoldásokat. Célja továbbá, hogy felmérje az egyes koncepciók, tervek adatvédelmi kockázatát, valamint hogy megoldási javaslatokat fogalmazzon meg az adatvédelmi problémák kiküszöbölésére. Ezen túlmenően a tanulmány törekszik arra is, hogy általános szempontrendszert nyújtson a döntéshozóknak és a fejlesztőknek egyaránt, amelynek segítségével az elektronikus kormányzati szolgáltatások újabb koncepcióinak kialakítása során már a tervezés fázisában érvényesíteni tudják az adatvédelmi elveket, az alkotmányos követelményeket és a vonatkozó jogszabályi rendelkezéseket.

Elemzésünkben elsősorban a Megbízó által összeállított feladat-meghatározásban feltett kérdésekre kívántunk választ adni, de figyelembe vettük a Megbízó által átadott írásos háttéranyagokat is, köztük az e-Közigazgatás 2010 Stratégia, és az e-Közigazgatás 2010 Programterv című kormányzati dokumentumokat, az MTA Információtechnológiai Alapítvány által 2007. júniusában készített „Elektronikus azonosító bevezetése: elvárások és igények, következtetések és javaslatok" című tanulmányt, valamint a KOPINT-DATORG Infokommunikációs zRt. „Közigazgatási Informatikai Közmű – Elektronikus azonosító rendszer bevezetése" című megvalósítási tanulmányát. Figyelembe vettük a Megbízó által a szakértői vizsgálatunk lefolytatásának időszakában átadott írásos részanyagait, az abban felvetett problémákat, megoldandó kérdéseket, valamint a Megbízóval folytatott rendszeres konzultációk során felvetetett kérdéseket egyaránt. Végül, általánosságban támaszkodtunk a különféle, az e-közigazgatás fejlesztési elképzeléseivel foglalkozó szakmai fórumokon elhangzottakra, háttéranyagokra is.

Szakértői vizsgálatunk bizonyos értelemben mozgó célpontra irányult: már a tanulmány elkészítésének időszakában is megváltoztak az eredeti kérdésfeltevések súlypontjai, változtak a döntéshozói prioritások, illetőleg változtak az e-közigazgatást érintő fejlesztési tervek

szereplőinek pozíciói, preferenciái, érdekviszonyai. Figyelemmel a változó prioritásokra és aktualitásokra, arra törekedtünk álláspontunk megfogalmazásában, hogy azok a pillanatnyi helyzettől függetlenül, egy más kontextusban is választ tudjanak adni a felvetett adatvédelmi problémákra, illetve hogy felhívjuk a figyelmet olyan adatvédelmi aspektusokra, amelyek egyáltalán nem szerepeltek az általunk megismert anyagokban. Emellett egyes kiemelt fontosságú, az elektronikus személyazonosítás problémáit érintő koncepciókat, illetve megoldási javaslatokat külön-külön is értékeltünk adatvédelmi szempontból.

Megközelítésünk interdiszciplináris szemléletű, amelyben kiemelt súllyal szerepelnek adatvédelmi jogi megfontolások, emellett azonban közigazgatás-elméleti, rendszerszervezési, társadalmi és informatikai aspektusokat is figyelembe vettünk szakértői állásfoglalásunk megfogalmazásában. Kifejezett törekvésünk, hogy ne csupán az adatvédelmi problémák katalógusát nyújtsuk e tanulmányban, ne csupán a vizsgált koncepciók megvalósíthatóságának adatvédelmi korlátait soroljuk fel, hanem a gyakorlatban alkalmazható konkrét megoldásokat javasoljunk a közigazgatási hatékonyság, a kormányzati célok, az informatikusi szemléletmód és a fejlesztők szakmai és üzleti érdekeinek szempontjait egyaránt figyelembe vevő, egyúttal adatvédelmileg korrekt adatkezelési rendszerek kifejlesztésére és jövőbeli üzemeltetésére. Törekvésünk az is, hogy az adatvédelmi szempontokat ne csupán az informatikusi és közigazgatási logika korlátozó peremfeltételeként, hanem követendő elvként, pozitív célként jelenítsük meg. Ezért általános javaslatokat is teszünk annak érdekében, hogy elvi iránymutatást adjunk a későbbi fejlesztésekhez, illetve a fejlesztéseket érintő döntésekhez, valamint hogy tervezési szempontokat és módszereket ajánljunk abból a célból, hogy az adatvédelmi szemlélet folyamatosan jelen legyen a magyar közigazgatás működését és polgárainak a hivatalokkal és a magánszektor szolgáltatóival való kapcsolatát hosszú távon befolyásoló rendszerek kialakításánál és üzemeltetésénél.

Vizsgálatunk fókuszában a személyazonosítás, ezen belül az elektronikus ügyfélazonosítás, illetőleg az azonosított vagy azonosítható személyek adatainak az adatkezelők közötti áramlása áll. Hangsúlyoznunk kell azonban, hogy egy azonosító, egy azonosítási mód, avagy egy azonosítási célt (is) szolgáló kártya sem informatikai, sem adatvédelmi szempontból nem tekinthető önálló elemnek, hanem egy adatkezelési rendszer részeként értelmezendő. Ezért több helyütt kitérünk az ügyfélazonosítás, illetve a különböző adatkezelések közötti interoperabilitás vizsgálatánál a tágabb adatkezelési környezet követelményeire is.

Ugyanakkor nem feladata e tanulmánynak, hogy a közigazgatás személyesadat-kezelésének egészét, annak informatikai fejlesztési koncepcióit elemezze és értékelje adatvédelmi szempontból.

Elemzésünk és megállapításaink – a vizsgálat időtartama alatti változások figyelembevételével – egy időpillanatra vonatkoznak. Noha tanulmányunk általános iránymutatást is tartalmaz jövőbeli hasonló személyesadat-kezelési problémák megoldására, mégis hangsúlyoznunk kell, hogy a hosszú távon állandónak tekinthető feltételek mellett elsősorban az információs technológia fejlődése, de a politikai prioritások változásai is alapvetően befolyásolhatják egy-egy elképzelés megvalósításának környezetét, adatvédelmi megfelelőségét. Ezért szükséges az adatkezelési rendszerek tervezésében, üzemeltetésében bekövetkező változások figyelemmel kísérése, adatvédelmi státuszuk követése, rendszeres aktualizálása.

A vizsgálat általános megállapításai

Vizsgálatunk legfontosabb megállapítása, hogy a magyar adatvédelmi szabályozás, illetve az alapjául szolgáló alkotmányos követelményrendszer nem teszi lehetetlenné a közigazgatás elektronikus ügyintézési alapokra helyezését. Az elektronikus személyazonosítás, a távoli ügyintézés és az ügyfelek felesleges közreműködésének csökkentése, amennyiben az indokolt keretek között marad, megvalósítható a jelenlegi alkotmányos keretek között is. Ez azonban nem jelenti azt, hogy az alkotmányos keretek ne jelentenének bizonyos mértékű korlátozást a változtatás számára, bizonyos normákra a reformnak is tekintettel kell lennie. A tanulmányban ezekre igyekszünk felhívni a figyelmet.

A tanulmány felépítése

Szakértői munkánk két, egymásra épülő részből álló tanulmányt eredményezett. Az első részben általános szempontokat kívánunk adni a döntéshozók számára, ennek keretében elsőként bemutatjuk az alkotmányos követelményeket, az ezekkel kapcsolatos joggyakorlatot, és az előző kettő alapján megalkotott jogi rendelkezéseket, amelyekre az egyes elektronikus ügyintézési és személyazonosítási koncepciók megalkotásakor és megvalósításakor álláspontunk szerint tekintettel kell lenni. Ezt követően számba vesszük az azonosító kártyák lehetséges további funkcióit, a magyar szabályozás szemszögéből elemezzük az ezekkel

kapcsolatos ismert külföldi megoldásokat, és általános véleményt mondunk az e körben kialakított egyik koncepcióról, a Közigazgatási Informatikai Közműről. Ezt követően röviden összefoglaljuk azokat az adatvédelmi természetű alapelveket, amelyeket valamennyi elektronikus azonosítási és ügyintézési koncepció tekintetében megfontolásra javasolunk.

A tanulmány második részében az egyes, a Megbízó által a szakértői csoporttal megismertetett koncepciók releváns alkotóelemeit elemezzük az általános elvek és követelmények szemszögéből. Nem az egyes koncepciók mentén haladunk, hanem az egyes koncepciók állandónak tűnő építőelemeiről mondunk adatvédelmi szempontú véleményt. Ennek indoka egyrészt az, hogy az egyes koncepciók részben egymást átfedő elemekből építkeznek, ez pedig indokolatlan ismétlésekhez vezetett volna, másrészt az, hogy maguk a koncepciók is állandóan változónak bizonyultak vizsgálatunk ideje alatt, harmadrészt pedig nem az egyes koncepciókat, hanem azok építőelemeit tartottuk adatvédelmi szempontból relevánsnak és így elemezhetőnek. Mivel az egyes építőelemek végső soron nem önmagukban valósulnak meg, figyelemmel voltunk arra, hogy ezek az elemek tágabb koncepciók részét képezik, ezért elemzésünk során, az egyes javaslatok és követelmények megfogalmazásakor utalunk a többi építőelemmel kapcsolatban megfogalmazott követelményekre. Tanulmányunk ezen része az általános részben megfogalmazott követelményeket fordítja le az egyes építőelemek jellemzőinek megfelelően. Ezt követően a Megbízó által átadott koncepciókban nem érintett kérdésekkel is foglalkozunk, amelyeket a későbbi koncepcióalkotáskor figyelembe veendőnek tartunk: olyan technológiai és szervezési megoldásokat említünk meg, amelyek szándékaink szerint hasznosnak bizonyulnak majd a jövőbeli tervezés során. Végül az adatvédelmi hatásvizsgálat szükségességéről szóló írással zárjuk a tanulmányt, amellyel kapcsolatban hangsúlyozzuk, hogy a Megbízó azzal, hogy már a koncepcióalkotás fázisában kikérte adatvédelmi szakértők véleményét, a legfontosabb lépést megtette az adatvédelmi szempontokat is figyelembe vevő megoldások kialakítása felé.

A Megbízó kérdéseire adott válaszaink

A megbízási szerződés mellékletét képező feladatleírás végén a Megbízó hat önálló kérdést fogalmazott meg. A kérdések mögött rejlő problémákat tanulmányunk különböző helyein részletesen elemezzük, ehelyütt csak röviden válaszoljuk meg őket a részletes magyarázatok mellőzésével, amelyekre e helyütt csupán utalunk.

1. „Elhelyezhető-e a hivatali kártyán tényleges azonosítási célú tanúsítvány is a közigazgatás belső használatára szánva?”

Álláspontunk szerint ennek nincs akadálya, a hivatali kártya birtokosa, a köztisztviselő személyesen jár el a közigazgatási eljárásokban, ennek megfelelően személye nemcsak azonosítható, hanem azonosíthatónak is kell lennie. A hivatali kártyával, annak adattartalmával kapcsolatos további megállapításainkat 2.2.4. pont alatt ismertetjük.

2. a) „Elhelyezhető-e az elektronikus TAJ-kártyán tényleges azonosítási célú tanúsítvány az állampolgár számára?”

Amennyiben ez önkéntesen történik, elhelyezhető. Az elektronikus TAJ kártya további funkciókra történő alkalmassá tételével kapcsolatban azonban itt is fontosnak tartjuk felhívni a figyelmet arra, hogy amennyiben a kártyát e további funkciókkal összefüggésben hivatalokban, bankban, stb. az ügyfélnek át kell adnia, az nem tartalmazhatja sem emberi, sem az adott alkalmazás számára olvasásra alkalmas formában a társadalombiztosítási azonosító jelet, arról csupán a megfelelő olvasó berendezéssel rendelkező társadalombiztosítással kapcsolatos feladatot ellátó szervezetek lehetnek képesek a TAJ-számot megállapítani. Erről bővebben a 2.2.3. pont alatt írunk.

2. b) „Amennyiben az előző kérdésre a válasz igen, úgy alkalmazható-e az ügyfél beleegyezése esetén a PKI alapú azonosítású kulcs a meglévő ügyfélkapus bejelentkezési megoldások megerősítésére a 193/2005. (IX. 22.) Korm. rendelet 9. §-a alapján?”

A kérdésben hivatkozott rendelkezés ma már nincs hatályban, ám ez nem jelenti azt, hogy ahol fokozottabb biztonságra lenne szükség, ne lehetne magasabb biztonsági szintet megvalósító alkalmazást használni. Álláspontunk szerint a PKI alapú azonosítás ilyen, és bizonyos elektronikus ügyintézési célokat nem is lehet ezek nélkül megvalósítani. Az azonosításra használt kulcs mellett azonban szükség lehet aláíró kulcsra és titkosító kulcsra is, attól függően, hogy milyen szolgáltatásokat biztosítanak az állampolgárok számára. Erről szóló részletes megállapításaink a 2.1.1. pont alatt találhatók.

3. „Lekérheti-e egy központi szolgáltatásként kialakított (vagy privát üzemelésben lévő) adattárba adatait az egyes nyilvántartásokból a személy, ahol nyilvános titkosító saját

kulcsával titkosítva tárolódnak az adatok. Ekkor, ha szüksége van valamelyik azonosítójára, azt e nyilvántartásból veheti ki, majd kulcsával oldhatja fel az adott alkalmazásnak átadva (nem kell megjegyeznie semmit).”

A céllal egyetértünk, a saját azonosítóit megjegyezni nem akaró állampolgárnak legyen lehetősége arra, hogy azokat egy központi (vagy inkább egy általa választott piaci szolgáltató által fenntartott) tárban elhelyezze. Azt a megoldást tartjuk azonban jónak, ha az adattárban adatokat kizárólag azok alanya tud elhelyezni és abból kivenni, és nem adhat meghatalmazást másnak (például egy nyilvántartó szervnek) arra, hogy ott adatokat elhelyezzen, illetőleg onnan adatokat letöltsön. Ennek oka, hogy a hozzájárulás önkéntessége nem biztosítható minden esetben. Ennek részletes kifejtését 2.3.2. pontban tárgyaljuk.

4. „Célszerű lenne, ha ugyanazon kártyatestre a rajta található érintkezéses mikroprocesszoron (chipen) kívül még egy független, érintkezés nélküli rádiófrekvenciás chip is elhelyezésre kerülhetne. A két chip között érdemi kapcsolat nincs; az olvasási technológiájuk is más. Megfelelő szervezés mellett egy ilyen ún. duálchipes kártya egyéb funkcióra is egyszerűen felhasználható.”

A több chip garanciát jelent arra nézve, hogy a különböző céllal a kártyára vitt adatokat csak a megfelelő chip olvasására feljogosítottak tudják olvasni. Ez a megoldás tehát jobb, mintha egy chipen helyeznének el a kártya különböző funkcióival összefüggő adatokat. Az érintkezés nélküli olvasást lehetővé tevő chipek azonban egészen más természetű adatvédelmi kockázatokat teremtenek, ezért az ilyen chipek közül a kontrollált aktív RFID chipek használatát tartjuk megfelelőnek. Részletes magyarázatát lásd a 2.2.6. pontban.

5. „Alkalmazhatók lennének-e a bankkártyák a közigazgatásban ügyfélkapus azonosítás megerősítésre úgy, hogy a bank csak viszontazonosítás jelleggel erősíti vagy cáfolja az azonosságot az ügyfélkapu felé?”

E megoldásokat nem támogatjuk. Meghatározott feltételek teljesülése esetén alkalmazhatóak, azonban szigorúan kiegészítő jelleggel. A megoldás adatvédelmi természetű feltételeit a 2.1.3. pontban ismertetjük.

6. „Van-e jogi akadálya a közigazgatásban központi, az azonosítási rendszerre épülő jogosultság-kezelő rendszer kiépítésének?”

Az ügyfelek jogosultságainak központi kezelését a hatályos jogszabályok, elsősorban az osztott információs rendszerek elvének megfelelően nem teszik lehetővé, ellenétben áll a különböző adatkezelések összekapcsolásával és az automatikus egyedi döntéssel kapcsolatos törvényi rendelkezésekkel. A hivatalnokok jogosultságainak központi kezelése az államigazgatáson belül jogi szempontból megvalósítható, ám megítélésünk szerint ez olyan bonyolult és bürokratikus rendszert eredményezne, amely ellentétes lenne az elektronikus kormányzati szolgáltatások fejlesztésének kitűzött céljaival, nehézzé tenné a speciális esetek, alternatív ügyintézési megoldások, kivételek alkalmazását is. E kérdéskörrel az 1.3.3. pontban foglalkozunk.

1. Általános megállapítások

1.1. Az alkotmányos követelmények, a megvalósítás keretei, a védelmi lehetőségek Magyarországon

Az Európai Unióban a személyes adatok védelmére vonatkozóan kialakított minimumkövetelmények tagállami implementálása lényegesen eltér. Az egyes országok politikai, társadalmi, gazdasági, kulturális és intézményi eltérése miatt lényeges különbségek tapasztalhatóak. Éppen ezért, bár a külföldi példák figyelembevétele fontos a projekt kivitelezése szempontjából, a megvalósíthatóságot valójában az egyes tagállamok belső adatvédelmi szabályai határozzák meg. Az alábbiakban ismertetjük a hazai adatvédelmi rendszer alapelveit: az alkotmányban és az adatvédelmi törvényben rögzített legfontosabb szabályokat, vonatkozó Alkotmánybírósági döntéseket és értelmezzük a személyazonosítás szempontjából felmerülő kérdésköröket.

Alkotmány 59. § (1) bekezdés

Az Alkotmány az alapjogok között nevesíti a személyes adatok védelméhez való jogot. Az Alkotmány 59. § (1) bekezdése kimondja, hogy a Magyar Köztársaságban mindenkit megillet a magántitok és a személyes adatok védelméhez való jog. A személyes adatok védelmére vonatkozóan az Országgyűlés megalkotta a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényt (a továbbiakban: Avtv.). Az Avtv. mellett további szektorális szabályok vonatkoznak a személyes adatok védelmére.

a személyes adat fogalma

Személyes adat minden olyan adat, ami természetes személlyel kapcsolatba hozható, és az adatból levonható, a természetes személyre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt - közvetlenül vagy közvetve - név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező

alapján azonosítani lehet. (Avtv. 2. § 1. pont) Az Avtv. definíciójából tehát az következik, hogy a személyes adatok köre igen tág: ide értjük a természetes azonosítókat, mint a név, születési hely és idő, a biometrikus adatokat, mint a DNS, ujjlenyomat, valamint a mesterséges azonosítókat, tehát az olyan alfanumerikus karaktersorokat, amelyek csak egyetlen emberhez tartoznak, ilyen a TAJ szám, az adóazonosító vagy akár egy személyes használatú mobiltelefonszám is. A hagyományos értelemben vett adatokon kívül személyes adat a személyes tulajdonság, a képmás és a vélemény is.

különleges adatok

A személyes adatok körén belül a törvény megkülönböztet egy további speciális adatkört, a különleges adatokat, amelyen belül további adatköröket specifikál. A különleges adat a személyes adat fogalmának erősebben védett alesete, de ezen a kategórián belül is különbözik a védelmi szint. Különleges adat a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat. (Avtv. 2. § 2. pont) Bűnügyi személyes adat a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetőleg a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat. (Avtv. 2. § 3. pont)

bűnügyi személyes adatok

Az európai jogban a személyes adatnak két értelmezése ismert: az abszolút értelmezésben mindaddig személyes adat az információ, ameddig az igénybe vett erőforrásokra tekintet nélkül el lehet attól jutni az adatalanyig. A relatív értelmezés szerint az a személyes adat, amelyet az adott adatkezelő képes megszemélyesíteni, tehát egyetlen személyhez kötni. A magyar törvény szövege, néhány ezzel ellentétes adatvédelmi biztosi állásfoglalás és bírói döntés dacára inkább az abszolút értelmezés talaján áll, **a**mely sokszor abszurd eredményekhez vezet.

A személyes adatok kezelésében is megmutatkozik a különbség a személyes adatok és a különleges adatok között, a törvény szigorúbb feltételeket állít a különleges adatok kezelésének feltételéül. Ennek oka, hogy a különleges adatok olyan információt tartalmaznak az érintettre vonatkozóan, amely a legbensőbb titkaira, személyes meggyőződésére, életvitelére, származására is utalhat, ezért kezelését szigorúbb feltételekhez köti a törvény.

anonimizált és statisztikai adatok

Különbséget kell tenni az azonosítást lehetővé tevő adatok és azon adatok között, melyeket anonim módon dolgoznak fel. A több adatszolgáltatásra kötelezett magánszemély adatainak összesítése (aggregátum) már nem feltétlenül személyes adat. Az anonimizált vagy a statisztikai adatok nem minősülnek személyes adatnak, hiszen azokból nem lehet személyre szabott következtetést levonni. Természetesen elképzelhető olyan aggregátum, ami megőrzi személyes adat jellegét. Statisztikai adatként funkcionáló személyes adatra példa, hogy meghatározott iskola IV. b. osztályában valamennyi gyermek fogyatékkal élő. Ezért az Avtv. kimondja, hogy statisztikai céllal felvett adatok kizárólag statisztikai céllal használhatók fel. (Avtv. 32/A. §)

kódolt információk

Az elektronikus adattovábbítás és az elektronikus úton történő azonosítás során többször felvetjük a kódolt információk garanciaként való használatát. A kódolt információ jelenti mindazt az adatot, amely az adott adatkezelőnél nem értelmezhető. Az, hogy ezek az adatok személyes adatok-e, hosszú ideig vita tárgyát képezte. 2003-ban az adatvédelmi biztos vizsgálata arra a következtetésre jutott, hogy ezek az adatok is személyes adatok. Az állásfoglalás kimondta, hogy „az APEH központjában, a központi TÜK irodában őrzött adatállományokat függetlenül attól, hogy azok csak a megfelelő számítógépes környezetben futtathatók, illetve attól, hogy az őrzésük igen biztonságos, és a hozzáférhetőségük is korlátozott és szabályozott, személyes adatok tárolásának kell tekinteni, amely csak akkor jogszerű, ha megfelel az adatvédelmi törvény, és az Európa Tanács adatvédelmi egyezménye követelményeinek.” (Tájékoztató az Adó- és Pénzügyi Ellenőrzési Hivatal (APEH) és más szervezetek rendkívüli

adatkezelésével (az adatállományok másolásával, továbbításával, tárolásával) kapcsolatos adatvédelmi biztosi vizsgálatról.)

1.1.1. Az adatkezelés alapelvei

információs önrendelkezési jog, informált beleegyezés

A személyes adatok kezelése tekintetében főszabályként az információs önrendelkezési jogot kell mindenkinek tiszteletben tartani. Eszerint a személyes adatok védelme – az elnevezéssel szemben – nem csupán védelmi jog (amely szerint az adatokat védeni kellene a jogosulatlan megismeréstől), hanem annak aktív oldala is megmutatkozik: mindenki maga rendelkezik személyes adataival. Általában bármely módon kinyilvánítható a hozzájárulás az adatkezeléshez, akár ráutaló magatartással is, így például azzal, hogy a kártyatulajdonos a bankkártyát átadja a kereskedőnek. A hozzájárulás feltétele az úgynevezett „informált beleegyezés", ami azt jelenti, hogy a beleegyezésnek önkéntesnek, határozottnak és tájékozottnak kell lennie. Az informált belegyezés minden esetben megfelelő tájékoztatáson kell, hogy alapuljon, tehát az érintettnek ismernie kell az adatkezelés célját, kik kapják meg az adatokat, mennyi ideig kezelik, stb. Az érintett felvilágosítása az adatkezelő feladata. A különleges adatok kezelésénél *írásos* beleegyezést kíván meg a magyar jog. Ez az előírás magyar sajátosság, az Unió ilyen szigorú feltételt nem határoz meg a különleges adatok kezeléséhez.

az alapelv első megfogalmazása

Az információs önrendelkezési jog első jogi dokumentuma a Német Szövetségi Alkotmánybíróság 1983. évi Népszámlálási törvényről hozott 1983. december 15-i határozatában jelent meg (15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83), gazdagítva az adatvédelem jogi érvkészletét. A bíróság az adatvédelem alkotmányos alapját az alaptörvény 2. cikk (1) bekezdéséből vezette le, összefüggésben az 1. cikk (1) bekezdésével. [2. cikk (1) „Mindenkinek joga van arra, hogy saját személyiségét szabadon kibontakoztassa, amennyiben az mások jogait nem sérti és nem ütközik az alkotmányos rendbe, vagy az alkotmányos törvénybe." 1 cikk (1) „ Az emberi méltóság sérthetetlen. Annak tisztelete és védelmezése kötelező

minden állami hatalom számára."] A Szövetségi Alkotmánybíróság álláspontja szerint „Az alapjog biztosítja az egyénnek azt a jogát, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról." E jog a bíróság szerint csak túlnyomó közérdekből, az arányosság követelményét szem előtt tartva korlátozható, olyan óvintézkedések mellett, melyek biztosítják a személyiségi jogok védelmét.

kontroll az adatok felett

Az egyén információs önrendelkezése feltételezi, hogy a modern információs technológiák világában is áttekintéssel bírjon a róla nyilvántartott adatokról. Csak így tud saját döntéseit követve viselkedni. Aki bizonytalan abban, hogy kik mit tartanak róla nyilván, törekedni fog arra, hogy ne saját késztetéseit kövesse, hanem olyan viselkedést tanúsítson, hogy azzal ne tűnjön ki. Az ilyen külső kényszertől kívánta védeni a polgárt az információs önrendelkezési jog elismerésével a német alkotmánybíróság.

az adatkezelés jogalapja

A jogszerű adatkezelés egyik feltétele, hogy megfelelő jogalap alapján történjen a személyes adat kezelése. Ez fejeződik ki abban a szabályban, amely szerint „Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárul, vagy azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete elrendeli." [Avtv. 3. § (1)] Különleges pedig adat akkor kezelhető, ha az adatkezeléshez az érintett írásban hozzájárul, vagy a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, vonatkozó adatok esetében, az adatkezelés vagy nemzetközi egyezményen alapul, vagy az Alkotmányban biztosított alapvető jog érvényesítése vagy a nemzetbiztonság, a bűnmegelőzés vagy a bűnüldözés érdekében törvény rendeli el, egyéb különleges adatok esetén, ha azt törvény elrendeli. [Avtv. 3. § (2)]

hozzájárulás mint jogalap

Az adatalany hozzájárulása, mint az adatkezelés jogalapja tekintetében nemcsak a fenti formai (írásbeliségre vonatkozó) követelményeket fogalmazza meg a törvény, érvényességéhez ugyanis tartalmi

követelményeknek is eleget kell tennie. Az Avtv. a következők szerint határozza meg a hozzájárulás fogalmát. A hozzájárulás az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez [Avtv. 2. § 6. pont]. A hozzájárulással szemben támasztott követelmény tehát, hogy az félreérthetetlen legyen, az adatalany tudja, mihez járul hozzá, végül szabadon, nem kényszer hatása alatt dönthessen. Az egyén önrendelkezési joga szerint minden autonóm személynek joga van szabadon, saját értékei és élettervei szerint dönteni és cselekedni, és ennek a jognak csak mások hasonló jogai szabnak határt. Ennek megfelelően a hozzájárulás csak akkor nyújt megfelelő jogalapot a személyes adatok kezeléséhez, ha az az érintett kívánságának önkéntes, határozott és tájékozott kinyilvánítása.

önkéntesség, határozottság, tájékozottság

Itt is fontosnak tartjuk megjegyezni, hogy a háttéranyagok szerint elképzelhető, hogy az intelligens egészségügyi kártyán különleges adatok tárolására is sor kerülhet, ezért indokolt a különleges adatok kezelésének feltételéül előírt írásbeliség vizsgálata az elektronikus környezetben is. Az írásbeliségre vonatkozóan az elektronikus aláírásról szóló 2001. évi XXXV. törvény három típusú aláírás között tesz különbséget: elektronikus aláírás, fokozott biztonságú és minősített elektronikus aláírás között. Az elektronikus aláírás e három szintje egymásra hivatkozik. A fokozott biztonságú elektronikus aláírás az elektronikus aláírás egy fajtája; a minősített elektronikus aláírás pedig a fokozott biztonságú elektronikus aláírás egy fajtája. Az írásbeliség elismerése szempontjából kizárólag a fokozott biztonságú és a minősített elektronikus aláírás felel meg. A fokozott biztonságú elektronikus aláírás, amely alkalmas az aláíró azonosítására és egyedülállóan hozzá köthető, kizárólag az aláíró befolyása alatt áll és a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető. A minősített elektronikus aláírás a fokozott biztonságú elektronikus aláírás egyik fajtája, ami magasabb szintű technológiai védelmet jelent és a minősített hitelesítés-szolgáltatóval

írásbeliség elektronikus közegben

szembeni szakmai és megbízhatósági követelményeknek is megfelel. A különleges adatok kezeléséhez, így a kártyán való tárolásához, vagy az orvosi adatbázisból a biztosítók felé történő adattovábbításhoz az érintett írásbeli hozzájárulása kell, amelyet vagy kézzel, vagy a fent leírt fokozott biztonságú vagy minősített elektronikus aláírással kell, hogy ellássa. A közigazgatási eljárások során használható elektronikus aláírás, az azokhoz tartozó tanúsítványok és az azokkal összefüggésben nyújtott elektronikus aláírással kapcsolatos szolgáltatások követelményeit elegendő rendeleti szinten szabályozni. [Ket. 3. § (6)].

Az adatkezeléshez való írásbeli hozzájárulás tehát elektronikus úton is végrehajtható. Annak biztonsági fokozatáról és megoldásáról rendeleti szintű jogszabályt kell elfogadni, feltéve, ha az alapjog gyakorlását nem érinti. Ez utóbbi esetben ugyanis törvényi szinten szükséges rendezni a kérdést, elsősorban a Ket. szabályainak bővítésével. Természetesen nincs olyan előírás, ami a különleges adatnak nem minősülő személyes adatok kezeléséhez való hozzájárulás írásba foglalását tiltaná. Amennyiben elektronikus aláírást elhelyeznek a kártyán, akkor valamennyi adat kezeléséhez való hozzájárulásnál érdemes alkalmazni a szigorúbb, de ellenőrizhető és a visszaéléseket kiszűrni képes írásbeli formát.

jogszabályi jogalap

Kötelező adatkezelés esetén – tehát a jogszabály által elrendelt adatkezeléskor - az adatkezelés célját és feltételeit, a kezelendő adatok körét és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg. A kötelező adatkezelésre példa a szakazonosítók képzése, bizonyos esetekben kezelése és továbbítása, amit törvény ír elő.

célhozkotöttség

Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben

és ideig (Avtv. 5. §). A célhozkötöttség alapelve a személyes adatok védelmének egyik legfontosabb alapelve, magában foglalja az információs önrendelkezési jogot és törvényes kötelezettségeket ró az adatkezelőkre. A célhoz kötöttség az adatkezelés teljes folyamatára vonatkozik, az adatfelvételtől az adattovábbításon át az adatok törléséig. Ez a rendelkezés kizárja a készletező adatgyűjtést is. Erről az Alkotmánybírósági döntéseknél írunk az 1.1.4. pontban.

adattovábbítás, az adatkezelések összekapcsolása

Személyes adat csak akkor továbbítható, a különböző adatkezelések pedig akkor kapcsolhatók össze, ha az érintett ehhez hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek. Ez akkor is így van, ha ugyanaz az adatkezelője az elkülönült adatkezeléseknek, valamint vonatkozik az állami szervek által kezelt adatok összekapcsolására is (Avtv. 8. §). Az adatkezelés és az adattovábbítás garanciális feltételeit szabályozó 8. § e cselekmények jogalapját és a cselekmény célhozkötöttségét határozza meg. A törvény határozottan kimondja, hogy a célhozkötöttség elve azt is magában foglalja, hogy egyetlen szervezeten belül – így a közigazgatási szervezeteken – belül is csak korlátozottan hajtható végre adattovábbítás és adatkezelés összekapcsolása. Éppen ezért az adattovábbítás és az összekapcsolás feltételeit köteles ellenőrizni az adatokat továbbító, összekapcsoló adatkezelő.

adatminőség

Az adatkezelőnek biztosítania kell, hogy az adatok felvétele és kezelése tisztességes és törvényes, pontos, teljes, időszerű legyen. Tárolásuk módja legyen alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani. (Avtv. 7. §) Az adatminőség követelményének csak úgy lehet eleget tenni, ha az érintettek tájékoztatása megfelelő, és ha lehetőségük nyílik az adatok pontosítására és kötelező adatkezelés kivételével törlésére is.

adatbiztonság

Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a

technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmét biztosítani kell a távközlési vagy informatikai eszköz üzemeltetésekor is, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszközön történik. (Avtv. 10. §) A személyes adatokhoz való jogosulatlan hozzáféréssel szembeni védelem kialakítása terén az adatkezelőnek nagy mozgástere van. Az adatkezelés helyének, eszközének, hozzáférők körének és a biztonsági intézkedések meghatározása az adatkezelő diszkrecionális jogkörébe tartozik. Ezzel együtt az adatkezelő felelőssége objektív: ha nem megfelelő biztonságot alakít ki, polgári és büntetőjogi felelőssége akkor is fennáll.

adatelkerülés

Az adatelkerülés, illetve az adattakarékosság elvét, az adatvédelmi törvény nem tartalmazza kifejezett rendelkezés formájában. Az adatelkerülés elve a célhozkötöttség elvéből származtatható alapelv: eszerint az adatkezelő köteles az adatfelvétel, -tárolás, -továbbítás során a személyes adatok kezelését minimalizálni, lehetőség szerinti elkerülni. Ha egy cél személyes adat kezelése nélkül elérhető, akkor ezt a megoldást kell választani. Amennyiben ez nem lehetséges, akkor az adatkezelést a lehető legkevesebb adat használatával kell megoldani. Fontos megjegyezni, hogy az adatelkerülés, illetve az adattakarékosság elve nem kellőképpen tükröződik sem a jelenleg tapasztalható informatikusi szemléletben, sem pedig az államigazgatási és üzleti adatkezelők szemléletében: adatelkerülés helyett adatéhség, adattakarékosság helyett inkább adatpazarlás tapasztalható. A korlátozás azonban csak személyes (vagyis azonosított vagy azonosítható természetes személyekkel kapcsolatba hozható) adatokra vonatkozik, ezért annak nincs akadálya, hogy anonimizált vagy aggregált adatokból adattárházakat építsen az adatkezelő, vagy ilyen adatait adatbányászati módszerekkel elemezze. Ha az adatok kezelésének célja megszűnik, akkor

azok a továbbiakban nem kezelhetők. A személyes adatokat törölni kell többek közt akkor, ha az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt [Avtv. 14. § (2) d)]. Az adattörlés nem jelent feltétlenül fizikai megsemmisítést. Az Avtv. az adatbázisokra és az új technológiai megoldásokra alkalmas értelmező rendelkezéssel él, amikor kimondja, hogy az adattörlést az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges. (Avtv. 2. § 12.) Ez megtörténhet a fizikai törlés mellett felülírással és átkódolással is. A törlésről az érintettet értesíteni kell, valamint mindazokat, akiknek a vonatkozó adat továbbításra kerül. Az értesítés csak akkor mellőzhető, ha az érintett jogos érdekét nem sérti. (Avtv. 15. §)

adattörlés

1.1.2. A védelem szükségessége – néhány történeti megjegyzés

Az információ, az ismeretek feletti ellenőrzés gyakorlása mindig a hatalom legfontosabb eszközei közé tartozott. A XX. századi diktatúrák megjelenésével, majd ettől függetlenedve, az információs technológiák rohamos fejlődésével, növekedni látszott az a veszély, hogy az informáltak még tájékozottabbak, az információtól elzártak még kiszolgáltatottabbak lesznek; az információs hatalom ollója szétnyílik. Németországban a nácik az IBM lyukkártya technológiája segítségével, hatalomra jutásukat követően azonnal megkezdték minden német állampolgár adatainak összegyűjtésével az információs diktatúra kiépítését. Kelet-Európában ez szelektíven, a belső ellenséget és gyanús személyeket érintő titkosszolgálati adatbázisok kiépítésével kezdődött, jellemzően papíralapú, kisipari módszerrel. A 70-es évek elejétől az elektronikus eszközök használata is bevezetésre került.

a diktatúrák információs hatalmukat erősítik meg a nyilvántartásokkal

Az Egyesült Államokban az első népszámlálást 1790-ben tartották és akkor mindössze négy kérdést tettek fel. 1830-ban két személyes kérdést tettek fel: hogy süket-e vagy vak-e a válaszoló. 1860-ban már 142 kérdést tettek fel. 1890-ben a kérdések már egyaránt kiterjedtek a betegségekre, testi hibákra, jövedelemre, pénzügyi helyzetre, és ekkor alkalmazták először Herman

népszámlálások és adatkezelések

Hollerith lyukkártya készülékét. Az adatokat három év alatt dolgozták fel. A gép továbbfejlesztéséről az IBM gondoskodott, nagyrészt állami megrendelésre. A New Deal időszaka tovább növelte az állam információéhségét: 1943-ra az amerikai társadalombiztosítás már több mint százmillió darab lyukkártyát tárolt. A nagykapacitású számítógépek megjelenésével 1946-ra az információgyűjtés forradalma következett be. A mágnesszalagok, a gyorsaság és a rendszerezett tárolás, a másolás, az újrastrukturálás előnyére váltak. A számítógépek egyik legfontosabb megrendelője kezdetben az amerikai Népszámlálási Hivatal volt.

a jogállam túlzott információs hatalma is veszélyes

Sokan vallják, hogy a jogállamot nem szabad a személyes adatok gyűjtésében korlátozni, hiszen nem fog visszaélni vele, a diktatúra esetében pedig mindegy, milyen adatállományokkal rendelkezik, kiszemelt áldozatait mindenképpen megtalálja. Ezt a vélekedést a történelem cáfolja. Friss példa a 90-es évek brutális ruandai polgárháborúja. A hutuk uszítói a birtokukba került nyilvántartások alapján a rádióban beolvasták a meggyilkolandók nevét és autóik rendszámát is. A társadalmi berendezkedés változásával könnyűszerrel megvalósítható a jogellenes felhasználás, akár a jogszerűen összegyűjtött adatokból. Mégsem mindegy tehát, hogy a még konszolidált hatalom milyen adatvédelmi rendszert alakít ki.

totális adat-összekapcsolás

Jelenleg is folyik a vita az Egyesült Államokban a Pentagon Total Information Awareness (TIA) programjáról. A TIA célja, hogy a terrorfenyegetettségre hivatkozva, az emberek félelmére, veszélyeztetettségkomplexusaira építve, adatbányászati módszerekkel az online adatforgalom egészét ellenőrizzék és hírszerzési információvá változtassák át. A rendszer elvben és gyakorlatban lehetővé tenné, hogy az autópályákon rögzített forgalmi adatoktól a hitelkártya használatáig, vagy az elektronikus úton átutalt jótékonysági adományokig minden bekerüljön a TIA rendszerébe. A rendszer támogatói azt az indokolást erőltetik, hogy a rendes embereknek nem lesz okuk félelemre, hisz csak kiderül róluk, milyen kiválóak.

1.1.3. Az univerzális személyazonosító adat

országonkénti eltérések

Az univerzális azonosítókra vonatkozóan nem egységes az uniós adatvédelmi rendszer. Egyes alkotmányok, és az azokon alapuló alkotmánybírósági gyakorlat kifejezetten megtiltják az általános azonosító kód(ok) használatát (Portugália, Németország, Magyarország), más országokban használnak ilyeneket (például Belgium, Dánia, Hollandia, Finnország).

személyi szám határozat

Az Alkotmánybíróság a 15/1991. (IV. 13.) AB határozatában – a személyes adatok védelméhez való jog értelmezése mellett – megsemmisítette azokat a szabályokat, amelyek szerint Magyarországon a polgárokat korlátozás nélkül használható, általános és egységes személyazonosító jel, a személyi szám segítségével kellett nyilvántartani. Kimondta, hogy az ilyen személyi szám alkotmányellenes. Később az adatvédelmi törvénybe is bekerült egy olyan rendelkezés, amely szerint a korlátozás nélkül használható, általános és egységes személyazonosító jel alkalmazása tilos [Avtv. 7. § (2) bek.].

univerzális jel

egységes jel

Az Alkotmánybíróság által megsemmisített, a minden állampolgárnak és országlakosnak ugyanazon elv szerint kiosztott személyi szám úgynevezett *univerzális*, sokcélú azonosító volt, amelyet elvileg mindenféle nyilvántartásban használni lehetett. Nem ilyen azonosító jel az, amely az adott adatkezelés céljához kötött, és csak azon belül alkalmazható, mint például a folyószámlaszám, ügyfélszám, bérletigazolvány-szám. Az *egységes* személyazonosító jel értelme az, hogy ugyanarra a személyre vonatkozó adatokat könnyen és biztosan lehessen azonosítani, illetve összegyűjteni egy olyan rövid, technikailag könnyen kezelhető karaktersor segítségével, amely megváltoztathatatlan és összecserélhetetlen. Így a személyazonosító jel természetes velejárója minden integrált nyilvántartási rendszernek. Az egységes személyazonosító jel továbbá kiválóan alkalmas a különböző nyilvántartásokban fellelhető személyes adatok eseti összekapcsolására is. Segítségével az adatok könnyen hozzáférhetőek, valamint kölcsönösen ellenőrizhetőek.

Ezek az előnyök azonban a személyiségi jogok, s különösen az információs önrendelkezéshez való jog szempontjából súlyos kockázatot jelentenek. A legtávolabb eső, különböző célú nyilvántartásokból összeszedett adatokból előállítható az ún. személyiségprofil, az érintett tetszőlegesen széles tevékenységi körére kiterjedő és intimszférájába is behatoló művi kép, amely ugyanakkor az adatok kontextusból kiragadott volta miatt nagy valószínűséggel torz is. Az adatkezelő mégis ennek alapján hozza meg döntéseit, állít elő és ad tovább újabb személyre vonatkozó információkat. A nagymennyiségű összekapcsolt adat, amelyről az érintett legtöbbször nem is tud, kiszolgáltatja az érintettet, egyenlőtlen kommunikációs helyzeteket hoz létre, amelyben az egyik fél nem tudhatja, hogy partnere milyen információkkal rendelkezik róla. A személyi számmal dolgozó államigazgatás hatalma így mértéktelenül megnő. Ha pedig a személyi számot a nem állami szférában is használhatják, ez nemcsak az ottani adatfeldolgozóknak ad az érintett felett hatalmat, hanem az állam további hatalomnövekedéséhez vezet: még messzebbre terjeszti ki az adatokon keresztüli ellenőrzés lehetőségét. A korlátozás nélkül használható személyi szám így a totális ellenőrzés eszközévé válhat.

személyiségprofil

egyenlőtlen kommunikációs helyzet

túlzott hatalomkoncentrációhoz vezet

Az államnak az alapjogok védelmére vonatkozó elsőrendű kötelességéből következik, hogy ezt a kockázatot a legkisebbre kell csökkentenie: a személyi szám használatát garanciális szabályokhoz kell kötnie. Ez két módszerrel történhet: vagy a személyi szám használatát magát korlátozza pontosan meghatározott adatfeldolgozásokra, vagy a személyi számhoz rendelt információk kiadhatóságát és az ezzel működő nyilvántartások összekapcsolását köti szigorú megszorító feltételekhez és ellenőrzéshez. Az Alkotmánybíróság úgy találta, hogy a személyi szám akkor hatályos szabályozása anélkül tette az állami szerveknél kötelezővé, másutt lehetővé a személyi szám korlátlan használatát, hogy az abban rejlő veszélyeknek megfelelő biztosítékokat határozott volna meg, ezért az Alkotmányba ütközőnek mondta ki őket, a személyes adatok védelméhez való joggal ellentétesnek, mert azt szükségtelenül és aránytalanul korlátozták.

az állam feladata e veszélyek csökkentése

Az Alkotmánybíróság a személyi szám alkotmányellenességét azért mondta ki, mert a népesség-nyilvántartásról szóló, , akkor hatályos törvényerejű rendelet a személyi számra vonatkozóan semmiféle korlátozást nem tartalmazott. Ez azonban nem jelenti azt, hogy a személyi szám alkotmányosságához bármiféle korlátozás elegendő. Ezt azért fontos hangsúlyozni, mert az államigazgatásban időről időre felmerül az általános és egységes személyazonosító jel ismételt bevezetésének gondolata. Az Alkotmánybíróság össze is foglalta álláspontját abban a vonatkozásban, hogy melyek azok a határok, amelyeken belül egy állandó személyi azonosító kód alkotmányosnak minősül.

- Az univerzális személyi szám lényegénél fogva ellentétes az információs önrendelkezési joggal.
- Ezért az alkotmánnyal csakis a meghatározott célú adatkezelésre korlátozott használatú azonosító szám egyeztethető össze.
- Az ilyen korlátozott használatú „személyi számot" bevezető törvénynek szabályozási és ellenőrzési garanciákat kell tartalmaznia arra, hogy ezt a számot más összefüggésben ne használhassák.
- Sem az „állami szféra", sem az államigazgatás egésze nem tekinthető olyan egységnek, amelyen belül egyetlen egységes személyazonosító kódot lehetne bevezetni vagy használni.

E keretek között hozta létre a jogalkotó az államigazgatás számára a három egymástól eltérő célú és eltérő körben alkalmazott azonosító jelet:

- a személyazonosító jelet, amelyet a népesség-nyilvántartás szervei használnak,
- az adóazonosító jelet, amelyet az adózással összefüggésben lehet használni, és
- a társadalombiztosítási azonosító jelet, amelyet a társadalombiztosítási ellátásokkal összefüggő adatkezelésekben használnak.

Ezek részletes szabályait, az Alkotmánybíróság által fontosnak tartott

garanciális szabályokat a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény tartalmazza. Az ezeket az azonosítókat (is) kezelő állami szervek adatkezelését pedig az azóta megalkotott szektorális törvények szabályozzák.

A 15/1991-es alkotmánybírósági döntést sokféleképpen értelmezik, érvényességét és indokoltságát is kétségbe vonják. A döntés értelmezése körüli viták a mai napig megmaradtak, erre találhatunk példát a háttéranyagokban is. Noha az az értelmezés is felmerülhet, hogy a korlátozás nélküli azonosító tilalmának megfelel egy olyan azonosító, melyet bármely célra lehet használni, csak a gázkompenzáció/kismamagondozáson való részvétel regisztrációjára nem, hisz így már használata nem *univerzális,* ez a jogértelmezés nyilván ellentétes az Alkotmánybírósági döntés és azt követő törvényi szabályozás céljával, szellemével. Az alábbiakban e határozatot a többi releváns határozat történetiségébe ágyazva ismertetjük, kiemelve az Alkotmánybíróság által meghatározott többi, a személyes adatok védelméhez való joggal kapcsolatos alkotmányossági tételt.

a határozat félreértelmezése

1.1.4. A magyar alkotmánybírósági joggyakorlat

Az Alkotmánybíróság 1990. május elsején az akkor univerzális azonosítóként használt személyi szám visszaszorítása érdekében a formai alkotmányosság körén belül maradva megtette az első lépést a testület a 11/1990. (V. 1.) AB határozatban. A hármas tanácsban meghozott döntés a cégbejegyzésről szóló 13/1989. (XII. 16.) IM rendelet részleges alkotmányellenességét állapította meg. A döntés kimondja, hogy a személyi szám nyilvános használatát miniszteri rendelet nem írhatja elő, mert a szabályozásra „az igazságügyminiszternek nem volt törvényes felhatalmazása." „A személyi szám nyilvános használatának kötelező elrendelése a személyes adat védelméhez fűződő alapvető jog korlátozása..."

11/1990. (V. 1.) ABh.

személyi szám először alkotmánybírósági határozatban

A hazai alkotmánybíráskodás történetének egyik legnagyobb és legvitatottabb eseménye a személyi szám határozat volt 15/1991. (IV. 13.)

15/1991. (IV. 13.) ABh.

AB határozat. Ebben a határozatban valóban szigorú volt az Alkotmánybíróság. Megsemmisítette a népesség-nyilvántartás akkori hazai jogrendjét. Ám ezzel sem elégedett meg, hanem előírta az Országgyűlésnek a megalkotandó adatvédelmi törvény meglehetősen részletes tematikáját, nem utolsósorban pedig általános jogelvi tételként állapította meg, hogy „a korlátozás nélkül használható, általános, egységes személyazonosító jel (személyi szám) alkotmányellenes", és azt is, hogy az „Alkotmánybíróság – a 20/1990. AB határozat szerinti, addigi gyakorlatát folytatva – a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, *információs önrendelkezési jogként.*"

a személyi szám alkotmányellenessége

Ezzel a döntéssel az Alkotmánybíróság addig a lehetséges határig elment, ameddig elmehetett. Nem teljesen alap nélkül fejére vonhatta a vádat, hogy nem csupán bírája, de versenytársa is kíván lenni a törvényhozó (és az alkotmányíró) hatalomnak. Álláspontunk szerint a döntés és jogalkotási iránymutatás nem független a történelmi helyzettől, hiszen a szocialista rendszerben alkotott jogszabályokat helyezett hatályon kívül. Ez természetesen nem elégséges alkotmányossági indok.

Az információs jogok a rendszerváltás környékén különös szerepet játszottak. Dönteni kellett abban az ügyben, hogy vagy fennmarad az ellenőrizetlen hatalomkoncentráció, vagy valamiképpen kialakításra kerül az információs hatalom-megosztás alkotmányos rendje. A totális információs hatalom az Alkotmánybíróság által vezérelt kisebb reformokkal aligha lett volna átalakítható. Ha a kései „szocializmust" nem is tekinthetjük minden ízében zsarnokinak, információpolitikájában kétségtelenül az volt. Az Alkotmánybíróság igen határozottan és következetesen bontotta le az állami népességnyilvántartás jogi kereteit A döntés megakadályozta, hogy az ellenőrizetlen politikai hatalom a modern információtechnológiával párosítva zavartalanul rombolja az egyén integritását. Mindebből persze az is következik, hogy ami történt: kivétel; szervesen, alkotmányos folyamatban fejlődő jogállamban ilyesfajta radikalizmusra nemigen kerülhet sor. Az

ellenőrizetlen hatalomkoncentráció vagy információs hatalommegosztás

Alkotmánybíróság korai „nagy” határozatainak – köztük ennek – volt egy további, a magyar társadalomra is jótékony hatással járó következménye: A hatalom ekkor ismerkedett meg azzal, hogy az Alkotmány a rendőrök, a miniszterek, az állami nyilvántartások felett áll.

az Alkotmány a nyilvántartások felett

A személyi szám határozatnak van egy további, különös sajátossága. Az információs ipar folyamatos robbanásos fejlődése évről évre új helyzetet teremt a személyes adatok védelmében, sokan már földgolyó méretű információs börtönt vizionálnak. Ehhez képest a személyi szám határozat közvetlen jelentésében az adatvédelemnek kissé ismétlős, ódivatú felfogását képviselte talán már létrejöttekor is, mégsem teszik az újabb fejlemények a határozatot idejétmúlttá. Maradéktalanul időszerűek lesznek mindig a célhozkötöttségről, a készletező adatgyűjtésről, az információs hatalom megosztásáról, az adattovábbításról, a nyilvánosságra hozatalról, az adatbiztonságról és főként a polgárok önrendelkezési jogáról mondottak.

a határozat ma is időszerű

Van azonban egy közvetlen szövegréteg, amelyen a fejlődés túlhaladt már. Az, hogy Magyarországon skandináv mintára bevezették az univerzális személyazonosító számokat, más országokban pedig a szektorális azonosítók általános használatot nyertek, nem kizárólag a polgárok totális ellenőrzését volt hivatott szolgálni. Sokkal fontosabb érv volt, hogy a számítógépek tárolóképessége, sebessége korlátozott volt. A mai technikai feltételek között teljesen mindegy, hogy egy személyt tizenegy vagy kétszázötven karakterrel lehet-e azonosítani. Az univerzális azonosítási rendszer elvetése, illetve átalakítása a technika fejletlensége miatt a hatalom koncentrációjának korlátja volt. Ma ez a garancia sokkal inkább szimbolikus, semmint valóságos. Fontos tudnunk, hogy az univerzális azonosítók helyett a szektorális személyazonosító kódok használata önmagában nem sokkal több, mint az állam gesztusa, semmint elégséges garancia. Ebből persze nem következik az, hogy ha már megtiltottuk az univerzális azonosító használatát, belátva, hogy a szektorális számok sem védenek meg bennünket, adjuk fel ezt az eredményt. Sokkal inkább, hogy olyan megoldást kell találnunk, amely további biztosítékul szolgál a személyes adatok védelme

a technika fejlődése nem indokolja a határozatban foglaltak feladását

terén. Az egységes azonosító tilalma és az osztott információs rendszerek alkotmányos követelménye adják az alapját az állampolgárok azonosításával kapcsolatos közigazgatási alapkövetelménynek. Azonban számos egyéb, ezen elvek kibontását lehetővé tevő megoldással kell élni ahhoz, hogy az Alkotmánybíróság által lefektetett alapkövetelmények valóban teljesüljenek.

29/1994. (V. 20.) ABh

több szakazonosító egyetlen célra alkotmányellenes

A 29/1994. (V. 20.) AB határozat, az addigi adatvédelmi tárgyú határozatok továbbfejlesztése. A határozat kimondja, hogy „két személyazonosító jelrendszer kötelező használata ugyanarra a célra alkotmányellenes". A szabálysértési határozaton a személyi szám feltüntetése alkotmányellenes, mert a szabálysértési törvény „az elkövető személy adatait" rendeli feltüntetni, a nyilvántartási törvény viszont a személy szám használatát erre a célra nem engedi használni. A Betegbiztosítási Igazolvány adattartalmának szabályozását a rendeleti szintje miatt találta alkotmányellenesnek az Alkotmánybíróság, ebben az esetben tehát formai alkotmányellenességet állapított meg.

44/2004. (XI. 23.) ABh: az adatvédelem alkotmányossági vonatkozásainak összefoglalása

nem abszolút jog

a korlátozás feltételei

a lényeges tartalom korlátozása

A 44/2004. (XI. 23.) AB határozat rámutat, hogy az „Alkotmánybíróság korábban több határozatában foglalkozott az adatvédelem alkotmányossági vonatkozásaival. Már a 2/1990. (II. 18.) AB határozatában megállapította, hogy „a személyes adatok védelme nem annyit jelent, hogy azokat az érintett személyen kívül semmiféle okból és semmilyen körülmények között nem ismerheti meg senki más". (ABH 1990, 18, 20.) „A személyes adatoknak az Alkotmányban biztosított védelméből nem következik, hogy jogszabály nem írhat elő személyes adatok közlésére vonatkozó kötelezettséget." [55/2001. (XI. 29.) AB határozat ABH 2001, 442, 460.] „Kivételesen törvény elrendelheti a magántitok és a személyes adat kötelező kiszolgáltatását, és előírhatja a felhasználás módját is. A magántitok és a személyes adatok védelméhez való jognak ilyen törvényi korlátozása azonban csak abban az esetben minősíthető alkotmányosnak, ha megfelel az Alkotmányban a korlátozásokkal szemben támasztott követelményeknek." [20/1990. (X. 4.) AB határozat, ABH 1990, 69, 70.] „Az alapvető jog lényeges tartalmának korlátozása tehát akkor állapítható meg, ha a korlátozás kényszerítő ok

nélkül történik és az nem áll arányban az elérni kívánt cél fontosságával. A törvényhozó a korlátozás során tehát köteles az adott cél elérésére alkalmas legenyhébb eszközt kiválasztani, mert amennyiben az alkalmazott korlátozás a cél elérésére alkalmatlan, az alapjog sérelme megállapítható." [7/1991. (II. 28.) AB határozat, ABH 1991, 22, 25.] „Az információs önrendelkezési jogot, az Alkotmány 59. § (1) bekezdésében biztosított szabadságjogot, mint alapjogot csak elkerülhetetlen esetben lehet alkotmányosan korlátozni, akkor, ha a korlátozás elkerülhetetlenül szükséges és az a korlátozással elérni kívánt célhoz képest arányos. [46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 222-223.] „Az információs önrendelkezési jog gyakorlásának feltétele és egyben legfontosabb garanciája a célhoz kötöttség. Ez azt jelenti, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie a bejelentett és közhitelűen rögzített célnak. (...) A célhozkötöttségből következik, hogy a meghatározott cél nélküli, „készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés- és tárolás alkotmányellenes." [15/1991. (IV. 13.) AB határozat ABH 1991, 40, 42.] „Az Alkotmányból a személyes adatok felhasználását illetően - az alapjogi védelem szempontjait érvényesítve - a célhozkötöttség elve, és az osztott információs rendszerek alkotmányos követelménye határozható meg. [46/1995. (VI. 30.) AB határozat, ABH 1995, 219, 225.] A 26/2004 (VII.7.) AB határozat ismét leszögezte, amit az Alkotmánybíróság már 1991-ben kimondott, hogy az Alkotmánnyal csakis a meghatározott célú adatfeldolgozásra korlátozott használatú azonosító szám egyeztethető össze (ABH 1991, 56.). Az adatfeldolgozás célját úgy kell az érintettel közölni, hogy az megítélhesse az adatfeldolgozás hatását jogaira, és megalapozottan dönthessen az adat kiadásáról; továbbá, hogy a céltól eltérő felhasználás esetén élhessen jogaival. Ugyanezért az adatfeldolgozás céljának megváltozásáról is értesíteni kell az érintettet. Az érintett beleegyezése nélkül az új célú feldolgozás csak akkor jogszerű, ha azt meghatározott adatra és feldolgozóra nézve törvény kifejezetten megengedi. Személyes adat felvételéről, gyűjtéséről, tárolásáról, felhasználásáról rendelkező jogszabály akkor felel meg az Alkotmány 59. §-ának, ha garanciákat tartalmaz arra

a korlátozás elkerülhetetlenségének követelménye

célhozkötöttség

készletező adatkezelés tilalma

osztott információs rendszerek

célról szóló tájékoztatás

a cél megváltozása

az érintett kontrollálni tudja adatai sorsát

nézve, hogy az érintett személy az adat útját a feldolgozás során követni, és jogait érvényesíteni tudja. „E garanciális jogintézményeknek - az ellenőrizhetőség érdekében is - objektív korlátok közé kell szorítaniuk az adat útját.” [24/1998. (VI. 9.) AB határozat, ABH 1998, 191, 194.] Az Alkotmánybíróság 65/2002. (XII. 3.) AB határozatában azt is megállapította, hogy a jogalkotó a személyes adatok, illetve a szigorúbban védett különleges adatok kezelését akkor rendelheti el, ha az adatkezelés lehetővé tételével egyidejűleg meghatározza az adatkezelés pontos feltételeit, azaz az Alkotmány 59. § (1) bekezdésben garantált személyes adatokhoz való alapjog korlátozásának konkrét részletszabályait. (ABH 2002, 357, 363.)

a különleges adatok kezelésének szigorúbbak a feltételei

Az adószám alkotmányosságára vonatkozóan a határozat kimondja, hogy az „ágazatspecifikus azonosító”. A törvény nem kerüli ki a személyi szám mint általános nyilvántartási azonosító alkalmazásának tilalmát: az adóazonosító szám átadása csak más adóhatóság részére lehetséges, a törvény így nem hoz létre a személyi számmal azonos értékű azonosítót. [26/2004. (VII. 7.) AB határozat.]

adószám, mint szakazonosító

Az Alkotmánybíróság álláspontja szerint csak a tényleges és a közvetlen, s nem az eshetőleges veszély értelmezhető a célhozkötöttség követelményét kielégítő alkotmányos ismérvként. Az alkotmányellenesnek minősített szabályozás csak távoli, elvont veszély elhárítására irányul és ennek érdekében ír elő ún. „készletre” történő adatkezelést, s nem tartalmaz kellő alkotmányos garanciákat. Aránytalan és szükségtelen a jogkorlátozás, ezért alkotmányellenes. [36/2005. (X. 5.) AB határozat]

ismét a készletező adatkezelésről

1.1.5. Adatvédelmi biztosi joggyakorlat

Az adatvédelmi biztos intézménye csak 1995-ben, az univerzális személyi szám megszűnte után jött létre Magyarországon, ezért joggyakorlatában e kérdéskörrel szorosan összefüggő ügyeket nem találunk. Vannak azonban olyan, az azonosítás módjával, azonosító kártyákkal kapcsolatos állásfoglalásai, amelyeket itt is megfontolásra érdemesnek tartunk.

Az adatvédelmi biztosi gyakorlatban a multifunkcionális intelligens kártyák kérdését a 419/A/2000. számú ügy vetette fel. A Magyar Orvosi Kamara tagnyilvántartási kártyáját az egyik kereskedelmi bank készítette volna el, azzal a feltétellel, hogy az – többek között – bankkártyaként is üzemelhetett volna, ha az érintettek ahhoz hozzájárulnak. Az egészségügyről szóló 1997. évi CLIV. törvény (Eütv.) alapján a kamara a működési nyilvántartásba vétellel egyidejűleg a nyilvántartó szerv a nyilvántartásba vett személy számára arcképes működési nyilvántartási igazolványt állít ki, amely az alapnyilvántartási szám és a működési nyilvántartási szám mellett tartalmazza a nyilvántartásba vett személy nevét (leánykori nevét), anyja nevét, a szakképesítéssel, szakirányú szakképesítéssel kapcsolatos adatokat (megnevezés, oklevél, bizonyítvány száma), a korlátozott alkalmasságra vonatkozó információt, a nyilvántartás érvényességének időtartamát, megújítás esetén ennek tényét és az újabb érvényesség időtartamát. A Magyar Orvosi Kamara (MOK) arcképes működési nyilvántartási igazolványa a működési tagnyilvántartási rendszer (MOKREG) adatbázisára támaszkodik, amely minden kamarai tag aktualizált adatait tartalmazza. A Magyar Orvosi Kamara és a bank közötti együttműködési megállapodás szerint az intelligens, többfunkciós orvosi kártya lényege, hogy olyan kamarai tagsági kártya kerül bevezetésre, mely a tagsági funkciók mellett valamilyen más, a tagok számára hasznos funkciót is megvalósít, például bankkártyaként is használható. Az új orvosi kártyán elhelyezett chip először a kamarai tagok személyes adatait rögzíti, később további adatokkal töltötték volna fel, és úgynevezett „orvosi professzionális kártya" alapja lehetett volna. A rendszer kifejlesztésének finanszírozását a bank vállalta, amely hosszú távú együttműködési megállapodást kötött a Magyar Orvosi Kamarával. Az adatvédelmi biztosi vizsgálat rámutatott, hogy nem volt tisztázott, hogy a bank adatfeldolgozói vagy adatkezelői minőségben járt volna el, azonban a jogviszony tartalma szerint önálló adatkezelőnek volt minősíthető. Több jogsértést is feltárt a vizsgálat, így az érintettek megfelelő tájékoztatási és hozzájárulási joga is sérelmet szenvedett. A legfontosabb kifogás az volt, hogy a bank az érintettek hozzájárulása hiányában nem kezelhette a tagok adatait, a hozzájárulás pedig nem lehetett a kamarai tagság feltétele. Az

többfunkciós kamarai tagsági kártya

nem biztosított önrendelkezés

ajánlás mindazonáltal azt nem állította, hogy a többfunkciós kártya alkalmazása önmagában sértené az adatvédelmi törvényt.

1.2. Szakazonosítók rendszere és elektronikus ügyintézés szabályai

Az alábbiakban számba vesszük az elektronikus ügyintézésre és a szakazonosítókra vonatkozó legfontosabb szabályokat, tekintettel arra, hogy a Megbízó által említett egyik szempont az volt, hogy lehetőség szerint a hatályos jogi keretek között, a magasabb szintű jogszabályok minél kevesebb módosításával kívánja a kitűzött céljait elérni. A későbbiekben csak utalunk az itt bemutatott szabályokra.

azonosítást igénylő elektronikus szolgáltatások

Az elektronikus közigazgatási szolgáltatások közül az azonosítást igénylő szolgáltatások az alábbiak: okmányirodai szolgáltatások; adó, járulék és vámszolgáltatások; egészségügyi és szociális szolgáltatások; oktatási szolgáltatások; munkavállalással kapcsolatos szolgáltatások; egyéb szolgáltatások (például építési engedély).

elektronikus ügyintézés alapvető szabályai a közigazgatásban

Az elektronikus úton bonyolított hatósági eljárásról a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól 2004. évi CXL. törvény (Ket.) X. fejezete tartalmazza az elektronikus ügyintézéssel kapcsolatos fő szabályokat, melyek részleteit az elektronikus ügyintézés részletes szabályairól szóló 193/2005. (IX. 22.) Korm. rendelet tartalmazza.

a kérelem kötelező adattartalma

A kérelemre indított eljárás azonosításra vonatkozóan a Ket. kimondja, hogy a hatósághoz benyújtott kérelem tartalmazza az ügyfélnek és képviselőjének a nevét (megnevezését), lakcímét (székhelyét, telephelyét), továbbá meg lehet adni a hivatalos célokra használható elektronikus levélcímet vagy távközlési úton való elérhetőséget. Ha az adott ügyfajtára vonatkozó különös eljárási szabály előírja, a kérelemben az ügyfél azonosíthatósága érdekében fel kell tüntetni az ügyfélnek az ügy jellege szerinti és az eljáró hatóság által törvény alapján kezelhető azonosítóját (adóazonosító jelét, adószámát, társadalombiztosítási azonosító jelét, személyi azonosítóját stb.). (Ket. 35. §)

tilalmazott adatkérés

Az ügyfél-azonosításhoz szükséges adatok kivételével az ügyféltől nem kérhető olyan adat igazolása, amelyet valamely hatóság jogszabállyal rendszeresített nyilvántartásának tartalmaznia kell, és a személyes adatok tekintetében az adat továbbítását az adott ügy elbírálásához szükséges célból törvény lehetővé teszi vagy az ügyfél saját személyes adat tekintetében ezt kéri. (Ket. 36. §)

elektronikus aláírás az elektronikus ügyintézésben

Ha az ügyfél legalább fokozott biztonságú elektronikus aláírással rendelkezik, a kérelem az ügyfél elektronikus aláírásával ellátva a központi elektronikus szolgáltató rendszeren keresztül vagy közvetlenül a hatósághoz benyújtható. A hatóság az azonosításhoz az aláírás érvényességét, valamint az érintett hitelesítés szolgáltatónál viszontazonosítás jelleggel az aláíró természetes azonosítóit ellenőrizheti, ez azonban nem érinti az eljárás lefolytatásához szükséges jogszabályban meghatározott adatok átadásának kötelezettségét. A hitelesítés szolgáltató elektronikus aláírás közigazgatási felhasználása esetén az ügyintéző hatóság megkeresésére elvégzi a viszontazonosítást, és az adatok egyezését, vagy az eltérés tényét a megkereső hatósággal közli. (Ket. 160. §)

ügyfélkapu

Az ügyfélkapu létesítéséhez szükséges ügyfél-azonosításhoz az ügyfélnek személyazonosításra alkalmas hatósági igazolvánnyal - külföldi esetében személyazonosító igazolvánnyal vagy útlevéllel - kell személyazonosságát igazolnia és a természetes személyazonosító adatait megadnia. Az ügyfélnek egyidejűleg közölnie kell az elektronikus ügyintézéshez hivatalos célra használható elektronikus levélcímét is. (Ket. 160. §) Az ügyfél ezt követően egyszer használható kódot kap, amelynek alkalmazásával az ügyfélkapu megnyitásához szükséges, legfeljebb öt évig használható egyedi azonosítót képezhet. Az egyedi azonosítót az ügyfél megváltoztathatja. Az ügyfél tartozik felelősséggel, ha az egyedi azonosító harmadik személy által, az ügyfél hibájából válik megismerhetővé. Az ügyfélkapun keresztül a hatósággal kapcsolatba lépő ügyféltől az elektronikus ügyintézés vagy hatósági szolgáltatás nyújtásához más azonosító nem kérhető, ez azonban nem érinti az eljárás lefolytatásához szükséges, jogszabályban meghatározott

adatok átadásának kötelezettségét.

célhozkötöttségi szabályok

A központi rendszer az általa kezelt személyes adatokat (ügyfél neve, születési helye és ideje, anyja neve, elektronikus levélcíme, egyedi azonosítója) az ügyfélkapu működtetéséhez, illetve a kormányzati portálhoz történő hozzáféréshez szükséges azonosításon túl csak viszontazonosításra használhatja fel. Adattovábbításra a rendszerben résztvevők számára csak a név és elektronikus levélcímét továbbítható. (Ket. 160. §)

szakazonosítók szabályai

A személyes adatok célhozkötöttséggel ellentétes összekapcsolásának megakadályozására, vagy inkább megnehezítésére „vágta" három részbe a jogalkotó a korábbi személyazonosító jelet, amikor úgy döntött, hogy az állampolgárnak az állammal való három típusú kapcsolatában különböző azonosító kódokat fog használni. Így jött létre a személyazonosító jel, amelyet a személyiadat- és lakcímnyilvántartás szerve használ, és a választási eljárásban jut elsősorban szerephez: az adóazonosító, amelyet a természetes személy adózók azonosítására használnak az adóhatóságok; valamint a társadalombiztosítási azonosító jel, amelynek a társadalombiztosítási ellátások igénybevételével kapcsolatos nyilvántartásokban van azonosító funkciója. Ezt a három azonosítót a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény (a továbbiakban: Szaz.) hozta létre, és egyszersmind rendelkezett arról, hogy ezek az azonosítók személyes adatok (függetlenül attól, hogy megfelelnek-e az Avtv.-beli definíciónak, vagy sem) [5. § (2) bekezdés], valamint arról, hogy mely szervek használhatják ezeket az azonosítókat, és hogy hogyan kommunikálhatnak egymással a különböző azonosítókat használó szervek.

A törvény szerint az azonosítási kódok továbbításához törvényi felhatalmazás hiányában az érintett előzetes, írásbeli hozzájárulása kell. Mint azt már többször említettük, a legalább fokozott biztonságú elektronikus aláírás az elektronikus közigazgatás bevezetése során ajánlott. Az egyablakos ügyintézés során egyes esetekben elkerülhetetlen az

adattovábbítás, így az érintett írásbeli hozzájárulása.

A Szaz. törvény rendelkezései szerint az azonosító kódok mindegyikéről külön hatósági igazolványt kell kiadni. A hatósági igazolvány csak egy azonosító kódot tartalmazhat.

eltérő tartalmú igazolványok

Az adóigazolvány tartalmazza a polgár családi és utónevét, anyja nevét, születési helyét és idejét, adóazonosító jelét, valamint a kiállítás keltét. A TAJ kártya tartalma a törvény szerint a családi és utónév, a születési idő, valamint a TAJ szám. A személyi azonosítót igazoló hatósági igazolvány tartalma: családi és utónév, leánykori név, születési hely, idő, anyja neve, személyi azonosító, a lakcím, a tartózkodási hely cím érvényességi ideje és az okmányazonosító. Látható, hogy az eltérő célokra létrehozott igazolványok eltérő adattartalommal rendelkeznek, érvényesítve azt a célhozkötöttségi követelményt, amelyből következően minden igazolvány csak a rendeltetésének megfelelő adattartalommal készülhet el.

kapcsolati kód

A Szaz. a szakazonosítók használatára feljogosított nyilvántartások közötti adatáramlás megvalósítása (vagyis a nyilvántartások interoperabilitásának biztosítása) céljából bevezette a kapcsolati kód használatának követelményeit. A törvény értelmező rendelkezései szerint a kapcsolati kód a különböző célú adatkezelések közötti törvényes kapcsolat elősegítésére, megvalósítására képzett ideiglenes számjegysor. A gyakorlatban a kapcsolati kód alkalmas arra, hogy egy adatalanyt egyértelműen és kizárólagosan azonosítson két adatkezelés közötti kapcsolatban. Ennélfogva minden adatalany számára kell képezni egy egyedi kapcsolati kódot az A és B nyilvántartások között, egy másik kapcsolati kódot a B és C nyilvántartások között és ismét egy másikat az A és C nyilvántartások között, ahol A, B és C nyilvántartások a három szakazonosító alapján vezetett nyilvántartások, jellemzően a KEK KH, az OEP és az APEH nyilvántartásai. A Szaz. a kapcsolati kód tartalmának és képzési szabályainak megállapítását a társadalombiztosítási szerv feladatává tette az ugyanazon polgárra vonatkozó, rendszeresen ismétlődő adatszolgáltatás igénylése, teljesítése,

valamint az adatszolgáltatást kérő nyilvántartásának karbantartása céljából, azzal a feltétellel, hogy a kapcsolati kód nem lehet azonos az adóazonosító jellel, a TAJ számmal és a személyazonosító jellel, továbbá nem származtatható azokból, valamint hogy ugyanazon polgárra adatkérőnként más-más kapcsolati kódot kell képezni. A Szaz. előírja, hogy a kapcsolati kód kizárólag a fenti célra használható, azt az adatkezelés céljának teljesülése után mind társadalombiztosítási szerv, mind az adatkérő nyilvántartásából törölni kell; továbbá hogy a kapcsolati kódot csak a társadalombiztosítási szerv, valamint az adatszolgáltatást kérő kezelheti és továbbíthatja. Hasonló szabályokat ír elő a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (Nytv.), valamint a végrehajtásáról szóló 146/1993. (X. 26.) Korm. rendelet is a személyiadat- és lakcímnyilvántartás szerve vonatkozásában. Ugyancsak tartalmazza hasonló célú és alkalmazású kapcsolati kód használatának lehetőségét a (2002. évi XLVII. törvénnyel módosított) a foglalkoztatás elősegítéséről és a munkanélküliek ellátásáról szóló 1991. évi IV. törvény [57/A. § (6–7)]. Ismereteink szerint a kapcsolati kódokat, a rendelkezésre álló számítástechnikai infrastruktúra és szakértelem rendelkezésre állása miatt a gyakorlatban a személyiadat- és lakcímnyilvántartás szerve képezte, és ez a szerv vezette az egységes személyi számról a szakazonosítókra való átállás informatikai lebonyolítását is.

kapcsolati kód más jogszabályokban

1.3. Multifunkcionalitás, intelligens kártya, központi jogosultságkezelés

1.3.1. Példák a lehetséges kártyafunkciókra

Az intelligens kártya magában hordozza, sőt vonzza a multifunkcionalitás esélyét. Az észtek ma már nem csak szavazhatnak interneten elektronikus személyi igazolványuk segítségével, de fizethetnek is vele a közlekedési eszközökön. A multifunkcionális kártyák széleskörű felhasználási lehetősége többféle megoldást eredményezhet:

– adózási információk: a kártyabirtokos és az állam közötti adóügyi

kapcsolatok igazolása;

- az állam és az állampolgár közötti közjogi jogosultságok igazolása, de az állampolgári jogok gyakorlásának vagy kötelezettségek teljesítésének adatait akár rögzítheti is:
  - az állampolgári kártya akár alapja lehet a közvetlen e-demokrácia gyakorlásának (ami a képviseleti demokrácia részleges kiüresedésével járhat), igazolhatja az állampolgári jogok gyakorlását, a kötelezettségek teljesítését;
  - igazolhatja például az állampolgár feddhetetlenségét vagy ennek hiányát;
  - megerősítő (pozitív diszkriminációt biztosító) politikák körében jogosultságot igazolhat.
- bankkártya: lehetőség van bármelyik intelligens kártya bankkártya megoldásokkal való kombinálására. Akár egyetlen kártyán több bankkártya funkció lehet, akár olyan formában is, hogy a polgár több banknak ügyfele, de egyetlen kártyát használ (az ilyen felhasználást a bankok érdekei, függetlenül a polgár jogaitól, nyilván felülírnák);
- a bankkártya funkció lehet korlátozott, úgy, hogy a fizetésre szolgáló kártya feltöltése bankszámláról közvetlenül a bankautomatákról történhet, de alapvetően más funkciót szolgál.

Arra is van példa, hogy bankkártyával közvetlenül vehessen tömegközlekedési szolgáltatást bárki. A bankkártyák ilyen jellegű elterjedésének, a jogi megfontolásokon túl, feltehetően kártyabiztonsági okok vetnek gátat.

- Közlekedési funkció: A kártya alkalmassá tehető bármilyen típusú (tömegközlekedés, vasút, közút, légiforgalom) közlekedési viteldíj kifizetésére.
- Fizető kártya: A fizető kártya alkalmazás megvalósítása az alaprendszert a fizetési rendszerek széles választékával kapcsolja össze: boltok, ételautomaták, telefonkártya-feltöltő automaták használatát teszi lehetővé.
- Parkolási rendszer: a parkolási rendszert kétféleképpen lehet integrálni:

egyszerű díjfizetésként vagy a viteldíjrendszerbe illesztve a parkolás ösztönzésére: ha az utas a városba érve átszáll a tömegközlekedési eszközre, akkor kedvezményt kap.

- Pontgyűjtő rendszer: A kártyabirtokos összegyűjt egy meghatározható számú pontot, akkor a kártyájára szolgáltatást/kedvezményt/ajándékot kap.
- Oktatási kártya a tanulók iskolai adataival: tanulói, diák-kedvezmények igazolása, iskolai szolgáltatások igénybevétele, belépési jogosultság igazolása oktatási intézménybe, stb.
- Egészségügyi kártya.

a jog válasza a funkciók határtalan körére

A többfunkciós kártyával szemben támasztott technikai követelmény sokszor mindössze az, hogy elegendő memória legyen rajta. Könnyen belátható, hogy a kártya használatának az alkotmányos államban nem a folyamatosan tágabbá váló technikai korlát szab határt: a példálózó felsorolással ezt kívántuk jelezni. Megállapítható, hogy a többfunkciós kártyák felhasználási lehetősége technikailag korlátlan, azonban az egyes országok adatvédelmi rendszere jelentősen korlátozza a megoldási lehetőségeket. A korlátlan, technikai és jogi biztosítékok nélküli szabályozási filozófia alkotmányosan elfogadhatatlan. Az alkotmányos követelmények a technikaiaktól eltérő természetűek, annál sokrétűbbek és szigorúbbak. A jogi és a technikai biztosítékok rendszere egymásra épül. A jog a védelem és a veszélyeztetés lehetőségeinek változásaira reagál.

1.3.2. Külföldi példák – a magyar jogrendszer szemszögéből

Az átadott háttéranyagok közül külföldi megoldások ismertetését kizárólag az MTA Információtechnológiai Alapítvány „Elektronikus azonosító bevezetése: elvárások és igények, következtetések és javaslatok” című tanulmányában találtunk. A külföldi példák bemutatására nem is érdemes oly nagy hangsúlyt fektetni, legfeljebb a külföldi tapasztalatok, esetleges sikertelenségek vagy sikerek érdemelnek említést, ám jogszerűség, az adatvédelmi követelményeknek való megfelelés tekintetében a külföldi

példák nem értékelhetők közvetlenül. A személyes adatok védelmi szintje, a védelem rendszere, alkotmányos követelményei az Európai Unió tagállamaiban eltérőek. Az uniós szinten szabályozott, személyes adatok védelmére vonatkozó dokumentumok ugyanis csak a minimumszabályokat tartalmazzák. A magyarországi adatvédelmi szintet, a jogharmonizáció csak minimális mértékben befolyásolta, hiszen hazánkban az adatvédelem szintje – a posztdiktatorikus berendezkedésű országokra jellemzően – igen magas, a minimumszabályoknak már az uniós csatlakozást megelőzően is eleget tett.

külföldi megoldásokat egészében átvenni nem lehet

A külföldi modellek egy az egyben történő átvétele legtöbbször nem lehetséges. Legfeljebb adaptálni lehet bizonyos megoldásokat a hazai környezetre, de ezekben az esetekben mindig szükséges szem előtt tartani az eltérő jogi és kulturális szempontokat is. A kulturális szempontok közé soroljuk az állampolgárok bizalmi szintjét a közigazgatási szervek iránt, illetve az adataik védelme érdekében megtett és elvárt intézkedéseket is. A szigorú adatvédelmi követelményrendszerre azonban nem kell úgy tekinteni, amely akadályozza az elektronikus közigazgatási megoldásokat, hanem olyan feltételrendszert kell kialakítani, ami megfelel a közigazgatás és az állampolgári igényeknek a hatályos jogszabályi környezetben. A megoldás első lépése tehát a célkitűzések meghatározása, majd ezt követően annak kialakítása, hogy milyen technikai, szervezeti és esetleg jogalkotási megoldások szükségesek ahhoz, hogy a projekt megvalósítható és sikeres legyen. (Ez következik az adatvédelem egész Európában ismert célhozkötöttségi elvéből is.)

A fentiek alapján a háttéranyagokban ismertetett külföldi megoldások hazai bevezetésének lehetőségeit és korlátait elemezzük. A példák felsorolása mellett kitérünk azok hazai implementálásának feltételeire, illetve akadályaira is.

az osztrák modell

Az osztrák modellben, hasonlóan a magyar megoldási variációkhoz, eredetileg szerepelt a többfunkciós kártya koncepció. A többfunkciós kártya egy plasztiklapon való elhelyezése kötelező jelleggel végül nem valósult

meg, de többfunkciós kártya lehetősége továbbra is biztosított.

egy törvényben elrendelt, szektorokon átívelő adatkezelés

Az osztrák megoldás jogdogmatikailag azt a megoldást választotta, hogy egy törvényben szabályozza a különböző területekhez tartozó megoldásokat. Álláspontunk szerint egy ilyen megoldás nálunk nem lenne megfelelő. A hazai adatvédelmi szabályozás vertikális elkülönítése a jogalkalmazás megkönnyítése érdekében fontos feladat, ezért az egyes adatkezelési módok esetén a vonatkozó jogszabályok módosítása szükséges. A Ket. és a szakazonosítókra vonatkozó jogszabályok olyan struktúrát alkotnak, amelyeket saláta-törvénnyel nem érdemes módosítani. (A Megbízó maga is közölte az egyik szóbeli egyeztetésen, hogy lehetőség szerint minél kevesebb és minél alacsonyabb szintű jogalkotással megvalósítható projektet támogatna, a sok szektoron átívelő törvénymódosítások nem ilyenek.)

Az osztrák modellben az elektronikus úton benyújtott kérelmek esetén az illetékmentesség olyan megoldás, amelyhez hasonló ösztönző megoldásokat a projekt sikeressége érdekében érdemes bevezetni. A legtöbb külföldi példa ugyanis azt mutatja, hogy az elektronikus azonosítás nemcsak a digitális írástudás hiányosságai miatt nem halad olyan tempóban, mint az eredetileg tervezték, hanem azért is, mert az ösztönző-rendszerek hiányoznak. Az új megoldások esetén a költségeknek az állampolgárra terhelése vagy a bonyolult regisztrációs módok riasztóan hatnak. (Lásd még erről a 2.2.2. pont alatt írtakat is.)

Az osztrák modellhez hasonló elektronikus ügyfélazonosítási megoldás egyébként elképzelhető Magyarországon is. Ausztriában titkosító kulcsot használnak, ami a központi nyilvántartó hivatal birtokában van, a lenyomatoló (hashing) eljárással származtatható szakazonosítók megfelelően titkosítottak. Az osztrák azonosítási rendszer az elektronikus aláírás használatára épít. Az elektronikus aláírás a hazai elektronikus azonosítási projektekben is kulcsszerepet játszik. Az elektronikus aláírás bevezetése megfelel az Avtv.-ben rögzített önrendelkezési jog gyakorlásának is. Bár a stratégiai anyagok nem célul tűzik ki, csupán a kitűzött célok egyik

lehetséges megoldásként említik az elektronikus aláírás bevezetését az azonosítás során, álláspontunk szerint mind az azonosítás, mind az önkéntesség követelményeinek eleget tenne az elektronikus aláírás széles körű bevezetése. Az elektronikus aláírás akár fokozott biztonságú, akár minősített, megfelel az írásbeliség jelenlegi követelményének. Fontos azonban megjegyeznünk, hogy az elektronikus aláírás a polgári jogi jogviszonyokban is használható lehet. A közigazgatás és az üzleti szféra által használt közös aláírókulcs használata azonban az adatok könnyűszerrel történő, a célhozkötöttség követelményeivel ellentétes összekapcsolását és személyiségprofil kialakítását is lehetővé teszi. Az univerzális azonosítók használata pedig alkotmányellenes (erről bővebben az 1.1.3. és a 2.1.1. pont alatt írtunk), ezért a közigazgatásban használt kulcspárok felhasználási területét szűkre kell szabni.

észt modell

Az észt modellben az azonosítási eljárások alkalmazása során nem válik szét az üzleti szféra és a közigazgatási szféra azonosítási módja. Az állampolgárok a bankok azonosító rendszerével és az észt elektronikus személyi igazolvánnyal is azonosíthatják magukat. Az elektronikus személyi igazolvány minden állampolgár és egy évnél hosszabb ideig az országban tartózkodó külföldi számára kötelező. Az észt modell alapul vétele azonban csak igen szűk körben képzelhető el. Ennek oka, hogy Észtországban a személyes adatok védelme teljesen eltérő logika alapján valósul meg. A személyes adatok védelmének két oldala – a védelmi és önrendelkezési oldal – jóval alacsonyabb szintű, mint hazánkban, vagy akár mint Európa sok országában. Észtországban személyazonosításra egyetlen azonosító számot használnak, amely nyilvános (!) adat. Az észt rendszerben tehát a személyazonosítás említett két eleme: az egyetlen szám és a nyilvánosság alapjaiban mond ellent a hazai szabályozásnak. Az univerzális azonosító vonatkozásában az Alkotmánybíróság 15/1991 (IV. 13.) AB határozatában kimondta, hogy „a korlátozás nélkül használható, általános, egységes személyazonosító jel (személyi szám) alkotmányellenes”. Ugyanez a határozat a nyilvánosságra vonatkozóan megfogalmazta, hogy a személyes adatok védelméhez való jog nem hagyományos védelmi jog, hanem annak

nyilvános személyi szám

aktív oldalát is figyelembe véve, információs önrendelkezési jog, ezért annak nyilvánosságra hozataláról főszabályként az érintett dönthet.

központi nyilvántartások

Az észt modell alapvetően központi nyilvántartásokra épül. A kártyán elhelyezett adatok (személyi azonosító szám, név, képmás, születési dátum, aláírás) mellett egy azonosítási célú, és egy aláírási célú minősített tanúsítványt tartalmaz. Ugyanakkor az észt modellben megvalósuló magánkulcsot védő kettős PIN kód megoldás megfelelő biztonságot jelent a jogosulatlan felhasználás ellen, így bár adatvédelmi szempontból a magyar viszonyok között önmagában elégtelen, adatbiztonsági szempontból kielégítő megoldást nyújt. Biztonsági megfontolásokból Észtországban nincs kulcs-helyreállítási lehetőség, a kulcsokat tehát nem tárolják központban, ami ugyancsak példaértékű megoldás lehet.

elektronikus levélcím az államtól

Ugyancsak megfontolandó az észt rendszerben az a megoldás, hogy mindenkinek kiosztásra kerül egy (saját, egyedi) elektronikus levélcím. Az e-mail cím nem postafiókot jelent, az állampolgár innen irányíthatja át saját postafiókjába az állam által adott címre küldött elektronikus küldeményeket. Ez a megoldás a kommunikáció titkosítását könnyűszerrel megoldhatóvá teszi. A megfelelő eljárással biztosított kommunikáció az állam és a polgárok közötti kommunikációban szükséges feltétele a személyes adatok védelmének.

a hitelesítés szolgáltatás kiszervezése a közigazgatásból

Az észt rendszerben a tanúsítványokat egy (magán) hitelesítés-szolgáltató bocsátja ki, amelyet két bank és két távközlési cég alapított. Ez a megoldás a fent említett, az üzleti szféra és az állami szféra közötti adatáramlás veszélyei miatt nem javasolt. Az igazolványok kiállítása mindenképpen közigazgatási feladat kell, hogy maradjon.

Mint arra már utaltunk, az észt megoldás a központosított architekturális megoldást választotta. A központosítás biztonsági problémái és a személyes adatok védelmének kritériumrendszere miatt ezt a megoldást Magyarországon nem lehet választani, egy-két eleme azonban bizonyos

feltételekkel megvalósítható.

brit megoldás

A brit megoldás közvetlenül az angolszász jogrendszerekben kialakult magánszférát (a magyar jogi fogalmakkal nehezen leírható *privacy*) védi, és nem a személyes adatok védelmén keresztül biztosítja az információs önrendelkezési jogot. Bár a háttéranyagok alapján a „brit hozzáállás és tapasztalat már több területen hasznos információkat nyújtott a hazai kormányzati informatikai döntések előkészítéséhez (az 1990-es évek elején az információtechnológiai kultúra egész megalapozását ezek segítették elő).”, álláspontunk szerint a brit rendszer nem szolgálhat mintaként a magyar döntéshozók számára. Az eltérő adatvédelmi és nyilvántartási rendszer, valamint a teljesen más állampolgári attitűdök miatt nem lehet összehasonlítani a megoldásokat.

eltérő hozzáállás az információs magánszféra védelméhez

elektronikus azonosításra alkalmas útlevél

A személyazonosításra szolgáló brit igazolványok közül az útlevél már képes (a helyszínen és nem távoli ügyfél-hivatal kapcsolatban történő) elektronikus azonosításra. „Ennek hangsúlyos szerepet szánnak, valószínűsítik, hogy ez a megoldás széles körben elterjed, ezért a személy azonosításában erre erősen támaszkodni kívánnak.” – szerepel az MTA Információtechnológiai Alapítvány háttéranyagában. Ennek a megoldásnak az előnye abban rejlik, hogy nem szükséges új infrastrukturális beruházásokat végrehajtani. Hazánkban bevezetésre kerültek a kártya alapú igazolványok, ezek egyszerre történő lecserélése nem indokolt. Hasonlóan a brit koncepcióhoz, érdemes a meglévő rendszereket továbbfejleszteni, hiszen nincs olyan kényszerítő erő, amely a teljes lakosság kártyacseréjét indokolná. Ez persze nem jelenti azt, hogy önkéntes alapon történő kártyacsere feltételeinek kidolgozását el kellene vetni.

1.3.3. A Közigazgatási Informatikai Közműről

A háttéranyagok áttanulmányozása során, csakúgy, mint az elektronikus kormányzati fejlesztések témájában tartott szakmai fórumokon elhangzottakban többször találkoztunk a Közigazgatási Informatikai Közmű

kifejezéssel. A kifejezést az egyes dokumentumok különböző értelemben használják: egyrészt a központi elektronikus kormányzati szolgáltatások fejlesztésének általános metaforájaként, másrészt egy központi azonosításon és jogosultságkezelésen alapuló konkrét elképzelés megnevezéseként, harmadrészt pedig egy olyan központi azonosításon és jogosultságkezelésen alapuló rendszer értelmében, amely egységes „intelligens állampolgári azonosító eszköz" (kártya) használatát feltételezi.

a kifejezés tartalma

Kiemelten hangsúlyozzuk, hogy az általunk ismert „intelligens állampolgári azonosító eszköz" koncepcióját, amely egységes és általános állampolgári ügyfél-azonosító bevezetésén, az azonosító eszköz elektronikus TAJ kártyaként, magán (egyéb) biztosítási kártyaként, személyazonosító okmányként, valamint számos egyéb közigazgatási, üzleti és magáncélú felhasználásra alkalmas integrált kártyaként való alkalmazásán alapulna, adatvédelmi szempontból elfogadhatatlannak ítéljük. Tekintettel arra, hogy a Megbízó által átadott írásos anyagok, koncepciók ennek az eszköznek a leírását és tervezett felhasználását nem tartalmazzák, részletes értékelésétől és bírálatától e helyütt eltekintünk – vonatkozó érveinket tanulmányunk más részeiben részletesen kifejtjük.

A KOPINT-DATORG Rt. „Közigazgatási Informatikai Közmű – Elektronikus azonosító rendszer bevezetése" c. megvalósítási tanulmánya ügyfelek és hivatalnokok központi azonosításán és jogosultságkezelésén alapuló, az Ügyfélkapu koncepciójára és továbbfejlesztésére épülő (de integrált állampolgári kártyát nem tartalmazó) elképzelést ír le. Megítélésünk szerint e rendszer egyes elemei önmagukban adatvédelmi szempontból nem kifogásolhatóak, sőt előnyösek, ilyen például a PKI alapú elektronikus ügyfélkapcsolat általánossá tétele; más elemeiről, például az átmeneti időszakban alkalmazandó, más szolgáltatókkal végzett viszontazonosításról pedig e tanulmány más fejezeteiben fejtjük ki álláspontunkat. E helyütt a Közmű koncepció két aspektusát emeljük ki: a központi azonosítás és a központi (ügyintézői) jogosultságkezelés adatvédelmi, illetőleg közigazgatási vonatkozásait, utalva a másutt is kifejtett érveinkre.

a koncepció egyes elemei támogatandóak

központi ügyfélazonosítás

A központi ügyfélazonosítás akkor fogadható el adatvédelmi szempontból, ha nem jár egy új, egységes és a közigazgatáson belül (esetleg azon kívül is) univerzálisan használható, sőt használandó állampolgári azonosító létrehozásával. Egy ilyen rendszer továbbá nem teheti kötelezővé és kizárólagossá saját PKI rendszerének használatát; lehetővé kell tennie más szolgáltatók funkcionálisan és biztonsági szempontból megfelelő elektronikus aláírási és tanúsítási rendszerének használatát. A központi ügyintéző- (pontosabban köztisztviselő-) azonosítás ezzel szemben lehet kizárólagos és centralizált, sőt, kívánatos is, hogy a köztisztviselői tanúsítványokat az állam kezelje. Álláspontunk szerint továbbá szükség van arra, hogy a köztisztviselők hivatali jogosultságaikat (függetlenül attól, hogy azok kártya vagy más eszköz használatához vannak-e kötve) civil élethelyzeteikben, például ügyfélként ne használhassák. Azok az elképzelések, amelyek szerint a köztisztviselők hivatali jogosultságait az egész közigazgatásra kiterjedő egységes rendszerben kellene szabályozni és a Közmű informatikai infrastruktúráján keresztül kezelni, vagyis hozzárendelni az ügyekhez és ügyfelekhez, megítélésünk szerint olyan bonyolult és bürokratikus rendszert eredményezne, amely ellentétes lenne az elektronikus kormányzati szolgáltatások fejlesztésének kitűzött céljaival. Ellentétes lenne továbbá a közigazgatás szervei közötti munka-, feladat- és felelősség-megosztás szempontjaival is, és igen nehézzé tenné a speciális esetek, alternatív ügyintézési megoldások, kivételek alkalmazását is. Felhívjuk a figyelmet az EU adatvédelmi irányelvében és a magyar adatvédelmi törvényben is szereplő azon rendelkezésre, amely az ügyfeleket érintő automatizált egyedi döntésekre vonatkozik. Eszerint kizárólag számítástechnikai eszközzel végrehajtott automatizált adatfeldolgozással az érintett személyes jellemzőinek értékelésére csak akkor kerülhet sor, ha ahhoz kifejezetten hozzájárult, vagy azt törvény lehetővé teszi. Az érintettnek álláspontja kifejtésére lehetőséget kell biztosítani, valamint az automatizált adatfeldolgozás esetén az érintettet – kérelmére – tájékoztatni kell az alkalmazott matematikai módszerről és annak lényegéről [Avtv. 9/A. §] Olyan gyakorlati ügyintézési eljárásokat kell tehát kidolgozni az

központi köztisztviselő-azonosítás

köztisztviselői jogosultságkezelés

automatizált egyedi döntés

elektronikus kormányzat keretei között is, amelyek szükség esetén eleget tesznek a fenti követelményeknek. Mindez természetesen nem jelenti azt, hogy rutinszerű, tömeges ügyfélfogalmat érintő ügytípusok jelentős mértékben automatizált intézését nem lehet megvalósítani, csupán a teljes egységesítést és központosítást látjuk adatvédelmi és közigazgatási szempontból aggályosnak.

1.4. Az elektronikus azonosítással kapcsolatban megfogalmazható adatvédelmi természetű alapelvek, követelmények

Az Alkotmány, az adatvédelmi alapelvek, ezek releváns alkotmánybírósági értelmezése, az adatvédelmi törvény és ennek adatvédelmi biztosi értelmezése, a hazai szakazonosítókra és elektronikus ügyintézésre vonatkozó szabályozás, valamint a külföldi példák tapasztalatai alapján megfogalmazhatjuk azokat az alapelveket, amelyeket bármilyen, a témába vágó koncepcióalkotáskor figyelembe kell venni. A 2. pont alatt elemzett koncepcióalkotó elemek vizsgálatakor ezen alapelveknek való megfelelőségüket fogjuk számon kérni.

önkéntesség elve

Az információs önrendelkezési jogból következik az önkéntes részvétel biztosításának követelménye. Ennek megfelelően: amíg ez nem tenné lehetetlenné a kitűzött, alkotmányosan elfogadható közigazgatási célt, lehetővé kell tenni, hogy az állampolgár önkéntesen járulhasson hozzá olyan adatkezelésekhez, amelyek nem eleve elengedhetetlenek, és ezért nem törvény által elrendeltek. Az önkéntesség a közigazgatás–állampolgár viszonylatban pedig, a polgár kiszolgáltatott helyzete miatt speciális garanciákat követel.

választási szabadság

Ugyancsak az információs önrendelkezési jogból következően az a megoldás támogatható elsősorban, amely az állampolgár számára valódi választási szabadságot, alternatívákat biztosít adatai sorsát illetően. Kerülendők az olyan egységes rendszerek, amelyek figyelmen kívül hagyják az állampolgárok eltérő felkészültségét a technikai újdonságok használatára,

nem veszik figyelembe az ezekkel szembeni eltérő bizalmukat és szándékaikat. Azok a jobb megoldások, amelyek az állampolgárok tudatos döntésén alapulnak, valamint lényegében azonos adatbiztonsági szintet megvalósító, de kényelmi vagy egyéb (gazdasági) szempontok szerinti választást is lehetővé tesznek.

adatelkerülés

A célhozkötöttség elvéből következik az adatelkerülés vagy adattakarékosság követelménye, amelyet bármilyen koncepció megvalósításakor figyelembe kell venni. Eszerint csak olyan adat kezelését szabad előírni és csak olyan adatot szabad kezelni, amely a kitűzött cél megvalósításához elengedhetetlen, amely nélkül a kitűzött cél nem lenne megvalósítható. Ebből következik például az, hogy ahol ez elegendő, ott az azonosító rendszereket kizárólag jogosultság-ellenőrzésre, és nem adattárolásra, további adatok gyűjtésére lehet használni. Ez az elv tartandó szem előtt akkor, amikor döntés születik arról, mely személyes adatok kerülnek egy azonosító eszközre, és melyek a központi adattároló egység(ek)be. Ugyanezen elvből következően az arcképes kártya – mivel az azonosítás során kevesebb további személyes adat megismerését igényli, és az ellenőrzés kényelmetlenségeit is csökkenti – kedvezőbb megoldás lehet. Amennyiben nem szükséges a használat közben keletkező személyes (forgalmi) adatok rögzítése a kártyán vagy más adattárolón, akkor úgy kell kialakítani a rendszert, hogy ez ne történjen meg. Az adatelkerülés elvéből következik továbbá az is, hogy megfelelő garanciákat kell kialakítani arra vonatkozóan, hogy az esetlegesen keletkező helymeghatározási adatok felhasználására csak akkor és olyan körben kerüljön sor, ami a kártya biztonságos használatát hivatott elősegíteni. (A kártyahasználat, a kártya nélküli kulcsok használata, nemcsak személyiségprofil-képzés szempontjából lehet kockázatos, de fizikailag is követheti a kártyajogosult, illetve kulcshasználó mozgását, akárcsak a mobiltelefonja, bankkártyája. A kártya használatának helye személyes adat, hiszen levonható belőle az érintettre vonatkozó következtetés.) A helymeghatározási adatok egyéb célú felhasználása, gyűjtése, tárolása jogellenes, hiszen nincsen olyan cél, ami az adatbiztonságon túl ezen adatok kezelését legitimálná.

célhozkötött hozzáférés az adatokhoz

Bárhol is történik a személyes adatok kezelése, azokhoz az adatalanyokon kívül mindenki más csak célhozkötötten férhessen hozzá. Ezt a kártyák esetében megfelelő technikai intézkedésekkel kell garantálni, a nyilvántartások esetében ezzel szemben elsősorban szervezési és jogi garanciák szükségesek. Igaz ez a nemzetbiztonsági és bűnüldöző szervek adatigényére is. Az adatkezelés célja a közigazgatás és az állampolgár közötti biztonságos adatáramlás megteremtése, a megbízható azonosíthatóság és nem a bűnüldözés vagy nemzetbiztonság. A bűnüldözési és nemzetbiztonsági célú adatkezelés esetén jogi garanciaként a jogszabályok az adatokhoz való hozzáférést bírói engedélyhez kötik. Ugyancsak garanciális elem lehet az adatvédelmi biztosi és az ügyészi ellenőrzés.

kontroll a saját adatok felett

Az önrendelkezési jogból következik, hogy az állampolgár számára lehetőséget kell biztosítani a személyes közreműködésre, ezzel biztosítva, hogy kontrollálni tudja adatai sorsát. Ebből következően például a kártyáján tárolt adatokhoz csak általa ismert jelszó használatával lehessen hozzáférni, illetve a polgár az adatai továbbításáról proaktív tájékoztatásban részesüljön. Ezen alapelvből következik többek között a fizikai kártya elvesztése, ellopása, vagy más adatok illetéktelenek kezébe jutása esetére az adatok letilthatósága és lehetőség szerint értelmezhetetlenné tétele. Ebből következik az is, hogy az az adatkezelési politika támogatandó, amelyben a személyes adatok a kártyát birtokló személy rendelkezése alatt állnak, szemben azzal, amelyben azok kikerülnek az ő rendelkezése alól.

profilépítés kizárása

Minden szakaszban vizsgálandó, miképpen kerülhető el a különböző célú adatkezelésekben tárolt, egy-egy személyre vonatkozó adatok jogellenes összekapcsolása, ezzel az egyes adatkezelési célok által nem megkívánt személyiségprofil képzése. Az adatkezelések összekapcsolásán túl e cél érdekében kell előírni az adatok megfelelő időben történő törlését is: miután az adatkezelés célja megvalósult, a célhozkötöttség követelménye miatt az adatok további tárolására nincs törvényes lehetőség, az adatokat törölni kell.

Az esetlegességek kiküszöbölése érdekében szabályokat kell alkotni az adatok megőrzésének rendjéről és idejéről, a selejtezéséről és a megsemmisítéséről is.

adatbiztonság

Olyan szervezési és technikai megoldásokat kell választani, amely az adatokat az egyes adatkezelések természetéhez mérten szükséges szinten megvédik a jogosulatlan hozzáféréstől, az indokolatlan sérülésektől, törlésektől. Az adatbiztonság szintjét állandóan tesztelni kell, hiszen annak nincs törvényben rögzíthető legmagasabb mértéke. Az adatkezelő annak színvonalát folyamatosan javítani köteles. Az adatfeldolgozó rendszerek komplexitása és folyamatos fejlődése, valamint a biztonságot veszélyeztető tényezők bővülése folyamatosan szélesíti az adatbiztonságra vonatkozó követelményeket.

2. A megismert koncepciók releváns elemeinek vizsgálata

A Megbízó részben a szerződés mellékleteként, részben pedig a későbbiekben írásban olyan koncepció-leírásokat ismertetett meg velünk, amelyek egyrészt több különböző célt valósítanának meg úgy, hogy az egyes koncepciók között részben átfedés volt az elérendő célok tekintetében, másrészt pedig a koncepciók részben egymást kizáró, és részben több koncepciónak is részét képező elemekből, technikai és szervezési megoldásokból építkeznek.

a koncepciók építőelemekből állnak össze

Adatvédelmi szakértői véleményt ezekről az építőelemekről lehet mondani, mert ezek jelentik a jogilag is definiálható tartalmát az egyes koncepcióknak. Az egyes építőelemek mentén történő vizsgálatot indokolja az is, hogy a Megbízó egyelőre érezhetően nem döntött egyik koncepció mellett sem, és az egyes koncepciók is meglehetősen diffúznak tűnnek, mind a leírt formájukban, mind a szóbeli konzultációkon elhangzottak alapján. Az alábbiakban adatvédelmi szakértői véleményt ezért a koncepciók által használt egyes szervezési és technikai megoldásokról mondunk, úgy, hogy rájuk vetítjük az előzőekben felvázolt, az Alkotmány 59. §-ából, valamint az annak végrehajtására megalkotott adatvédelmi törvény rendelkezéseiből következő elvek, követelmények rendszerét. Ennek eredményeként ki fog derülni, hogy mely építőelemeket, technikai és szervezési megoldásokat tartjuk támogathatónak adatvédelmi szempontból, és milyen feltételekkel, és melyeket tartjuk elfogadhatatlannak. A későbbi koncepcióalkotáskor, a meglévő koncepciók további kidolgozásakor ez a vélemény szándékaink szerint eligazításul tud majd szolgálni a kidolgozásban közreműködők számára.

összevetés az elvekkel

Azokat az építőelemeket vesszük sorra, amelyeket az átvett dokumentumokból és a szóbeli konzultációkon megismertünk. Bizonyosak vagyunk abban, hogy ezeken kívül is léteznek ilyen, a kitűzött célokat megvalósító technikai és szervezési megoldások, amelyek eddig elkerülték a

a kimaradó elemek is megítélhetők

koncepcióalkotók figyelmét, és amelyeket így részletesen nem érintünk. Az előzőekben ismertetett általános követelmények, elvek megfelelő alkalmazásával azonban ezek megengedhetősége, adatvédelmi elemzése is elvégezhető.

2.1. A távoli ügyintézést lehetővé tevő elemek

kitűzött célok

A megismert koncepciókban kitűzött, egyik ismétlődően felmerülő célként határozható meg az állampolgárok hivataltól távoli, otthonról, munkahelyről, nyilvános internet-elérési pontból történő ügyintézésének lehetővé tétele. Ehhez biztosítani szükséges a személyek távoli azonosítását, a hitelességet és a letagadhatatlanságot.

2.1.1. Aszimmetrikus kulcspárok

felhasználási lehetőségek

A Megbízó által átadott dokumentumok, valamint a személyes megbeszélések alapján egyértelműnek látszik, hogy az elérendő célok mindenképpen szükségessé teszik az állampolgárok asszimetrikus kulcspárokkal való ellátását, valamint ezzel együtt egy hitelesítő szolgáltatás felállítását. Így valósítható meg ugyanis a lehető legtágabb körben az elektronikus ügyintézés (a feladó állampolgár aláírókulcsával elektronikusan aláírt dokumentumok), így kommunikálhatnak a hivatalok biztonságosan az állampolgárral (a címzett állampolgár nyilvános kulcsával titkosított dokumentumok, határozatok, idézések, hivatalos levelek, stb.), és ez szükségeltetik ahhoz is, hogy az állampolgár számára adat-letéti szolgáltatást nyújtson az állam úgy, hogy az ott elhelyezett adatokhoz kizárólag az férjen hozzá, aki ott azt elhelyezte (titkosítás saját titkos kulccsal).

Mindezek alapján az átadott dokumentumokban több helyen előfordul az aláíró/titkosító kulcspárral való ellátás ötlete, amely informatikai szempontból könnyen megvalósítható, a hitelesítés (személyazonosítás, a kulcspár és a személy összetartozásának tanúsítása) pedig az ügyfélkapu-nyitáshoz hasonlóan megoldható lenne az okmányirodákban.

A kulcspár (akár aláírásra, akár titkos kommunikációra használatos), annak is a nyilvános része, azonban könnyen válhat (egy a korábbinál sokkal hosszabb és bonyolultabb) személyi számmá, olyan azonosítóvá, amely a magyar alkotmányos keretek között nem megengedett. Kiosztásakor és használatakor ezért arra kell törekedni, hogy ne rendelkezzen azokkal a jellemzőkkel, amelyekkel az 1991-ben alkotmányellenesnek minősített személyi szám rendelkezett, ne le legyen tehát minden állampolgárnak és országlakosnak ugyanazon elv szerint kiosztott, tehát *egységes* karaktersor, amely *univerzális*, sokcélú azonosításra alkalmas, vagyis amelyet elvileg mindenféle nyilvántartásban használni lehet.

a nyilvános kulcs mint univerzális azonosító

A két attribútum, az egységesség és az univerzalitás együttesen tilos, az egységes azonosító azonban alkotmányosan megengedett (ilyenek a ma használatos szakazonosítók, céljuk, hogy ugyanarra a személyre vonatkozó adatokat könnyen és biztosan lehessen azonosítani, illetve összegyűjteni egy olyan rövid, technikailag könnyen kezelhető karaktersor segítségével, amely megváltoztathatatlan és összecserélhetetlen). Alkotmányosan akkor aggályos az egységes azonosító, ha univerzális is egyben, mert többek között ettől alkalmas a különböző nyilvántartásokban fellelhető személyes adatok eseti összekapcsolására. Segítségével az adatok könnyen hozzáférhetőek, valamint kölcsönösen ellenőrizhetőek. Ezek az előnyök a személyiségi jogok, s különösen az információs önrendelkezéshez való jog szempontjából súlyos kockázatot jelentenek. A legtávolabb eső, különböző célú nyilvántartásokból összeszedett adatokból előállítható az úgynevezett személyiségprofil, az érintett tetszőlegesen széles tevékenységi körére kiterjedő és intimszférájába is behatoló művi kép, amely ugyanakkor az adatok kontextusból kiragadott volta miatt nagy valószínűséggel torz is. Az adatkezelő mégis ennek alapján hozza meg döntéseit, állít elő és ad tovább újabb személyre vonatkozó információkat. A nagymennyiségű összekapcsolt adat, amelyről az érintett legtöbbször nem is tud, kiszolgáltatja az érintettet, egyenlőtlen kommunikációs helyzeteket hoz létre, amelyben az egyik fél nem tudhatja, hogy partnere milyen információkkal rendelkezik róla. A személyi számmal

egységes azonosító önmagában nem tilos…

… de ha univerzális is egyben, az profilképzés alapjául szolgálhat

dolgozó államigazgatás hatalma így mértéktelenül megnő. Ha pedig a személyi számot az állami szférán kívül is használhatják, ez nemcsak az ottani adatkezelőknek ad az érintett felett hatalmat, hanem az állam további hatalomnövekedéséhez vezet: még messzebbre terjeszti ki az adatokon keresztüli ellenőrzés lehetőségét. A korlátozás nélkül használható személyi szám így a totális ellenőrzés eszközévé válhat. [Lásd bővebben: 15/1991. (IV. 13.) AB határozat, ABH 1991, 51.]

Az aláíró/titkosító kulcspárok tehát nem lehetnek ilyenek. Nem lehetnek

konjunktív negatív feltételek

- egységesek, azaz minden országlakosnak egyazon elv szerint kiosztottak (egyazon algoritmus alapján képzettek, megváltoztathatatlanok és összecserélhetetlenek, ideértve a mindenkinek kiosztott véletlen számokat is), és ezzel egyidejűleg
- univerzálisak, azaz korlátlanul használhatóak.

Ennek a következő követelmények figyelembe vételével lehet eleget tenni:

1. A közigazgatási célra az állam által adott kulcspár nem lehet kizárólagos, vagyis nem írható elő, hogy a polgár ezt és csak ezt a kulcspárt használhatja a közigazgatási szervekkel folytatott kommunikációja során. A piaci szereplő hitelesítés-szolgáltatók által nyújtott, hasonló biztonsági fokozatú aláírást is el kell fogadni. Ez a Megbízó által is hangsúlyozott garancia azonban csak szűk körben biztosít védelmet az azonosító univerzálissá válásával szemben, ugyanis nem várható, hogy a polgárok nagy tömegben fognak alternatív aláírásokat a közeljövőben beszerezni, eddig sem tették, és különösen így lesz ez akkor, ha az állam ingyenesen biztosít a számukra egyet. Ennek ellenére ez egy fontos garancia.

kerülendő a kizárólagosság

2. A közigazgatási célú aláíró kulcspár használatát – bármilyen vonzó lenne ennek ellenkezője – ki kell zárni a nem közigazgatási szervekkel folytatott kommunikációban. A kulcspár ugyanis később könnyen válhatna univerzális, a polgár sokféle életviszonyában használatos azonosítóvá, adatok összekapcsolásának, így személyiségprofil létrehozásának eszközévé. A különböző célú adatkezelések között

kerülendő a nem közigazgatási használat

egyfajta állandó kapcsolati kódként funkcionálna. Ezt a közigazgatás és a piaci szolgáltatások között legalábbis ilyen szigorú szabállyal lehet kizárni.

3. Időben korlátozni kell a kulcspár érvényességét. Ahogy a mai ügyfélkapu sem korlátlan ideig érvényes, úgy a kulcspár érvényességét is limitálni kell, mégpedig úgy, hogy az érvényesség nem meghosszabbítható, minden lejáratkor új kulcspárt kell kiosztani. Ez időben teszi – egy bizonyos mértékben – nehezebbé a nem megengedett adat-összekapcsolást, profilépítést.

korlátozott érvényességi idő

4. További garanciát jelentene, ha nemcsak időben korlátoznák a kulcspár használatát, hanem horizontálisan (azaz szektorálisan) is, ami, ha minden szektorhoz külön kulcspár tartozik, némi kényelmetlenséget okoz az állampolgárnak, de nem teszi lehetetlenné az alkalmazást, ezért csak mint legjobb gyakorlatot említjük. A kényelmetlenséget kiküszöbölő megoldás, amivel ugyanez a cél elérhető, úgy képzelhető el, hogy a polgárnál lévő egyetlen kulcs több „zárba illik", ahhoz több nyilvános kulcs tartozik, amelyek közül különbözőeket kell használni közigazgatási szektoronként. Hogy matematikailag, illetve informatikailag ez lehetséges-e, arról nincs tudomásunk, ugyanakkor a modellt vizsgálatra érdemesnek tartjuk. A kulccsal visszaélni így csak akkor lehet, ha a polgártól ellopják a személyazonosítóval együtt (azaz ha a tolvaj tudja, kié). A másik (a közigazgatási szerv) oldalán szektoronként más és más karaktersor lenne eszerint a kulcs, így ugyan feltehetően könnyebben törhető fel, mint a szigorúan egy-egy kulcsból álló kulcspárok használata esetén, de ez az alacsonyabb biztonsági szint igazodhat ahhoz, mennyire szenzitív az adott ügy vagy nyilvántartás. Ez tehát egy további garancia lehet az univerzalitással szemben, matematikai, illetve informatikai megvalósíthatóságáról nincsenek ismereteink, ám az egy kulcs több zár koncepciót továbbgondolva esetleg eljuthatunk a szektorális azonosítók megszüntetésének gondolatáig is.

horizontális korlátozás

egy kulcs - több zár

5. Jogi eszközökkel ki kell zárni azt, hogy (az egy nyilvános és egy titkos kulcsból álló kulcspárokhoz visszatérve) az egyes közigazgatási nyilvántartások a kulcspár nyilvános részét elszakítva eredeti funkciójától, azonosító jelként kezdjék használni. Nem lehet tehát az egyes nyilvántartások rekordjait, az egyes állampolgárokat megjelölő azonosító a nyilvános kulcs. Meg kell őrizni a szakazonosítók jelenlegi rendszerét, a különböző szakazonosítókat használó szervek csak a jelenlegi jogi keretek között, kapcsolati kód (lásd az 1.2. pontban) segítségével kapcsolhatnak össze adatokat, nem lehet az összekapcsolást a mindkét nyilvántartásban megőrzött kulccsal megkönnyíteni. Adott esetben meg kell tiltani a nyilvános kulcsok megőrzését az egyes nyilvántartásokban, azt csak funkciójuknak megfelelően, az azzal összefüggő mértékben szabad kezelni, nevezetesen a nyilvános kulcstárból csak az aláírt üzenet kicsomagolásának idejére, a polgárnak címzett üzenet titkosításának idejére lehet letölteni, utána törölni kell. Erre nézve jogi kötelezettséget kell alkotni. A szerveknek maguknak naplózniuk kell a kulcstárból történő letöltéseket és a törlés tényét, a naplófájlokat pedig ellenőrizhetővé kell tenni (többek között az adatvédelmi biztos számára).

nyilvántartások azonosítója nem lehet a nyilvános kulcs

célhozkötött felhasználás

a felhasználás ellenőrizhetősége

6. Abban az esetben, ha a kulcsokat az adatalanyok adatainak felhasználásával képzik (léteznek ilyen eljárások, az elektronikus aláírás ma használatos módszerei nem ezeket alkalmazzák), akkor csak egyirányú algoritmusokkal szabad képezni, úgy, hogy azokat visszaalakítani, a képzéshez használt adatokat újból előállítani a kulcsból ne lehessen. Az erre használható algoritmusokat rögzíteni kell, a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről szóló 2/2002. (IV. 26.) MeHVM irányelv mellékletében foglaltakhoz hasonlóan. Ezzel egyenértékű megoldás az elektronikus aláírásoknál ma használt módszer, amely esetén a kulcspárokat véletlenszerűen generált nagy prímszámok származékaiként hozzák létre, amelyekből semmilyen további adat nem derül ki

a kulcs nem lehet „beszédes adat”

7. Abban az esetben, ha alkalmazásra kerülnek a 2.1.2. pontban említett egyszeri használatra generált azonosítók, amelyek a polgár tudta nélkül kerülnek a gépére és kerülnek visszaküldésre a jognyilatkozattal együtt, akkor az aláíró kulcspár mellett egy másik kulcspárra is szükség van, amely tanúsítványa szerint személyazonosításra alkalmas ugyan, de használata nem jár az aláírással azonos jogkövetkezményekkel. A polgár ugyanis ebben az esetben olyan jognyilatkozatot tenne, amely tartalmaz olyan adatot, amit nem is lát, tartalmát nem befolyásolhatja, ez pedig igen nagy biztonsági rést nyitna a rendszeren. Ha tehát olyan alkalmazások kerülnek kidolgozásra, amelyekben a polgárok által nem kontrollált adatok kommunikációja is folyik, az aláíró kulcspár mellett ki kell osztani egy csupán azonosításra szolgáló kulcspárt is, ahogy ezt más országokban is tették.

az aláírás jogkövetkezményeivel nem járó külön azonosító kulcs

A fenti követelmények részben a célhozkötöttség elvére vezethetők vissza, nevezetesen arra, hogy az aláíró kulcspár kizárólag aláírásra legyen használatos, más természetű azonosításra nem, a titkosításra szolgáló kulcspárral pedig a polgárral folytatott kommunikáció biztonságát, valamint a saját részre történő titkosítást lehet megoldani, az azonosító kulcspár pedig arra jó, hogy a polgár ne tehessen olyan jognyilatkozatot, amely tartalmát nem ismeri, saját adatai felett kontrollt tudjon gyakorolni, mégis azonosítható legyen. A kulcspár(ok)kal való ellátás az elérhető céloknak csupán egy részére nyújt tehát megoldást, önmagában kevés az elektronikus ügyintézés, a jognyilatkozatának letagadhatatlansága problémáinak megoldásához. A megfelelő biztonságú azonosítást csak egyszer használatos azonosító kódokkal lehet megoldani, amellyel a következőkben foglalkozunk, az itt leírt feltételeket ezért a következőkkel együtt kell figyelembe venni.

2.1.2. Egyszer használatos jelszók és azonosítók használata

A megismert elképzelések között találkoztunk olyannal, amely az elektronikus kommunikáció hitelességét egy további – az elektronikus

bankok esetében megismert – módszerrel is biztosítanák. Ennek lényege, hogy az ügyfél által kezdeményezett elektronikus tranzakció érvényességéhez szükséges az is, hogy egy másik csatornán (például mobiltelefonon) keresztül küldött, a szervnél az adott állampolgárral ideiglenesen összerendelt egyszer használatos jelszót is helyesen megadjon. Az ismertetett megoldást csak mintegy kiegészítő biztosítékként, költségtérítés fejében biztosítanák az állampolgárok számára.

másik csatornán küldött egyszer használatos jelszó

E megoldás adatvédelmi szempontból előnyös és hátrányos is egyben. Álláspontunk szerint azonban a hátrány kisebb súlyú az elérhető eredményhez képest, ezért megvalósítását – az aláíró kulcsok alkalmazásával együtt – javasoljuk. Az adatvédelmi hátrányt az jelenti, hogy a közigazgatási szervnek ismernie kell az ügyfélnek egy további elérhetőségi adatát ehhez az eljáráshoz, például a mobiltelefon számát. Lehet arra számítani, hogy sok állampolgár kifogásolná a mobiltelefon-száma kötelező megadását az elektronikus ügyintézéshez. (Nem adatvédelmi természetű hátrány, de figyelembe veendő, hogy ezzel elesnek a távoli ügyintézés lehetőségétől azok, akiknek nincs mobiltelefonjuk, illetve, hogy a szöveges üzenetküldés pénzbe kerül.) A módszer adatvédelmi természetű előnye, hogy tudatos állampolgári magatartást feltételez. A polgárok igen könnyen kattintanak az „elküld” gombra, figyelmüket az internetes oldalakon sok betöltődő elem elvonhatja, ám ha egy rövid szöveges üzenetben érkező jelszót is külön meg kell adniuk, meggondolják, mit is tesznek éppen. Ez a hozzájárulás érvényességéhez szükséges határozottságot és tájékozottságot növeli.

további adat kezelését feltételezi

állampolgár tudatos döntésének egy lehetséges biztosítéka

Nem tartjuk ugyanakkor jó megoldásnak, hogy ez csak mintegy emelt szintű szolgáltatásként kerüljön bevezetésre, külön díj ellenében. Ha a közigazgatás – részben saját kényelme, a költségvetés kímélése érdekében – arra ösztönzi az állampolgárokat, hogy elektronikusan intézzék ügyeiket, az elektronikus kommunikáció hitelessége és biztonsága tekintetében mindent szükséges intézkedést meg kell tennie. A közigazgatásban – szemben a piaci szolgáltatókkal – nem történhet meg az, hogy aki hajlandó az emelt szintű szolgáltatásért fizetni, annak a kommunikációja biztonságosabb lesz, az ilyen

alapszolgáltatásként kell biztosítani, ha bevezetik

polgárok által küldött jognyilatkozatok hitelességének szintje magasabb lesz, akik pedig nem fizetnek, azokéval szemben bizalmatlanabb lesz az állam. A szöveges üzenetküldés költségei egyébként nyilván elenyésznek a hagyományos, nem elektronikus ügyintézés ember- és eszközigényének költségeihez képest.

Arra azonban lehetőség van, hogy egyes szolgáltatások, ügytípusok esetében ne kerüljön egyszer használatos jelszó kiküldésre, azok esetében, amelyek nem annyira érzékeny viszonyokat érintenek, ennélfogva oly nagy mértékű hitelesség és állampolgári tudatosság nem is megkövetelendő. Ehhez egyenként értékelni kell az egyes szolgáltatásokat, és dönteni kell arról, melyeknél vezetik be a külön csatornán küldött egyszer használatos jelszó használatát, és melyeknél nem.

egyszeri használatra generált azonosító

A fentitől eltérő egyszer használatos kód segítségével történő azonosítás bevezethetőségének lehetősége is felmerült. E megoldás logikáját tekintve hasonlít a később (2.3.3. pont) tárgyalandó egyszer használatos kapcsolati kód alkalmazásához a közigazgatás szervei közötti adatintegráció folyamatában, ám míg ott szervek közötti kommunikációban alkalmaznák, addig itt a polgár és a közigazgatási szerv közötti kommunikáció biztosítéka lenne.

a művelet lépései

E szerint az állampolgár egyfelől saját kulcsait használja aláírásra, másfelől ezzel egyidejűleg egy egyetlen alkalommal használt azonosítót. Lépései a következők: A közigazgatási szerv egy véletlen elemet tartalmazó kapcsolati kódot generál, azt elküldi az állampolgárnak, átmenetileg összekapcsolja saját nyilvántartásában ezt az egyszer használatos azonosítót az érintett személy nyilvántartott személyazonosító adataival. Az állampolgár pedig a jognyilatkozatát, beadványát, stb. e kóddal együtt aláírva küldené vissza a közigazgatási szervnek, így az tudná, hogy a beérkező dokumentum attól származik, akinek az egyszer használatos azonosítót korábban kiküldte, úgy, hogy az általa generált egyszer használatos azonosító segítségével a megkapott beadványt hozzárendeli a saját nyilvántartásában az érintett

személyhez. Az állampolgár számára a folyamat nem lenne ellenőrizhető, hiszen az egyszer használatos azonosító (valójában kulcs) hosszú, értelmezhetetlen karakterlánc, a műveletet a számítógépén futó kliens végezné. Ennek az egyszer használatos „kapcsolati kódnak" a nagyobb biztonságot nyújtó változata az, ha a hivatal nem csupán egy kapcsolati kódot generál, hanem egy egyszer használatos *szimmetrikus* kulcsot küld el ily módon az ügyfélnek. Az ügyfél ezzel az egyszer használatos szimmetrikus kulccsal titkosítja ügyiratát vagy üzenetét, majd a titkosított üzenetet saját magánkulcsával aláírva küldi el a hivatalnak. A hivatal az ügyfél nyilvános kulcsával kinyitja az üzenetet, benne találja az egyszer használatos szimmetrikus kulccsal titkosított ügyiratot, de mivel ezt a szimmetrikus kulcsot éppen ő generálta, ki tudja nyitni, és egyben ellenőrizni is tudja, hogy valóban az használta, akinek kiküldte. A szimmetrikus kulcsot ezután mindkét fél rendszere törli.

profilalkotásra alkalmas azonosító nem jön létre

E megoldás úgy oldja meg a személyazonosítás kérdését, hogy egyúttal nem hoz létre egy új, profilalkotásra alkalmas azonosítót, mert minden alkalommal új azonosítót kell generálni. Hátránya azonban, hogy a művelet a háttérben történik, az adatalany nem lehet rá hatással, és nem tudja ellenőrizni, hogy az egyszer használatos azonosító valóban attól a szervtől érkezett, amelyiktől várta. E megoldás nem rendelkezik azzal az előnnyel, amellyel a külön csatornán érkező egyszer használatos jelszó megadása igen: nevezetesen nem teszi tudatosabbá az állampolgár magatartását, inkább megkíméli őt, kényelmesebbé teszi az eljárást.

az adatalany nem tudja kontrollálni

azonosító kulcsok alkalmazásával valósítható meg

Álláspontunk szerint nem biztonságos a rendszer akkor, ha nem társul hozzá egy állandó, az aláíró kulcstól független kulcs használata az állampolgár részéről. Az állampolgár ugyanis itt részben olyan adatot (az egyszer használatos azonosítót) is aláírna, amely felett nincs semmiféle kontrollja, ezért gondolni kell arra, hogy ennek az aláírásnak nem lehet ugyanaz a jogi következménye, mint az aláírt dokumentumoknak. E megoldás ezért csak egy olyan kulcspár alkalmazásával oldható meg, amelynek jogi hatása nem felel meg az elektronikus aláírásával, csupán a személy azonosítására

szolgál. (Lásd még az aszimmetrikus kulcspárokról szóló 2.1.1. pont alatt ismertetett 7. számú észrevételt az 56. oldalon.)

A fent vázolt két megoldás közül az előzőt javasoljuk megvalósítani.

2.1.3. Idegen azonosítás, viszontazonosítás igénybevétele

A Megbízó által feltett kérdések között – a „Kapcsolódó további kérdéskörök" kategóriájában – szerepelt az az elképzelés, amely szerint a bankkártyák használhatóak lennének a közigazgatásban alkalmazott ügyfélkapus azonosítás megerősítésére, viszontazonosítás jelleggel. (Megjegyezzük, hogy a viszontazonosítás kifejezést – a háttéranyagok szóhasználatát követve – e helyütt nem a Ket.-ben meghatározott értelmében használjuk, hanem a közigazgatástól független azonosító rendszerek bevonását értjük alatta.) Ez a koncepció is több helyütt felvetődött a háttéranyagokban, illetve a személyes konzultációk során, egyfelől a viszontazonosítás jellegű szolgáltatást nyújtó szervezetek körének bővítésével (például mobilszolgáltatók), másfelől általános szinten, az idegen azonosítás elfogadásának problémakörében.

a külső azonosítás igénybevételének szükségessége

Értelmezésünk szerint egy ilyen azonosítás-megerősítésnek csak az ügyfélkapu „gyenge" (nem elektronikus aláírás alapú) azonosítása esetén lenne értelme. Ha ugyanis az ügyfélkapu egy olyan hitelesítésszolgáltató tanúsítványára alapozza az azonosítást, amelynek a személyazonosítási alapja a központi személyiadat- és lakcímnyilvántartás, akkor minden komolyabb hitelesítésszolgáltató ezzel a központi nyilvántartással kér adategyeztetést a személyazonosító adatok helyessége tekintetében. Vagyis ilyen esetben (ha az ügyfélkapu kételkedik a hitelesítésszolgáltatónál rendelkezésre álló személyes adatok pontosságában), akkor a központi nyilvántartáshoz mint etalonhoz kellene fordulnia, nem pedig egy másodlagos adatkezelőhöz. De egyébként is abszurd szituációt jelentene, ha valaki a hitelesítésszolgáltató adatainak hitelességében kételkedne.

Amennyiben nem a természetes személyazonosító adatok pontosságában „kételkedik” az ügyfélkapu, hanem a személy és az önmagában pontos személyazonosító adatok összetartozásában, akkor valóban indokolt lehet külső azonosítás-megerősítés igénybevétele. Ennek jogszerűségéhez és az adatvédelmi követelményeknek való megfelelőségéhez szükséges az alábbi feltételek teljesülése:

1. Az azonosítás-megerősítés (viszontazonosítás) az üzleti szektor adatkezelőinek közreműködésével nem lehet kötelező eleme a közigazgatási ügyfélkapcsolatnak, illetve ügyintézésnek. Ennek egyik alapvető oka az, hogy nincs mindenkinek bankkártyája vagy mobiltelefonja, de nem is lehet arra kényszeríteni mindenkit, hogy legyen. Más szóval, nem lehet az ügyfeleket arra kényszeríteni, hogy egyik vagy másik szolgáltatóval jogviszonyban álljanak.

   nem lehet egyetlen módszert kötelezővé tenni

2. Amennyiben a közigazgatási ügyfélkapcsolat egyes területein, különösen online ügyintézés esetén (és a „gyenge” azonosítás továbbélése esetén) a viszontazonosítás kötelező lenne, akkor a viszontazonosítást nyújtó szolgáltatások széles körét – közüzemek, távközlő szervezetek, bankok stb. – kellene elfogadnia a közigazgatásnak, az ügyfélre bízva, hogy melyik szolgáltató azonosítás-megerősítésére kíván támaszkodni.

   több szolgáltatóval párhuzamosan kiépítendő a rendszer

3. Az azonosítás-megerősítés csakis és kizárólag az adatok teljes egyezőségére, illetve nem egyezőségére vonatkozó, igen/nem válasz lehet a viszontazonosítást végző szolgáltató részéről.

   igen/nem (egyezik/nem egyezik) típusú válasz

4. Biztosítani kell azt, hogy a viszontazonosítást kérő adatkezelő és az azt nyújtó adatkezelő között csak a fenti igen/nem válasz megadásához elengedhetetlenül szükséges adatok kerüljenek továbbításra. Ennek egyik adatvédelmi szempontból előnyös megvalósítási formája lehet, ha az adatalany maga jelentkezik be elektronikus úton a viszontazonosító adatkezelőnél (banknál) és a közigazgatáshoz már csak az azonosítás megtörténtét jelentő válasz érkezik meg.

   az azonosítás nem a közigazgatás, hanem a külső szolgáltató felületén

5. Tekintettel arra, hogy a személyes adatokra vonatkozó egyezik/nem egyezik válasz maga is személyes adat, ennek továbbítását a banknak vagy más viszontazonosítónak naplóznia kell és meg kell őriznie. Hasonlóképpen naplóznia kell az azonosítás-megerősítést kérő szervnek is a viszontazonosítás kérésére és megtörténtére vonatkozó adatokat. A napló adattartalmának azonban csak az esetleges későbbi ellenőrzés vagy jogorvoslat céljaihoz elengedhetetlenül szükséges adatkörre kell korlátozódnia, ami a célhozkötöttség követelményéből is következik.

naplózás az ellenőrzés céljaira

6. Biztosítani kell, hogy a viszontazonosítási szolgáltatást nyújtó szervezet ne köthesse össze az adatalany egyéb adataival azt, hogy milyen adatkezelőtől, milyen gyakorisággal érkeztek adategyeztetési kérések. Ebből a szempontból előnyös megoldás, ha az ügyfélkapu az adatalany által kezdeményezett ügytípustól és az ügyben érintett közigazgatási adatkezelő személyétől függetlenül egységes felületként áll szemben a viszontazonosítást nyújtó külső szolgáltatóval.

profilépítés kizárása a külső szolgáltató oldalán

2.2. Az adatokat hordozó és a személyazonosítást lehetővé tevő azonosító kártyák

kitűzött célok

Az e-Közigazgatási stratégia kimondja, hogy állampolgári azonosító eszközök esetén az elektronikus úton, távollévők közötti ügyintézés esetén elengedhetetlen az állampolgárok megbízható azonosítása, az állampolgárok adatainak elérésének biztosítása, a hiteles és letagadhatatlan kommunikáció. A cél olyan egységesen szabályozott állampolgári közmű-rendszer kialakítása, ahol konzisztens módon valósul meg a szereplők azonosítása, a rendszerben kezelt, tárolt adatok, információk és dokumentumok megváltoztathatatlansága és bizalmassága, a végzett műveletek letagadhatatlansága. Az azonosító eszköznek és a hozzá kapcsolódó azonosítási rendszernek biztosítania kell, hogy a magyar állampolgárok igénybe tudják venni az European Citizen Card szabványban rögzített és opcionális funkcióit, és az EU tagállamok állampolgárai Magyarországon is használhassák az ECC szabványokra épülő nemzeti elektronikus személyazonosságot igazoló kártyáikat.

egymással összefüggő célok

A Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az elektronikus kormányzat társadalom egészének javára történő létrehozásának felgyorsításáról szóló, i2010 eGovernment című cselekvési tervre kiadott bizottsági közlemény (COM(2006) 173) szerint a cél a határokon átívelő közszolgáltatások használatának biztosítása az Európai Unión belül. Ehhez természetesen nem csak a személyazonosító igazolványok kölcsönös elismerését és az adatok Unión belüli áramlását kell tudni biztosítani, hanem az elektronikus aláírások kölcsönös elismerését és interoperabilitását is. (Az Unión belüli azonosításról lásd a „A Roadmap for a pan-European eIDM Framework by 2010” dokumentumot.)

több szakazonosító egy kártyán: a törvény kizárja

A Szaz. szabályaiból az következik, hogy egyetlen kártya a jelenlegi keretek között nem tartalmazhatja több kártya adatait. A Megbízó által átadott háttéranyagok azonban többféle módon felvetik az egyetlen kártyán tárolt

szakazonosítók, ennek megfelelően egyetlen kártya több célra történő felhasználásának lehetőségét. A továbbiakban áttekintjük a kártyák összevonásának lehetőségét. Az egy kártyás megoldás olyan horderejű módosítást jelent: jogalkotási, rendszertervezési és fejlesztési feladattal jár, hogy mindenképpen célszerű előzetes hatásvizsgálattal alátámasztani. Szükséges felmérni, hogy mekkora az igény az egykártyás rendszerre, a költség haszon arány hogyan állítható fel a kártya kibocsátásának, a rendszerek átalakításának és az adminisztráció csökkenésének összefüggésében. Az osztrák azonosítási rendszer átalakításánál is egységes kártyakoncepciótól kiindulva jutottak el a jelenlegi megoldáshoz, az univerzális kártyától a többfunkciós kártyáig. (Erről lásd az 1.3.2. pontot.) Fontosnak tartjuk, hogy a koncepció kialakítása során a külföldi példák és a hazai attitűdök figyelembevétele is megtörténjen.

univerzális vs. többfunkciós kártyák

A következőkben elsőként az azonosító kártyák témában született elképzelések adatvédelmi szempontból releváns elemeit funkcionális megközelítésben vizsgáljuk (erről szólnak a 2.2.1.-tól a 2.2.4. számú szakaszok), majd ezt követően a kártyák tartalmát és „létformáját" technológiai megközelítésben elemezzük (2.2.5-2.2.7. számú fejezetek).

funkcionális és technológiai megközelítés

2.2.1. Univerzális kártya kiadása

Az elektronikus azonosításra szolgáló univerzális azonosító kártyára vonatkozó tervek már korábban is ismertek voltak. Ezek közül az előző parlamenti ciklusban T/3735 számon benyújtott, az Avtv. módosításáról szóló törvényjavaslat eredeti változatának 21. § (2) bekezdése egy univerzális vagy többfunkciós kártya bevezetésére vonatkozó javaslatot tartalmazott, amely szerint a szakazonosítókat és a természetes azonosítókat egyetlen kártyán helyezték volna el: „A polgár részére - kérelmére - megfelelő biztonsági rendszerrel ellátott azonosító kártya is kiadható, amely természetes személyazonosító adatait és azonosító kódjait tartalmazza. Az azonosító kártyát úgy kell kialakítani, hogy adattartalmából az adatkezelő csak azokat az adatokat és azonosító kódokat ismerhesse meg, amelyek

minden azonosító egy kártyán

kezelésére jogosult.” E rendelkezés végül nem került elfogadásra. Ennek oka, hogy a tervezet nem felelt meg sem a hazai adatvédelmi, sem az adatbiztonsági követelményeknek. De egy esetleges elfogadás esetén az Alkotmánybíróság a fent ismertetett határozatai alapján bizonyosan alkotmányellenesnek nyilvánította volna. Erre hívta fel az adatvédelmi biztos is a figyelmet (Lásd az adatvédelmi biztos 472/H/2003 és 1286/J/2003 számú aktáit.) Az egyetlen kártyával történő azonosítás lehetősége különböző műhelymunkák, koncepciók, stratégiák szintjén azonban továbbra is létezik. A fenti rendelkezés elutasításának indokai azonban ma is fennállnak, a szakazonosítóknak egyetlen kártyán történő elhelyezését ma ugyanazokkal az indokokkal utasítanák el, mint korábban.

sikertelen kísérlet

Az alábbiakban áttekintjük az univerzális kártya, azaz a jelenlegi természetes személyazonosító adatok és a szakazonosítók egyetlen kártyán történő tárolásának jogi megítélését.

A szakazonosítók egyetlen kártyán történő elhelyezésére vonatkozó tervezetek két fő okot szoktak megjelölni: az állampolgárok számára egyrészt kényelmesebb az egyetlen kártya, a közigazgatással való kapcsolattartás során másrészt pedig egyszerűsödik az eljárás, ha a közigazgatási szerv azt az adattartalmat ismerheti meg, amelyre szüksége van. (Jobb esetben hozzátéve, hogy természetesen nem túlterjeszkedve a szükséges adatokon.)

az univerzális kártya igényének indokai

A jelenleg használt szakazonosítók és a természetes személyazonosító adatok (esetleg ezek körének bővítésével: biometrikus adatok, üzleti szféra által kezelt adatok és azonosítók: ügyfélszám) egyetlen kártyán való tárolása több okból is aggályos – azon túlmenően is, hogy a fentiek szerint a Szaz. nem engedi meg. Aggályaink abban az esetben is fennállnak, ha az azonosítók különböző titkosítási módszerrel kerülnek elhelyezésre, úgy, hogy ahhoz nem férhet hozzá csak az,

az univerzális kártya aggályos

- aki rendelkezik a megfelelő kártyaolvasóval, és
- akinek a kártyaolvasást az érintett polgár megengedte.

1. Az univerzális kártya bevezetése esetén az adatok könnyen hozzáférhetővé válnak harmadik személyek számára. Nincs feltörhetetlen rendszer. Potenciális veszélyt jelent a kártya elvesztése vagy illetéktelen személyek által történő megszerzése. Az egyetlen kártya kényelme mellett figyelembe kell venni, hogy annak elvesztése esetén a pótlás is igen problémás lehet, hiszen az összes személyazonosításra alkalmas adat elvész. Emellett az identitáslopás veszélyét is magában hordozza. Az egyetlen kártya megszerzésével való visszaélés komoly kockázati tényező, mind az érintett, mind a közigazgatási szervek számára.

   jogosulatlan hozzáférés lehetősége egyszerre több adathoz

   Egy ilyen kártyából teljes személyiségprofil felállítható, különösen akkor, ha a közigazgatásban használt azonosítók mellett egyéb adatok is kártyára kerülnek, így könyvtári kölcsönzés, parkolási, behajtási engedély. Az univerzális kártya tartalmához való illetéktelen hozzáférés hasonlít arra az esetre, amelyben a mai, több különböző kártya párhuzamos használatakor valaki elveszítené azt a pénztárcáját, amelyben valamennyi kártyáját egyszerre tartja. Ez utóbbi esetben azonban saját döntése alapján tárolta egy helyen valamennyi kártyáját, vállalva ezzel annak kockázatát, hogy egyszerre veszíti el, juttatja illetéktelen kezekbe, míg az univerzális kártya esetében ez a választási lehetőség már nem áll nyitva számára, nincs is lehetősége ara, hogy külön tárolja a kártyáit.

2. Az egyetlen kártyás megoldás súlyosan veszélyezteti az érintett információs önrendelkezési jogát. Nem várható el ugyanis, hogy az érintettek minden esetben tudják, illetve érvényesíthessék, hogy az adatok közül melyikre van szükség, ezért feltehetően a későbbi hiánypótlás elkerülése érdekében hozzájárulnak minden, a kártyán tárolt adat kezeléséhez. Az emberek adatmegadási hajlandósága a számukra „virtuális”, még csak nem is látható, csak elektronikusan létező adataik esetében még nagyobb. A tapasztalatok szerint továbbá az emberek azon személyes adataikat, amelyek valamilyen módon tárgyiasulnak, sokkal inkább óvják, mint a számukra értéktelennek tűnő virtuális –

   korlátozott önrendelkezési jog

jelentéstartalom nélküli adatokat, mint amilyen társadalombiztosítási azonosító jel, vagy az adóazonosító. A szakazonosítók és egyéb, hatóság által kezelt adatok értéktelenebbnek tűnnek számukra, mint a természetes személyazonosító, vagy közvetlen kapcsolatot biztosító adatok. Egy fénykép (természetes azonosító) vagy egy személyes használatú mobilszám (közvetlen kapcsolat) kezeléséhez való hozzájárulás érthetőbb az adatvédelemben kevésbé jártas, az adatvédelmi kockázatokat kevéssé felmérő állampolgár számára is, és a magánszféra gyakorolt hatása számára is könnyűszerrel felmérhető, szemben egy matematikai algoritmussal készült szakazonosítóval. Természetesen a közigazgatás és az üzleti szféra szempontjából, éppen ezek az értéktelennek tartott adatok válhatnak nagyon fontossá az ügyfélprofil kialakítása során. Ezért kell hangsúlyozni, hogy az adatok kezeléséhez mindig az érintettek megalapozott döntése, informált beleegyezése kell. Ezért már itt is fontosnak tartjuk megjegyezni, hogy bármilyen új azonosítási rendszer kerül bevezetésre, az arra vonatkozó adatvédelmi tájékoztatást mindenképpen el kell végezni és azt több platformon is elérhetővé tenni.

veszélytelennek tűnő adatok és adatkezelések

a tájékoztatás elengedhetetlen

Az önrendelkezési jog gyakorlásának feltétele az érintett megfelelő tájékozottsága. Az Avtv. megkülönböztet előzetes és utólagos tájékoztatást. Az előzetes tájékoztatás (Avtv. 6. §) alatt azt értjük, hogy az adatkezeléshez való hozzájárulást megelőzően tájékoztatási kötelezettsége van az adatkezelőnek, annak érdekében, hogy az adatalany megalapozott döntés tudjon hozni adatai sorsát illetően. Az utólagos tájékoztatás alatt pedig azt értjük, hogy az érintett az adatkezelés bármely szakaszában érdeklődhet adatai sorsáról, az adatkezelő pedig ezt az igényét köteles kielégíteni (Avtv. 12. §)

tájékoztatás az Avtv.-ben

A tájékoztatásnak minden esetben egyértelműnek és érthetőnek kell lennie, ami azt is jelenti, hogy technikai és jogi ismeretek nélkül is értelmezhető tájékoztatást kel adni az adatalanyok számára. A tájékoztatásnak ki kell terjednie az adatok kezelésével kapcsolatos minden tényre, különösen az adatkezelés céljára és jogalapjára, az

a tájékoztatás tartalmi követelményei

adatkezelésre és az adatfeldolgozásra jogosult személyre, az adatkezelés időtartamára, illetve arra, hogy kik ismerhetik meg az adatokat. Az adattovábbítás esetén a fenntartott nyilvántartásra is. Emellett tájékoztatni kell az érintetteket a jogairól és jogorvoslati lehetőségeiről is. A tájékoztatásnak folyamatosan elérhetőnek kell lennie. Erre megfelelő a közigazgatási szerv honlapja, telefonos ügyfélszolgálata. Emellett természetesen a személyes kapcsolatfelvétel esetén a szóbeli tájékoztatás egyidejű biztosítása is fontos.

3. Az univerzális kártya lehetővé teszi a garanciális okokból egymástól elkülönítve felállított különböző célú nyilvántartások könnyűszerrel történő összekapcsolását. Általános az a gyakorlat a közigazgatásban és az üzleti szférában, hogy a célhozkötöttség és a jogalap konjunktív feltételét kizárólag a jogalap szempontjából vizsgálják. Az érintett hozzájárulása (jogalap) nem elegendő feltétel, a célhozkötött adatkezelést is meg kell, hogy valósítsa az adatkezelés. Ennek vizsgálatának hiányában egy hozzájáruló nyilatkozat kitöltésével összekapcsolhatóvá válnak a különböző adattartalmak.

adatösszekapcsolás lehetősége, mint fő ellenérv

A célhozkötöttség és a jogalap konjunktív feltételének alkalmazása az Avtv.-ből következik. A célhozkötöttségre vonatkozóan az Avtv. kimondja, hogy személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig. (Avtv. 5. §) Az adatkezelés jogalapját vagy az érintett hozzájárulása, vagy törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete alapozhatja meg. (Avtv. 3. §) A két szabálynak együttesen kell érvényesülnie: szükséges egy jogalap az adatkezeléshez, így vagy az érintett hozzájárulása vagy törvényi felhatalmazás és szükséges az is, hogy csak a meghatározott célból, az ahhoz

jogalap és célhozkötöttség: két konjunktív feltétel

elengedhetetlen adatmennyiség kerüljön kezelésre.

4. Profilírozás: Az adatokból könnyűszerrel összeállítható személyiségprofil, anélkül, hogy az érintett bármilyen befolyással lehetne arra, ez pedig alkotmányellenes. (Részletesebben lásd az 1.1.3. pont alatt.)

személyiségprofil kialakításának lehetősége

5. Az adatvédelmi biztos többször rámutatott az üzleti szféra adatéhségére. A szakazonosítók közül a pénzintézetek egyidejűleg több azonosítót is kezelnek: egy lakáshitellel kombinált életbiztosítás esetén valamennyi szakazonosítót elkérik, nem mindig tisztázott indokkal. A kiszolgáltatott helyzetben lévő emberek hozzájárulási készsége ezekben az esetekben jelentősen megnő. Mivel a jogtudatosság igen alacsony szintű, ezért nem várható, hogy az adatkezeléshez való hozzájárulást ne adnák meg az érintettetek, ha ettől a legminimálisabb előnyhöz jutnak. Itt jegyezzük meg, hogy ebben az esetben nem beszélhetünk jogszerű hozzájárulásról, hiszen az Avtv. azt mondja ki, hogy a hozzájárulás az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. (Avtv. 2. § 6.) A megfelelő tájékoztatás és az önkéntesség hiánya miatt nem érvényes a hozzájárulás, azonban nincs olyan eszköz, amellyel az adatkezelők adatéhségét ilyen alapon csökkentsék. A hozzájárulásra való hivatkozás, illetve annak érvénytelenségének bizonyítása lehetetlen vállalkozásnak tűnik.

nem érvényesül az önkéntesség elve

6. Az univerzális kártya megvalósíthatja az univerzális azonosítót. Nem lehet arra hivatkozni, hogy egyes adatok felhasználási köre más és más. Az egyetlen kártyán tárolt adatok olyan egységes és egyedi azonosítóvá válhatnak, amelyek súlyosan veszélyeztetik a személyes adatok védelmének alkotmányos alapjogát. Ennek elkerülése érdekében az univerzális kártya száma nem használható azonosító adatként, és a kártyán tárolt adatok bármilyen módon egységes adatbázisba rendezése is

univerzális kártya = univerzális azonosító

jogellenes. A kártyák használatának, az azon tárolt adatok kezelésének garanciáit a jogi szabályozás mellett technikailag is biztosítani kell.

A fentiek alapján kimondhatjuk, hogy a jelenlegi kártyák adattartalmának egyetlen kártyán való elhelyezése, illetve az összes kártya fizikai integrálása nem felel meg a személyes adatok védelmére kialakított adatvédelmi rendszernek. Ugyanakkor több egymástól független kártyának egy plasztikkártyán való elhelyezése megoldható úgy, hogy a személyes adatok védelmének szintje ne csorbuljon. Erről lásd a következőket.

2.2.2. Az állampolgárok ellátása egy többfunkciós kártyával

A többfunkciós kártyák közül különbséget kell tenni az azonosítási célú kártyák és az adattovábbításra, adattárolásra is alkalmas kártyák között. A kártyákra vonatkozóan különböző adatelhelyezési igények fogalmazódtak meg, azonban ezek közül egyik sem tekinthető kidolgozottnak. Az adatok elhelyezésére vonatkozó igény meghatározásához szükséges azok gazdasági, informatikai és jogi követelményrendszerének kialakítása.

általános megállapítások a többfunkciós kártyakoncepciókról

A jelenlegi háttéranyagokban szereplő megoldásokra az alábbi általános megállapításokat tudjuk tenni. Az egyes külön koncepciókban megjelenő különös észrevételekre ezek után térünk át.

szegmentált adattartalom

1. A kártyák adattartalmával összefüggésben megjegyezzük, hogy a kártya mindkét oldalának használata nyomtatott adatok megjelenítésére garanciális elemként jelenik meg a háttértanulmányokban. Ezzel kapcsolatban fontos hangsúlyozni, hogy a kártya adatokkal való feltöltése esetén az említett garancia csak akkor érvényesül, ha a kártyák, mint intelligens chip-kártyák tekintetében az olvashatóság szempontjából (fizikailag, illetve technikailag) szegmentált a kártya adattartalma. A kártyák kialakítása során fontos, hogy azokon csak a kártya funkciójának, a kártyával elérni kívánt célhoz szükséges adatok rögzítésére kerüljön sor, illetőleg az egyes felhasználásokkor, kizárólag az adott cél

eléréséhez szükséges adatok legyenek leolvashatók a kártyáról. Minden további, a törvény által nem előírt adat elhelyezéséhez az érintett – különleges adat esetén írásbeli – hozzájárulása szükséges. Az egyes technikai megoldások, ezeken belül például a mikrofizetésekhez használható elektronikus pénztárcaként történő használat, nem lehet kötelező. Azonban a több chip vagy szegmentált chip elhelyezése jelentős többletterhet ró a kibocsátóra, ezért szükséges hatásvizsgálatot végezni arra vonatkozóan, hogy valóban van-e igény ilyen jellegű alkalmazásra. A külföldi példák azt mutatják, hogy a többfunkciós kártya használata jóval elmarad az eredeti feltételezésektől (Ausztria, Észtország, Portugália). Az univerzális kártyákkal kapcsolatos azon ellenvetések, amelyek abból fakadnak, hogy egy plasztikkártyára kerülnek az információk/több chipen tárolt információk, igaz szűkebb körben, itt is fennállnak.

2. Az összevont, többfunkciós kártya, bármilyen minimális adattartalommal legyen feltöltve, a jelenlegi alkotmányos keretek között csak abban az esetben jogszerű, ha annak kiváltása és használata nem kötelező. Az ilyen kártyák önkéntes kiváltására való ösztönző mechanizmusok (kedvezmény, illetékmentesség) nem jelent automatikusan megoldást, mert ez a koncepció valójában sokszor nem felel meg az önkéntesség követelményének, csak látszat-önkéntességet jelent, hiszen olyan gazdasági előnyt helyez kilátásba, amelynek hatására a polgárok valójában nem az adataik sorsáról, hanem arról döntenének, hogy drágábban vagy olcsóbban jutnak a kártyához. Hozzájárulásuk ennélfogva nem lenne önkéntes, azt egzisztenciális kényszer vagy gazdasági előnyök hatása alatt hoznák meg. A nem önkéntes hozzájárulás pedig nem lehet az adatkezelés jogalapja. Ez a piaci alapú megközelítés a közigazgatásban tehát nem elfogadható. Más a helyzet az adattárolást lehetővé tevő technikai megoldásokkal. Üres chipeket el lehet helyezni a kártyán, annak adatokkal való feltöltésére vonatkozóan az érintett hozzájárulása szükséges, a hozzájárulást megfelelően, írásban dokumentálni szükséges. Ez pedig igencsak megnöveli a kártya-

önkéntes kiváltás

előállításának költségeit és bonyolulttá teszi használatának folyamatát.

3. A kártya kiváltására vonatkozó ösztönzők rendszerének kialakítása során figyelembe kell venni, hogy csak olyan rendszer kialakítása jogszerű, amely biztosítja az érintett számára a választási lehetőséget. Ezért javaslatunk az, hogy a kedvezményeket az adatvédelem szempontjait messzemenőkig figyelembe vevő megoldásokra alkalmazzák, így az elektronikus aláírásra is. A többfunkciós kártya esetén a kényelmi szempontok miatt a többletköltségek megtérítése kérhető az állampolgároktól.

választási lehetőségek

4. A kártya kialakítása során két eltérő megoldás képzelhető el: vagy a kártya maga tartalmazza az adatokat, vagy olyan kártyáról van szó, amely önmagában csak az azonosítást teszi lehetővé, és amely így a központilag nyilvántartott adatbázisból való lekérdezésre ad lehetőséget. A kártyán elhelyezett adatok megismerésének jogát a kártyabirtokosok számára biztosítani kell. Nem elégséges tehát chipen a kártyatulajdonos számára megismerhetetlenül tárolni az adatokat, még akkor sem, ha a kártya esetleges elvesztése, illetéktelen személyek által történő megszerzése esetén az adatvédelmi kockázat kisebb mértékű.

adatok a kártyán – adatok a központi nyilvántartásban

Álláspontunk szerint jogszerűen kialakítható olyan megoldás, amely szerint a többfunkciós kártya a jelenleg azonosításra használt kártya adattartalmán túl kizárólag azokat a kulcsokat tárolja, amelyek a központi nyilvántartásokban már szereplő adatoknak a polgár általi lekéréséhez ad hozzáférést. Ebben az esetben a hatóság tárolja az érintettek nyilvános kulcsait, és ő maga rendeli hozzá a személyazonosító adataikat. Az érintett nyilvános kulcsával kódolt azonosítást csak az érintett (illetve a kártyát olvasó szerv vagy személy pl.: orvos) a kártya birtokában tudja elolvasni, mivel az tárolja a titkos kulcsárt.

5. Mint fentebb kifejtettük, a kártyán a többletadatok elhelyezéséhez és az azon tárolt adatok megismeréséhez az érintett informált beleegyezése

szükséges. Az informált beleegyezés módja lehet az, ha a polgár aktív magatartással, a kártya átadásán túl is további személyes közreműködést hajt végre: például megadja az olvasáshoz szükséges kulcsot, jelszót. A kártyán tárolt adatok olvashatóságára vonatkozóan alapvető követelmény, hogy annak olvasására csak az arra jogosult szerv legyen képes, többfunkciós kártya esetén pedig – bármilyen többfunkciós kártyáról legyen szó – az olvasásra jogosult szerv is csak azokhoz az adatokhoz férjen hozzá, amelyek megismerésére joga van.

adatfelírás informált beleegyezéssel

6. A kártya a fentiek szerint elláthat egy jelenlét esetén történő azonosítást, tartalmazva az érintett természetes azonosítóit. A kérdés az, hogy emellett milyen egyéb szakazonosítók helyezhetők el a kártyán. Mint azt már a 2.2.1. pont alatt kifejtettük, a szakazonosítók egy kártyán történő elhelyezése, még akkor is, ha azok szegmentált chipen helyezkednek el, nem felelnek meg a fent leírt adatvédelmi követelményeknek. Elképzelhető azonban egy olyan megoldás, amelyben a kártyán a természetes azonosítókon túl (amellyel jelenlét esetén azonosítani lehet az érintetett), aláírásra, titkosításra szolgáló kulcsok kerülnek tárolásra. E megállapítás az egy kártyán történő tárolásra vonatkozik, nem a kulcsok használatára általában. Az egységes kulcsok ugyanis adatvédelmi kockázatot hordoznak magukban (egységességük folytán ellentmondanak az adatvédelem alapelveinek), erről a 2.1.1. szakaszban írtunk).

több szakazonosító nem írható fel a kártyára

A Megbízó által átadott dokumentumokban több olyan koncepció jelenik meg, amely ilyen többfunkciós kártyákat valósítanának meg. Ezekre nézve a fenti megállapítások mind fennállnak.

2.2.3. Egy speciális kérdés: az elektronikus társadalombiztosítási kártya

A dokumentumokból megismert egyik eredeti elképzelés egy olyan azonosító kártya bevezetését tervezte, amely a jelenlegi társadalombiztosítási azonosító jelet tartalmazó hatósági igazolványt váltaná fel egy olyan

kártyával, amely nyomtatott és elektronikus formában is tartalmazná a kártyabirtokos nevét, születési helyét, idejét, anyja nevét és társadalombiztosítási azonosító jelét. Lényegében a közös európai egészségbiztosítási kártyának megfelelő társadalombiztosítási kártyáról van szó Ennek egyfunkciós kártyaként történő megvalósítását adatvédelmi szempontból kivitelezhetőnek tartjuk, létrehozatalakor azonban arra nézve kell garanciákat kidolgozni, hogy az elektronikusan tárolt adatok csak az érintett közreműködésével legyenek bárki számára hozzáférhetőek, vagyis az adatok megfelelő biztonságát kell garantálni. Minden egyéb tekintetben a kártya funkcionálisan azonos lenne a jelenlegi papír igazolvánnyal. Ugyanazok használhatnák, ugyanazon célokkal és ugyanazon jogalap felhatalmazása alapján.

egyfunkciós társadalombiztosítási kártya

A kártyát azonban a megismert elképzelések további funkciókkal is ellátnák, más természetű élethelyzetekben is azonosításra alkalmassá tennék, illetve olyan adathordozóként is használnák, amely alkalmas lenne titkosító/aláíró kulcsok tárolására is. A háttéranyagokban már előkészített tervként konkrétan az egészségügy, oktatás és közlekedésre vonatkozó adattartalom egyetlen kártyán való elhelyezése is megjelent.

többfunkciós társadalombiztosítási kártya

A többfunkciós elektronikus társadalombiztosítási kártyát csak a fenti követelmények együttes érvényesítésével tartjuk megvalósíthatónak, az alábbi kiegészítésekkel, illetve az adott helyzetre történő értelmezésekkel.

1. Amennyiben az elektronikus társadalombiztosítási kártyát más funkciókra is alkalmassá teszik, illetve az más (opcionális) funkciókra is alkalmassá tehető, és azt esetleg át kell adni, fel kell mutatni bizonyos, a társadalombiztosítási ellátásoktól különböző feladatokat ellátó hivatalokban, nem szerepelhet rajta a TAJ-szám emberi olvasásra alkalmas formában, csak az adatalany személyazonosító adatai, esetleg fényképe. Ha ugyanis a TAJ-szám rá lenne nyomtatva egy többfunkciós kártya felületére, akkor ez lehetőséget adna a TAJ-szám célhozkötöttséggel ellentétes felhasználására, és ellentétes lenne a Szaz.

a TAJ-számot csak a jogosult szervek tudják kiolvasni (elektronikusan és hagyományosan is)

ismertetett rendelkezéseivel.

Ha az ilyen elektronikus társadalombiztosítási kártyán nem szerepel olvasható formában az érintett TAJ-száma, és azt az érintett nem jegyezte meg, elfelejtette, vagy elveszítette, ilyen esetben az alábbi módokon ismerheti meg vagy tudhatja meg a TAJ-számát újból: a kártya kiadásakor kinyomtatott papír-alapú igazolásról, internetes lekérdezés útján, hivatalos helyeken kártyaleolvasó használatával, esetleg otthoni kártyaleolvasóval.

adatalany hozzáférhet a tartalmához

2. Az elektronikus társadalombiztosítási kártya további funkciókkal való felszerelése csak lehetőségként és nem kötelezettségként állhat az állampolgár rendelkezésére. Ha például nem akarja, hogy kulcsokat is elhelyezzenek az egészségügyben használatos kártyáján, akkor álljon számára nyitva az a lehetőség, hogy azokat külön kártyán, esetleg virtuális kártyán kapja meg.

a több funkció csak opció lehet

3. A főszabálynak az egyfunkciós kártyának kell lennie, ehhez képest a további funkciókkal való ellátás (további adatokkal való felszerelés) kivételes, ennek opt in alapon kell történnie. Nem jó megoldás tehát az, hogy alaphelyzetben mindenki többfunkciós kártyát kap, és amennyiben nem akarja ezt, akkor lehetősége van arra, hogy egyfunkciós kártyája legyen, leválassza, illetve kérelmére leválasszák a további funkciókat a kártyájáról. Ez az adatvédelmi szempontból nem megfelelő opt out megoldás lenne.

opt in alapon

4. Nagy hangsúlyt kell fordítani arra, hogy minden, a kártyát azonosításra használó szerv, csak azokhoz az adatokhoz férjen hozzá, amelyek megismerése a jelenlegi jogi keretek között fel van hatalmazva.

célhozkötött szegmentálás

5. Több, különböző célú adatnak az érintett hozzájárulásával egyetlen kártyán történő elhelyezése esetén sem lehet egy központi tárban tárolni a kártyán lévő adatokat például elvesztés vagy megrongálódás esetére.

központi archiválás nem megengedett

Minden szerv csak a saját szakazonosítóját tárolhatja, az esetleges további adatok (például kulcsok) helyett elvesztés esetén újat kell biztosítani, a szakazonosítókat pedig külön-külön, újból be kell szerezni a megfelelő szervezetektől.

2.2.4. Másik specialitás: hivatali és képviseleti kártya

A köztisztviselők vagy hatósági eljárásban vállalkozás képviseletét ellátó személyek azonosítása céljából kiadott hivatali kártyára a fentiek megfelelően irányadók a következők figyelembevételével.

1. Adatvédelmi szempontból csak az a megoldás támogatható, amelyik független hivatali kártyát valósít meg, vagyis a hivatali kártya, minden más, magáncélra használt (az érthetőség kedvéért: állampolgári) kártyától teljesen független. E követelményt azért tartjuk elengedhetetlennek, mert a köztisztviselői lét nem lényegíti át a köztisztviselői munkakört betöltő személyét, az egyéb életviszonyaiban ugyanolyan magánszférával rendelkező személy marad, mint bárki más. A külön hivatali kártya kiadása ugyanakkor praktikusabb is, mivel viszonylagos szabadságot ad a hivatali kártya kialakításakor, mert a köztisztviselők – mint köztisztviselők és nem mint magánszemélyek, akik mellesleg köztisztviselők – viszonylatában nem kell olyan mértékben tekintettel lenni az önrendelkezési jogra, amennyiben a hivatali kártya, minden más, magáncélra használt kártyájuktól teljesen független. Ez a nagyobb szabadság megnyilvánul abban, hogy a hivatali kártya használata természetesen kötelezővé tehető, az azon tárolt adatok körének meghatározásakor a köztisztviselők hozzájárulása nem olyan fontos szempont, stb. Nem lehet a köztisztviselők állampolgári kártyáit a hivatali kártyáikkal összekapcsolni már csak azért sem, mert a köztisztviselők sem kötelezhetők az állampolgároknak kiadott kártyák kiváltására, a hivatali kártya használatára azonban munkakörüknél fogva igen. A két különböző funkciójú kártyát tehát egymástól külön kell kezelni.

nem lehet összeolvasztani a hivatali kártyát az állampolgári kártyával

az állam nagyobb szabadsága a hivatali kártya kialakításában

2. A hivatali kártyán szereplő magánkulcs nyilvános párja mindenki számára legyen elérhető, ellentétben az állampolgárok közigazgatási ügyintézés céljára rendszeresített kulcspárjának nyilvános részével, ez utóbbi a kulcsok használatának a közigazgatási célra történő leszűkítéséből (lásd ezt a 2.1.1. pont alatt az 53. oldalon) az következik, hogy csak a közigazgatás számára megismerhetők, többek között így biztosítható, hogy csak a közigazgatás használhatja őket.

a hivatali kártyához tartozó nyilvános kulcs

3. A hivatali kártya tulajdonosának a kártyához kapcsolódó személyazonosító adatait és (egy vagy több) kulcspárjával kapcsolatos hitelesítési, letiltási, visszavonási, kulcsmenedzselési, dokumentálási és archiválási teendőket biztonsági okokból mindenképpen az állam végezze, azért elsősorban a közigazgatás valamely szerve legyen felelős, még akkor is, ha a technikai lebonyolítást esetleg ki is szervezi.

hitelesítési teendők

4. A vállalkozás képviseletére jogosult személyek kártyája tekintetében nem támogatjuk azt az elképzelést, amely szerint a képviselettel kapcsolatos adatokat a képviselő állampolgári kártyájára további adatként írnák fel.

5. Nem támogatjuk a képviselő kártyáján valamennyi képviselettel kapcsolatos adatának az elhelyezését. Ez részben nagyon bonyolult eredményre vezetne: egy személy több céget is képviselhet és egymástól teljesen eltérő lehet a képviseleti jogosultság terjedelme és gyakorlásának módja nemcsak a különböző cégek tekintetében, hanem ugyanazon cég esetében is más és más hatóságokkal szembeni eljárásban. Az osztott információs rendszerek elvével lenne ellentétes a képviselő személyéhez egy helyen (a kártyán) összerendelni valamennyi képviselettel kapcsolatos jogát.

egy kártyán minden képviselettel kapcsolatos adat: nem támogatott

6. Amennyiben a képviseleti adatokat mégis magán a kártyán kívánják elhelyezni, akkor csak több kártyával tartjuk elfogadhatónak (például képviselt cégenként). Ez egyébként nyilvánvalóan nem lenne életszerű.

7. Mindezzel szemben támogathatónak tartjuk azt a megoldást, amely valójában a jelenlegi, előre bejelentett állandó képviseleten alapuló rendszer továbbfejlesztése, amelyben az érintett hivatalok tartják nyilván, hogy mely céget ki és milyen feltételekkel képviselhet elektronikusan, és a képviselőként jelentkező személyének azonosítása után e nyilvántartás alapján eldönti a szerv, hogy az adott jognyilatkozatot megteheti-e érvényesen az, akit azonosított, vagy sem. Ez a megoldás nem igényel külön képviseleti kártyát, e célra (a személy azonosítására) használható az állampolgári kártya.

bejelentett állandó képviseleti nyilvántartás + személyazonosítás

2.2.5. Plasztikkártya vagy virtuális kártya

A jelenlegi szakazonosítók kiadása fizikai kártyán történik. Ez azonban nem jelenti azt, hogy csak ebben a megoldásban lehet gondolkodni. A plasztikkártyára felvitt személyes adatokról, akár fizikailag nyomva, akár chipen elhelyezve már fentiekben szóltunk. A plasztikkártyás megoldás azonban részben kiegészíthető úgynevezett virtuális kártyával is.

A virtuális kártya egy olyan megoldás, ahol az azonosító adatok nem fizikai adathordozón kerülnek kiadásra (szemben a plasztikkártyával, intelligens kártyával), hanem az adatok elektronikus úton kerülnek a polgárokhoz. A biztonságos felhasználás érdekében javasoljuk, hogy az ügyfelek a virtuális kártya adattartalmát nyílt kulcsú titkosítással (PKI) működő aláíró kulcs(ok)kal felszerelve kapják meg. A virtuális kártya kialakítása során figyelembe kell venni, hogy az érintett kérheti egyes adatainak vagy valamennyi a közigazgatási szervek által kezelt személyazonosító adatának virtuális kártyán való kiadását. A virtuális kártya használata azt is jelenti, hogy az adatok tárolásának helyét és módját az ügyfél választja meg, döntése szerint tárolhatja számítógépén, mobiltelefonján, vagy akár letétbe helyezheti. A virtuális kártya tehát az ügyfelek részére nyújtott szolgáltatás, ami kényelmi többletszolgáltatásként funkcionál. A virtuális kártya bevezetésével az ügyfelek a virtuális kártya adattartalmát nem csak az

titkosító kulcs szükséges hozzá

az adattárolás helye sokféle lehet

adatvédelmen kívüli előnyök

ügyfélkapu elérésre használt gépükön érhetik el, hanem lehetőségük van munkahelyi számítógépük, internet kávézó számítógépei vagy mobiltelefonjuk használatával is az adattovábbításra.

A virtuális kártya bevezetése azzal az előnnyel jár, hogy igen olcsó, könnyen kialakítható, valamint az érintett önrendelkezési jogát a jelenlegi adatvédelmi rendszer megbontása nélkül gyakorolhatja. Hiszen a virtuális kártya adatvédelmi szempontú megítélése során az érintett aktív közreműködésével használt adattovábbítás megfelel az adatvédelmi törvény által támasztott követelményeknek. Az adatok időszerűségéről és pontosságáról az érintett bizonyos tekintetben maga is tud gondoskodni.

A virtuális kártya használatának lehetőségeit a háttéranyagok is ismertetik. Előnyeként felvetik, hogy a virtuális kártya „nem igényel tömeges kártyaellátást, alacsony a költsége, és gyorsan kivitelezhető", valamint, hogy a hitelesítés-szolgáltatás felállítása is gyorsan és olcsón megoldható. A hitelesítés-szolgáltató működésére vonatkozóan, illetve az adatelhelyezés lehetőségeire vonatkozó megállapításainkat a 2.3.2. pont alatt tárgyaljuk.

A virtuális kártya használatának adatvédelmi természetű feltételeit, korlátait és hátrányait az alábbiakban foglaljuk össze.

1. A virtuális kártya mindenkinek kioszthető, használatát azonban ma még nem lehet kötelezővé tenni. A fizikai adathordozó mellett kiegészítő megoldásként funkcionálhat azon állampolgárok szakazonosítói vonatkozásában, akik ezt igénylik.

használata opcionális

2. A virtuális kártya igénylése megegyezhet az ügyfélkapu használatának igénylésével, a Ket. jelenlegi szabályai alkalmazhatóak a virtuális kártyára is. A virtuális kártya és a hozzátartozó kulcsok személyes megjelenéssel vagy az ügyfélkapun keresztül lehetne igényelni. Az ügyfél egyszer használható kódot kaphat virtuális kártyájához, amelynek alkalmazásával meghatározott ideig használható egyedi azonosítót

nem kell alapjaiban megváltoztatni az elektronikus ügyintézés Ket.-beli szabályait

képezhet. Az egyedi azonosítót az ügyfél megváltoztathatja. Az ügyfél tartozik felelősséggel, ha az egyedi azonosító harmadik személy által, az ügyfél hibájából válik megismerhetővé.

3. Amiatt, hogy a virtuális kártya esetén az érintett birtokába, az ő ellenőrzése alá kerülnek az adatok, minden egyes adattovábbítás esetén az érintett döntésén túl, további lépéseket kell tennie az adattovábbításhoz, ahhoz tevőleges magatartás szükséges. Mivel a polgár maga küldheti, illetve teheti hozzáférhetővé adatait más számára, határozott és tudatos hozzájárulása e cselekményében benne foglaltatik, abból következik, hogy arra a célra, amelyre megadta adatait, hozzájárulásával kezelik azokat. Biztosítani kell ugyanakkor az érintett számára, hogy az adatok pontosságának és naprakészségének érdekében azok helyesbítését, vagy esetleg törlését maga tudja kezdeményezni, ha nem is tudja maga elvégezni

az önrendelkezési jognak nagymértékben megfelel

4. A virtuális kártya nem igényel jelentős beruházást. A virtuális kártyát igénylőkről vezetett adatbázis, és az állampolgárok PKI-val való felszerelésén túl többletkiadások nincsenek, nincs szükség plasztikkártya kiállítására. Ugyancsak nem veszélyezteti a projekt sikerét az, ha a felállított infrastruktúra kihasználtsága alacsony. A kártyaolvasók beszerzésére nincs szükség, ami ugyancsak jelentősen csökkenti a beruházási összeget.

olcsó, nemcsak az állam, hanem a polgár számára is

5. Biztosítani kell, hogy csak azok az állampolgárok kapják meg, akik igényt tartanak rá, és akik saját megítélésük szerint képesek infrastrukturálisan kezelni a virtuális kártyát. Mint azt az 1. pontban említettük, a virtuális kártya használatát nem lehet kötelezővé tenni. Ugyanakkor a kényelmi okok és az egyszerű használhatóság miatt várhatóan sokan kezdik el használni. Azt is biztosítani kell, hogy a virtuális kártyát az érintett bármikor, indoklás nélkül meg tudja szüntetni.

az adatalany legyen képes kezelni

6. A virtuális kártya használata során az adatok letéti kezelése jogszerűen

az adatok letéti kezelése

megvalósítható, erről lásd a központi adattárolás pontnál írottakat. (A 2.3.2. pont alatt.)

7. A virtuális kártya bevezetésével kapcsolatban jelentős kockázatot jelent, hogy az állampolgár által adattárolásra használt eszköz elromolhat, vagy elveszhet. Ez jelentheti akár a kártya személyes adattartalmának megsemmisülését, akár a magánkulcs elvesztését is. Éppen ezért akár a személyes adatok, akár a kulcs elvesztése, megsemmisülése esetén azok pótlásáról gondoskodni kell, ez azonban nem vezethet oda, hogy a virtuális kártyán tárolt valamennyi adatot egy központi adatbázisban, a polgártól függetlenül, biztonsági céllal nyilvántartják. (Ez nem azonos az előző pontban említett letéttel, amely esetében a polgár maga dönt adatai biztonságos helyen történő elhelyezéséről.)

véletlen adatvesztés

központi archiválás tilalma

8. Az állampolgároknak a virtuális adataikat lehetőség szerint biztonságos helyen kell tárolniuk. Az erről szóló tájékoztatás megadása kötelezettségén túl további feladat nem terheli a közigazgatást, nem köteles a biztonsági tárolást lehetővé tenni (de nyújthat ilyen szolgáltatást). Analógia alapján alkalmazható a Ket. ügyfélkapura vonatkozó szabálya, amely szerint az ügyfél tartozik felelősséggel, ha az egyedi azonosító harmadik személy által, az ügyfél hibájából válik megismerhetővé. [Ket. 160. § (7) bekezdés.]

a kártya adatainak biztonságos helyen történő megőrzése a polgár felelőssége

9. Nem szabad megfeledkezni arról, hogy a virtuális kártya használata az állampolgár részéről komoly technikai ismereteket és megfelelő technikai eszközöket feltételez, ezekre tekintettel kell lenni már csak az állampolgárok adatainak biztonsága érdekében is, azért, hogy véletlenül ne küldhessék el illetéktelennek azokat az adataikat, amelyeket valójában nem akarnak megismertetni másoknak. Ezért a rendszer kialakítása során törekedni kell az egyszerűsége. Az eszközigény azonban nem jelentős kockázati tényező, ismerve a hazai mobiltelefon penetrációt és a számítógép-ellátottságot.

technikai ismeret- és eszközigényre tekintettel kell lenni

10. A fejlesztések során figyelembe kell venni, hogy az ügyfél által történő adattovábbítás esetén az adatok megfelelően titkosítva legyenek. Ebben egy PKI alapú titkosítási módszer bevezetése is megfelelő biztonsági szintet nyújthat. Az elektronikus aláírások kiadásával pedig tovább növelhető a biztonsági szint.

    Az adatvédelmi problémák kiküszöbölése érdekében célszerű támaszkodni az elektronikus aláírás technológiája adta lehetőségekre. A háttéranyagokban felvetett állami kulcskiadási rendszer felállítása esetén az ügyfélkapu továbbfejlesztéseként virtuális kártyaszolgáltatás kialakítása viszonylag egyszerűen és költség-hatékonyan megoldható. Azonban (mint arra a 2.1.1. pont alatt az 1. számú észrevételben az 53. oldalon rámutattunk) az állami kulcskiadás nem lehet monopólium, a piaci szereplők bevonása is fontos, hogy az érintett választási lehetősége biztosítva legyen.

2.2.6. Rádiófrekvenciás azonosító chip a kártyán

A rádiófrekvenciás azonosító (RFID) chipek használata egyre több személyazonosító rendszer részévé válik a világban, ezért fontosnak tartjuk, hogy az ezek használatával kapcsolatos adatvédelmi kockázatokra és követelményekre is felhívjuk a figyelmet. A Megbízótól átvett dokumentumokban nyomokban fellelhető a technológia használatának szándéka, némely alkalmazás kifejezetten igényelni szokta ezt a technológiát, amelyet az átvett munkadokumentumok is említenek. (Itt elsősorban az MTA Információtechnológiai Alapítvány 2007. júniusi anyagára utalunk, amelynek címe Elektronikus azonosító bevezetése: elvárások és igények, következtetések és javaslatok, ennek 3.5. és 3.6. pontja alapján két konkrét kártyafajtát, a közlekedési kártyát és a diákigazolványt említhetjük ebben a körben.)

Európában több adatvédelmi hatóság foglalkozott az RFID technológiával kapcsolatos adatvédelmi követelményekkel, valamint az európai adatvédelmi

hatóságok képviselőiből álló, úgynevezett 29. Munkacsoport is aggodalmának adott hangot az egyre szélesebb körű alkalmazása miatt. (Article 29 Data Protection Working Party: Working document on data protection issues related to RFID technology. WP 105.) Az aggodalmak jogosak, hiszen a technológia számos előnye mellett arra is lehetőséget ad, hogy akár az állam, akár a magánszervezetek folyamatos adatgyűjtést folytassanak segítségükkel egy-egy személyről, kövessenek valakit a közterületen (repülőtéren, pályaudvaron, üzletközpontban), profilt építsenek a fogyasztási szokásaik megfigyelésével, leolvassák egy-egy ember által viselt ruhák, ékszerek, zsebben hordott gyógyszerek adatait, megszámolják a pénztárcában lévő pénzt, stb.

Az RFID személyes adatok gyűjtésére használható

Természetesen az RFID-technológia használata nem minden esetben jár együtt személyes adatok kezelésével. Az alábbiakban kizárólag a személyes adatok védelmével összefüggő megállapításokkal foglalkozunk.

Az egyik leggyakoribb adatvédelmi kifogás a technológia alkalmazásával szemben, hogy használatának célja általában közvetve vagy közvetlenül személyes adatok gyűjtése. Amennyiben az RFID chip egy tárgyon van elhelyezve, amely valójában egy áru, egészen addig nem személyes, amíg a tárgyat, és vele együtt az RFID chipet valaki magához nem veszi, meg nem vásárolja. Ettől kezdve azonban – különösen ha bankkártyával vásárolt, esetleg számlát kért a vevő – egy adatbázisban már egymás mellett is tárolják a vevő és az áru azonosítóját. Ettől kezdve az RFID chip bármilyen követése, mozgásáról való adatgyűjtés újabb személyes adatok gyűjtését jelenti.

Ha személyazonosításra szolgáló kártyán helyezik el az ilyen chipet, annak a személyhez tartozása az előző példánál még nyilvánvalóbb. Akárhányszor azonosítja a kártyán lévő chipet egy vevőberendezés, annyiszor azonosítja magát a kártyabirtokost, ezzel adatokat gyűjt róla (például azt, hogy melyik időpontban, hol járt, melyik más kártyabirokosokkal együtt azonosították, stb.).

Ezekben az esetekben, mivel az RFID technológia segítségével természetes személyekkel kapcsolatba hozható adatok gyűjtése folyik, az Avtv. 2. § 1. pontjában foglalt személyes adat definícióra való tekintettel nyilvánvalóan személyes adatok gyűjtése történik, ezért adatvédelmi szabályok vonatkoznak erre az adatkezelésre. Olyan adatkezelésről van szó, amely személyiségprofil képzésre ad módot, ez pedig óriási üzleti és más természetű lehetőségeket rejt magában. Fel kell készülni arra, hogy az RFID technológiával felszerelt azonosító kártyákat esetleg az állami szerveken kívül mások is szeretnék azonosításra felhasználni, például az üzlet ajtaján belépő személyek vásárlási szokásait rögzíteni és felhasználni az érintett személyek tudta és beleegyezése nélkül.

Az előzőekhez képest más minőségű adatvédelmi kérdéseket vet fel az az eset, amelyben maga az RFID adathordozó tartalmaz személyes adatokat. Jó példa erre a tömegközlekedési kártya, amely esetleg a tulajdonos (bérletes) nevét és elérhetőségi adatait is tartalmazza. Ez lehetővé tenné a közlekedési vállalat számára, hogy állandóan figyelemmel kísérje, a bérletes merre utazik, így nyilvánvalóan felvet adatvédelmi kérdéseket. További adatvédelmi kérdés, hogy mivel más is használhat RFID olvasót, mások is megszerezhetik ugyanezt az információt. Fontos megjegyezni, hogy az RFID technológia nagyon könnyen támadható ilyen módon. Mivel érintés nélkül működik, offline módon azonosít, a támadó – az alkalmazott RFID technológia jellemzőitől függő mértékben – távolról és észrevétlenül szerezheti meg az adatokat. (Jelentősége van például annak, hogy hány cm-ről lehet aktiválni és leolvasni.)

Az RFID chipen személyes adat is tárolható

Amennyiben személyes adatok gyűjtésére, tárolására és összekapcsolására használatos a technológia, az adatvédelmi törvény szabályai irányadók. Az RFID-azonosítás nem minden alkalmazásának vannak adatvédelmi következményei, mindig az adott alkalmazás vizsgálatával dönthető el, hogy az Avtv. szabályai vonatkoznak-e az adott rendszerre, vagy sem. Tekintettel arra, hogy itt személyazonosításra (közvetlenül egy-egy személynél hordott igazolvány, kártya azonosítására) való felhasználásról van szó, az adatvédelmi vonatkozás kétségtelen.

adatvédelmi követelmények

Számos olyan technológiai megoldás létezik, amelyek az adatvédelmi követelményeket igyekezik figyelembe venni, az adatvédelmi szakemberek pedig arra tettek javaslatot, hogy az adatvédelmi követelményeket a technológiai szabványok részévé kell tenni, [mint például az ISO szabvány részévé (ISO 18000 Part 6 Type A) az OECD adatvédelmi irányelveit, erre tesz javaslatot Christian Floerkemeier, Roland Schneider és Marc Langheinrich: Scanning with a Purpose -Supporting the Fair Information Principles in RFID protocols. 2nd International Symposium on Ubiquitous Computing Systems (UCS 2004), November 8-9, 2004, Tokyo, Japan.]

adatvédelmi követelményeket érvényesítő szabványok az RFID-re

A technológia helyes megválasztásán túl figyelemmel kell lenni az információs önrendelkezési jog maradéktalan érvényesülésére az RFID-t alkalmazó azonosítási rendszer megszervezésekor is. Ennek keretében a következő követelményeknek kell eleget tenni:

1. Az adatalanyoknak joguk van ahhoz, hogy tisztában legyenek azzal, mire képes az azonosító chip. Ebből következően a kártyakiadáskor részletesen tájékoztatni kell őket arról, hogy a kártya ezzel van felszerelve, arról, hogy távolról is olvasható, hogy milyen adatokat tartalmaz, és hogy esetleg illetéktelenek is hozzáférhetnek az adatokhoz.

részletes tájékoztatás

2. Az adatalanyoknak joguk van ahhoz, hogy kontrollálják a chip és a külvilág közötti kommunikációt. Erre több technikai megoldás kínálkozik: lehetséges a chipet időlegesen vagy véglegesen deaktiválni, illetve a kommunikációját blokkolni, zavarni, erre szolgálnak a különböző RFID tag-killerek és faraday-konténerek valamint aktív zavaró berendezések. Az állam által adott azonosító kártya esetében azonban ezek a megoldások nem jók, hiszen az államnak nem szabad potenciális veszélynek kitenni az állampolgárt, amely ellen neki kell védekeznie, éppen ellenkezőleg: az államnak kell megvédenie polgárait. Az RFID feletti kontroll gyakorlása lehetőségének biztosítására ezért az egyik javasolt megoldás a kódolt RFID használata, amely az adatalany közreműködését igényli az azonosítás elvégzéséhez, az azonosítás bár távolról is elvégezhető, mégsem történhet meg az érintett tudta és beleegyezése, aktív közreműködése, a dekódolás nélkül. A másik lehetséges technológiai megoldás a passzív RFID chip helyett az aktív chip választása,

az adatalany joga az RFID chip működése feletti kontrollhoz

amely maga küldi a jeleket a vevőberendezésnek (és nem a vevőberendezés energiáját használja), és azt is az adatalany által kontrolláltan teszi (úgynevezett kontrollált aktivációjú aktív RFID chip).

3. Tekintettel arra, hogy az RFID technológia alkalmazása mindenképpen további személyesadat-kezeléseket valósít meg, nem lehet a közigazgatás szolgáltatásait az RFID-alapú azonosításhoz, mint feltételhez kötni. Kell hogy legyen az ügyintézésnek, valamint a közszolgáltatások igénybevételének olyan alternatív útja, amely RFID chip segítségével történő azonosítás nélkül is biztosítja az adott szolgáltatást az állampolgárnak. Így tudatosan, önrendelkezési jogát gyakorolva tud választani a polgár a kényelmes és a biztonságos lehetőségek közül.

alternatív út biztosítása

4. Az adatalanyokat megilleti az RFID chipen tárolt adatokhoz, illetve az RFID chipen tárolt egyedi azonosítóhoz egy adatbázisban hozzárendelt adatokhoz való hozzáférés, helyesbítés és töröltetés joga, amennyiben e jogok értelmezhetők e körben. Lehetőséget kell biztosítani az adatalanyok számára, hogy bármikor, különösebb nehézség nélkül ellenőrizni tudják az RFID chipben vagy azon keresztül máshol róluk kezelt személyes adatokat, és amennyiben hibát észlelnek, vagy nem akarják, hogy valamely adatot róluk kezeljék, és nem írja elő törvény az adott adat kötelező kezelését, akkor kijavíttathassák vagy töröltethessék azokat.

az adatalany személyes részvételi jogainak biztosítása

5. Végül az adatalanyoknak joguk van ahhoz, hogy tudják, kik, mikor és miért olvassák és olvashatják le az adatokat a chipről. Minden leolvasó berendezésnél fel kell tehát hívni a figyelmüket arra, hogy itt leolvasás történik, amelyhez ideális esetben egyébként is kell az adatalanyok közreműködése (lásd a 2. pontban leírt követelményt is).

minden azonosításról külön tájékoztatás

2.2.7. Biometriai adatok a kártyán és biometrikus azonosítás

Tekintettel arra, hogy időről időre felmerül az azonosító okmányok biometrikus azonosítást is lehetővé tevő adatokkal való felszerelése, szükségesnek tartjuk az ezzel kapcsolatos adatvédelmi tudnivalókat is

összefoglalni.

Az egyre szélesebb körű felhasználásra, illetve az ezzel kapcsolatos tervekre reagálva az Európai Unió adatvédelemmel foglalkozó munkacsoportja (29. Munkacsoport, tekintettel arra, hogy ezt a független tanácsadó testületet az Európai Parlament és a Tanács az egyénnek a személyes adatok feldolgozásával kapcsolatos védelméről és ezeknek az adatoknak a szabad áramlásáról szóló 95/46/EK irányelve 29. szakasza alapján állították fel) a biometrikus azonosító rendszerek adatvédelmi kérdéseivel foglalkozó munkaanyagot fogadott el 2003 augusztusában (Working document on biometrics Adopted on 1 August 2003 by Article 29 - Data Protection Working Party, WP 80). Magyarországon az adatvédelmi biztos először 2000-ben foglalkozott a biometriai személyes adatok kérdésével (832/K/2000. számú ügy, Az adatvédelmi biztos beszámolója 2000, 249. oldal). Mindeddig elmaradt azonban a biometriai adatok kezelésének adatvédelmi szempontú hazai vizsgálata, vagyis annak összefoglalása, hogy az ilyen adatok gyűjtése és felhasználása az általános adatvédelmi szabályokra való tekintettel milyen feltételek mellett és milyen szabályok szerint történhet. Bár az adatvédelmi biztoshoz időről időre érkeznek a biometriai adatok kezelésének feltételei felől érdeklődő konzultációs kérdések, mindeddig nem született olyan állásfoglalás, amely a teljesség igényével számba venné a felmerülő kérdéseket és az azokra adandó válaszokat.

A biometriai adatok azonosításra való használata nem újdonság, gondoljunk csak a nyomozás során már régóta használt ujjlenyomat-vizsgálatokra. Ha úgy definiáljuk ezeket az adatokat, mint az emberek mérhető testi tulajdonságait valamilyen módon leképező adatokat, akkor könnyű belátni, hogy ilyen adatok felhasználásával azonosít minden olyan igazolvány, amely tartalmazza tulajdonosának arcképmását. A fénykép ugyanis az arc geometriájának egyfajta leképezése, az azonosítás során ezt a képet hasonlítjuk össze az eredeti arccal. Ha ezt továbbgondoljuk, rájövünk, hogy biometriai adatok alapján azonosítunk mindenkit, aki velünk szembe jön az

utcán, vagy aki felhív telefonon, ha az emlékezetünkben tárolt emlékképet hasonlítjuk össze ismerősünk arcával vagy hangjával.

A biometrikus azonosításban az egyik újdonság az, hogy a tárolt biometriai adatot a valósággal újabban már nemcsak az ember tudja összehasonlítani, hanem erre a célra létrehozott számítástechnikai eszközök is, az azonosítás tehát már csak az azonosítandó személy közreműködését igényli, más emberét nem, a folyamat automatikusan történik. A másik újdonság a felhasználási területek kiszélesedése. A biometriai adatok használata korábban a DNS- és az ujjnyomat-azonosításra korlátozódott, ezeket az adatokat elsősorban büntetőeljárásokhoz kapcsolódóan gyűjtötték. Manapság viszont ezeket a speciális, egy-egy meghatározott személy viselkedési és fiziológiai jellegzetességeit megjelenítő, és a személy egyedi azonosítását lehetővé tevő adatokat a büntetőeljáráson kívül is gyakran használják ellenőrzési, bizonyítási, igazolási és azonosítási célokra, különösen fizikai vagy virtuális területekre való belépésre való jogosultság fennállásának eldöntésére. Az egyre szélesebb körű felhasználás együtt jár ezeknek az adatoknak a sokkal több helyen való tárolásával, ami pedig magában rejti annak veszélyét, hogy mások azokat saját, az eredetitől teljesen eltérő céljaikra használják fel. Az egyre szélesebb körű felhasználás végső soron azzal a veszéllyel járhat, hogy megszűnik az emberek érzékenysége ezen adataikat használó rendszerekre, és a biometrikus azonosítás teljesen mindennapivá válik az élet minden területén. Az ilyen adatok széles körű felhasználása az adatvédelem iránti érzékenységet, az adatalanyok tudatosságát ronthatja. Erre a veszélyre hívja fel a figyelmet a 29. Munkacsoport már említett dokumentuma, amely azt a példát hozza fel, hogy ha egy iskolai könyvtárban biometrikus azonosítókat használnak, a gyermekek későbbi életük során sokkal kevésbé lesznek elővigyázatosak személyes adataikat illetően, hiszen számukra természetesebb lesz az, hogy ezeket az adataikat ők másoknak megadják, mások pedig azokat használják.

biometrikus azonosító rendszerek meghatározása

A biometrikus azonosító rendszereket úgy definiáljuk, mint eszközök és eljárások összességét, amelyek a személyek mérhető testi tulajdonságait

használják fel valamilyen technika segítségével azonosításra vagy a személyazonosság megállapítására. Az azonosítás és a személyazonosság megállapítása közötti különbségtétel a vizsgált tárgy szempontjából fontos: az eltérő cél eltérő eljárásokat és adatfajtákat igényelhet. Az azonosítás az *„az vagyok, akinek mutatom magam?”* típusú kérdésre ad választ, ilyenkor a rendszer a tárolt biometriai adatoknak a személy testével való összehasonlítása után igen vagy nem választ ad. A személyazonosság megállapításakor a *„ki vagyok én?”* kérdésre kapunk választ, ebben az esetben a rendszer felismeri a személyt oly módon, hogy megkülönbözteti másoktól, akiknek a biometriai adatai már eltárolásra kerültek. Az első esetben két adat egymással való összehasonlítása történik, az utóbbiban egy adat összehasonlítása az összes többi adattal.

azonosítási célnak megfelelő rendszer

A biometrikus azonosító rendszerek használatának terjedését a biometriai adatok speciális jellemzői indokolják. Ezek az adatok egyrészt univerzálisak, abban az értelemben, hogy ilyen adatai mindenkinek vannak. Az azonosításra vagy a másoktól való megkülönböztetésre leginkább a DNS-minták, az ujjnyomatok és a retinaképek alkalmazhatók, ám a kéz és az arc geometriája és az emberi hang is gyakran használt ilyen célokra. Ilyen jellemzőkkel – a testi hiányosságokkal élőktől eltekintve – mindenki rendelkezik. (Gondolni kell azokra is, akiknek nincs kezük, amivel ujjnyomatot adnának, vagy nincs szemük, amelynek retinaképét használnák, stb.) A biometriai adatok másrészt egyediek, harmadrészt ezek az adatok állandóak, lényegileg nem változnak az idővel. Ez természetesen nem minden biometriai adatra igaz, azonosítási célokra azonban csak az állandóak használhatók.

az azonosítás alapja, a biometriai adat univerzális…

… és egyedi

Ha tágabb értelemben vesszük a biometrikus azonosító rendszereket, a személy fiziológiai tulajdonságait alapul vevő technológiák mellett ide sorolhatjuk a viselkedési tulajdonságokat alapul vevő rendszereket is, így az ujjnyomat-azonosítás, az írisz-felismerés, a retina-analízis, az arcfelismerés, a kézgeometria-vizsgálat, a fül alakjának vizsgálata, a test illatának felismerése, a hangfelismerés és a DNS-analízis mellett ide tartozik az

aláírás-minta vizsgálata, a billentyűleütés-vizsgálat és a járáselemzés is. A biometrikus azonosító rendszerek egy része kombinálja az egyes biometriai adatfajták felhasználását (például ujjnyomat és hangazonosítás együttes alkalmazásával), mások pedig a biometrikus azonosítást más azonosítási módszerekkel egészítik ki: olyanokkal, amelyek az azonosítandó személy ismereteit vizsgálják (tudja-e a jelszót, a PIN-kódot), vagy amelyek a birtokában lévő tárgyakat vizsgálják (kártya, kulcs, stb.).

kombinált biometrikus azonosítás

A személyek mérhető tulajdonságainak, az úgynevezett biometriai mintáknak, a „nyers" biometriai adatoknak (az ujjnyomatnak, a retina képének, a hangnak, stb.) a felvétele az eljárás első fázisa. A rendszer ezt követően ezekből a nyers adatokból valamilyen algoritmus segítségével kiemel bizonyos számú jellemzőt, amelyekből összeállítja az úgynevezett biometriai sablont. Ez a sablon nem más, mint a nyers biometriai adat redukált változata: a személy rögzített biometriai méretei. Az azonosító rendszerek többnyire csupán ezt a sablont tárolják valamilyen digitalizált formában, és nem magát a képet, hangmintát, bár vannak olyan rendszerek is, amelyek ezeket a nyers adatokat használják sablon képzése nélkül.

a biometriai adat felvétele

sablonképzés

Adatvédelmi szempontból az adatok felvételének a fázisa számít a legkritikusabbnak, mivel a nyers adatok, a sablonok és a kettő közötti átalakítást megvalósító algoritmus csupán ekkor áll együttesen rendelkezésre. Adatvédelmi szempontból fontos kérdés, hogy milyen formában tárolják a sablonokat. Ez természetesen függ a felhasználás céljától, a sablonok méretétől, ám leegyszerűsítve háromféle tárolási módszert különböztethetünk meg: a sablonokat vagy egy központi adatbázisban, vagy magukon az azonosítást végző eszközökön, vagy pedig valamilyen adathordozón, például mikrochippel felszerelt kártyán tárolják. Ez utóbbi módszer lehetővé teszi, hogy az érintettek saját sablonjaikat maguknál tartsák, ellenőrzésük alatt tartva azokat. Elvileg nem elengedhetetlen az összehasonlítás alapjául szolgáló referencia-adatokat valamilyen adatbázisban tárolni, ha a cél pusztán az azonosítás, a személyes adatok decentralizált tárolása is elegendő. Ezzel szemben a személyazonosság megállapítása csak központi

a sablontárolás módja

adatbázisban tárolt adatokkal való összehasonlítás útján érhető el, hiszen ilyenkor valamennyi nyers vagy sablonizált adattal való összehasonlítás szükséges.

az adatalany közreműködésének szükségessége

Különbség tehető az egyes rendszerek között aszerint is, hogy egyesek olyan biometriai adatokra támaszkodnak, amelyek az adatalany tudta nélkül is gyűjthetők, mint például az ujjnyomatok vagy a DNS-minták. A pohár oldalán talált ujjnyomat alapján megállapítható, hogy az azt otthagyó személy azonos-e azzal, akinek az ujjnyomat-sablonját valamely adatbázisban tárolják, és ha igen, akkor az is, hogy ki az, pusztán azzal, hogy a két sablont egymással összehasonlítják. Ugyanez történik a billentyűleütés-vizsgálat és a közterületen alkalmazott arcfelismerő rendszerek esetében is. Ezekkel a rendszerekkel kapcsolatban a probléma az, hogy míg az érintettek tudta nélkül gyűjtött adatokra támaszkodnak, addig az érintettek számára kevéssé zavaróak, így szélesebb körben, akár általánosan is alkalmazhatóak. Mindezek következtében speciális biztosítékok szükségesek a személyes adatok védelméhez való jog érvényesülése érdekében.

a biometriai adatok személyes adatok

Az Avtv. szerint személyes adat bármely meghatározott (azonosított vagy azonosítható) természetes személlyel kapcsolatba hozható adat, az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet. E fogalom-meghatározás szerint a biometrikus azonosító rendszerek által kezelt nyers adatok vagy ezek digitális leképezései, a sablonok mind személyes adatok. A biometriai adatok mindig valamely „meghatározott természetes személlyel kapcsolatba hozhatók”, mivel olyan adatok, amelyek természetüknél fogva egy adott személyre vonatkozó információt hordoznak magukban. Az érintett azonosíthatósága sem kérdéses: a biometriai adatokat éppen azonosításra vagy a személyazonosság megállapítására használják, így

az adat alanya legalábbis az azonosító rendszerek által mindenki mástól megkülönböztetett. Az adatvédelmi törvény szabályai – a hatályát korlátozó rendelkezéseire tekintettel – tehát alkalmazandók az ilyen adatok kezelésére, a biometrikus azonosító rendszerek tehát csak e törvény szabályainak figyelembevételével működtethetők jogszerűen: ha megfelelő jogalappal történik az adatok kezelése, ha betartják a célhozkötöttségi, adatminőségi és adatbiztonsági szabályokat.

célhozkötöttség a biometriai adatok kezelésekor

Az adatvédelmi törvény célhozkötöttségi szabályai egy sor követelményt állítanak az adatkezelő elé, ezeknek pedig számos következménye van a biometriai adatok kezelésére nézve is. A biometrikus azonosító rendszerek kiépítésekor elsősorban ezeket a kérdéseket kell számba venni és megválaszolni, a jog által kijelölt keretek ugyanis jelentősen leszűkítik a lehetséges rendszer-típusok, megoldások körét.

A célhozkötöttség elve szerint személyes adatot kezelni csak valamilyen jól körülhatárolt cél érdekében lehet. Normatív módon ez Magyarországon úgy fogalmazódik meg, hogy személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet [Avtv. 5. § (1) bekezdés]. Az elvből következően a biometriai adatok kezelésének pontos célját előre meg kell határozni. Mivel az adatkezelés egy alkotmányos jog, a személyes adatok védelméhez való jog „kárára” történik, a céljának jelentősége van annyiban is, hogy az adatkezeléssel járó, az érintett magánszférájába való beavatkozásnak arányban kell állnia az elérendő céllal. Amennyiben a cél elérhető kisebb beavatkozással, vagy adatkezelés nélkül, akkor a kisebb beavatkozással, vagy adatkezelés nélküli megoldást kell választani. Ha tehát az azonosítási, személyazonosság-megállapítási vagy más cél nem érhető el ugyan biometriai adatok kezelésével, de elérhető kevesebb adat felhasználásával, vagy az adatok „kíméletesebb” kezelésével, esetleg olyan adat használatával, amely kevésbé érinti az érintett magánszféráját, akkor így kell eljárni, ilyen adatot kell használni. A magyar adatvédelmi törvényben az arányosság követelménye a célhozkötöttségi szabályok között kapott helyt, ezek szerint csak olyan személyes adat

a cél eléréséhez szükséges, arányos adatkezelés

a lehető legkisebb sérelem okozása

kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig [Avtv. 5. § (2) bekezdés].

A hozzáférési, belépési jogosultság ellenőrzése, az azonosítás – ha más módon, mint biometrikus azonosító rendszer segítségével nem lehetséges – akkor jár az érintett jogainak legkisebb mértékű sérelmével, ha a rendszer úgy van kialakítva, hogy abban az érintett fizikai tulajdonságainak nem marad nyoma (mint a DNS-minta vagy az ujjnyomat esetében), illetőleg ha marad is nyoma, az olyan eszközön marad, amely az érintett birtokában van. Az adatokat tehát nem tárolják egy központi adatbázisban vagy az azonosító eszközön, hanem csak az érintettnél lévő adathordozón. A 29. Munkacsoport számos európai ország adatvédelmi hatóságaival egyetértve arra a megállapításra jutott, hogy a biometriai adatokat lehetőség szerint nem szabad adatbázisban tárolni, sokkal inkább egy olyan eszközön, amely kizárólag az érintett, az azonosítandó személy számára hozzáférhető, mint amilyen a mikrochippel felszerelt kártya, a mobiltelefon vagy a bankkártya. A biometriai adatok azonosítási célú felhasználásánál elkerülhető, ennélfogva el is kerülendő az adatok adatbázisban való tárolása. Az azonosítandó személy birtokában lévő adathordozó megsemmisülése, elvesztése, sérülése, stb. esetére sem kell az adatokat tárolni az új adathordozó pótlása érdekében, hiszen az adatokat fel lehet venni ilyen esetben maguktól az érintettektől.

az eredeti céltól eltérő felhasználás tilalma

A célhozkötöttség elvéből következő további követelmény, hogy az adatokat csak az eredeti cél elérése érdekében szabad kezelni, használni, új célú adatkezelés nem megengedett. Az adatvédelmi törvény ezt úgy fogalmazza meg, hogy nem elegendő a cél meghatározása, az adatkezelésnek minden szakaszában meg kell felelnie e célnak [Avtv. 5. § (1) bekezdés]. Az adatkezelés jogalapjaként funkcionáló hozzájárulás vagy az adatkezelés törvényben történő elrendelése ugyanis csak az eredeti célra érvényes: ha valaki egy meghatározott célra megadja biometriai adatait, akkor azok kezelhetők, de csak erre az eredeti célra, ettől eltérő, más célra való

felhasználásuknak ez az eredeti hozzájárulás nem lehet a jogalapja. Ha például a biometriai adatok kezelésének eredeti célja egy beléptetőrendszer működtetése, a munkavállalók érzelmi állapotának felmérésére, vagy munkavégzésük megfigyelésére az adatok már nem használhatók fel, ez ugyanis egy új célú adatkezelés lenne. A biometriai adatok egyedi és egyben univerzális volta miatt különösen alkalmasak lehetnek mindig újabb és újabb célú felhasználásra, ezért ennek tilalmát nem lehet eléggé hangsúlyozni.

az azonosításra használt biometriai adat kiválasztásának célhozkötöttségi szempontja

Vannak olyan biometriai adatok, amelyeket akaratunkon, sőt tudtunkon kívül hagyunk magunk után mindennapi életünk során. Ha például megiszunk egy pohár vizet, akkor a pohár oldalán ujjnyomatot, a pohár peremén pedig hámsejteket hagyunk a DNS-ünkkel. Az ilyen nyomokból is gyűjthetők biometriai adatok. Nem igényel különösebb magyarázatot, hogy ezek sokkal kevésbé használhatók fel a célhozkötöttség elvének megsértésével, ha az adatokat nem tárolják valamilyen központi adatbázisban, hanem azok maguknál az érintetteknél vannak, és mások számára nem hozzáférhetők. A központi adatbázisban tárolt adatok ugyanis mindig összehasonlíthatók lesznek a nyomok adataival. A munkahelyi főnök például a beléptetőrendszer központi ujjlenyomat-adatbázisát felhasználhatná ilyen esetben saját nyomozására.

a biometriai adatok profilépítésre alkalmasak lehetnek

A biometriai adatok központosított kezelése magában rejti annak veszélyét is, hogy a régi személyi számhoz hasonlóan univerzálisan alkalmazható általános azonosító adatként kezdenek funkcionálni, és segítségükkel különböző adatbázisok összekapcsolhatóvá válnak, hiszen ezek az adatok egyediek, így önmagukban kapcsolati kódot jelenthetnek az egymástól elkülönült nyilvántartások között, így hozzásegíthetik az adatkezelőket akár egy részletes személyiségprofil kialakításához is.

A célhozkötöttség és az arányosság elve mindig komoly mérlegelést igényel. Az előzőekben kifejtetteken kívül az is megfontolandó, hogy az elérendő cél milyen biometriai adatfajták kezelésével érhető el. Az egyes biometriai adatfajták között is különbség tehető annyiban, hogy mennyire érintik magát

a személyiséget. A viselkedési elemeket leíró biometriai adatok önmagukban is sokkal többet árulnak el egy-egy személyiségről, az érintett aktuális lelkiállapotát, mint a statikus biometriai adatok. Az emberi hang elemzésével például több következtetésre juthatunk a tulajdonosára vonatkozóan, mintha a fülének geometriáját vizsgálgatjuk. Vannak olyan biometriai adatok, amelyek a többcélú felhasználásra a többinél alkalmasabbak, így a célhozkötöttségi szabályok megsértésének veszélyét sokkal inkább magukban hordozzák, mint más adatok. A célhozkötöttség elvéből következően csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. [Avtv. 5. § (2) bekezdés] A francia adatvédelmi hatóság például a célhozkötöttség elvére tekintettel nem találta elfogadhatónak egy iskolai étkező bejáratánál működtetett beléptetőrendszer esetében a tanulók ujjnyomatának használatát, de elfogadhatónak tartotta ugyanezen célra a kéz geometriájának alkalmazását. Az ujjnyomat ugyanis egyrészt nyomot hagy, másrészt az érintett tudta nélkül is gyűjthető, harmadrészt pedig túl széles körben alkalmazott (A Commission Nationale de l'Informatique et des Libertés 00-015. számú, 2000. március 21-én kelt határozata). A portugál adatvédelmi hatóság elfogadhatatlannak találta a biometrikus (ujjnyomat-) azonosítást egy egyetem nem oktató munkavállalói pontos munkába járásának ellenőrzésére. Állásfoglalása szerint az ilyen rendszer alkalmazása az adatkezelés céljára tekintettel aránytalan, túlzott, hiszen a munkahelyre érkezés ellenőrzése biometrikus azonosítás nélkül is megoldható. A rendszer körülbelül százhetvenegyven személy ujjnyomat-sablonját tárolta volna egy biometrikus azonosító eszközön (A Comissão Nacional de Protecção de Dados 11/2002. számú határozata.).

a biometriai adatok beszédes adatok lehetnek

A biometriai adatok kezelésével kapcsolatban felmerülő további kérdés az, hogy ezek az adatok az esetek egy meghatározott részében több információt hordoznak magukban az adott személyről, róla többet árulnak el, mint amennyi információ az azonosítási vagy a személyazonosság-megállapítási cél eléréséhez egyáltalán szükséges. Bizonyos biometriai adatok például a származásra vagy az egészségi állapotra utalhatnak. A nyers biometriai

adatokat használó rendszerek esetében ennek lehetősége nyilvánvalóbb, mint az azokat sablonokká alakító, majd a továbbiakban a sablont használó rendszereknél, hiszen a sablonok már az azonosítási, személyazonosság-megállapítási célra való tekintettel kivonatoltan tartalmazzák az érintett sajátosságait. A célhozkötöttség elvéből következően a cél eléréséhez nem szükséges adatok kezelését amint lehet, meg kell szüntetni, az adatvédelmi törvény szerint az adatokat csak a cél megvalósulásához szükséges mértékben és ideig szabad kezelni [Avtv. 5. § (2) bekezdés], a szükségtelen adatkezelés jogellenes, a jogellenesen kezelt adatokat pedig törölni kell [Avtv. 14. § (2) bekezdés a) pont]. A sablonokat használó rendszerek tehát adatvédelmi szempontból előnyben részesítendők, azok közül is elsősorban azok, amelyek az ilyen „felesleges", különleges adatokra való következtetésre alapot adó információkat „letisztítják" a biometriai adatról.

adatvédelmi előnyei

A célhozkötöttséggel kapcsolatos gondolatok között említendő meg az is, hogy a biometrikus azonosítás szolgálhat adatvédelmi célokat is bizonyos körülmények között, segítségével ugyanis több személyes adat kezelése elkerülhető, mint például a névé, a lakóhelyé, a lakcímé.

az adatfelvétel tisztességessége

Az adatvédelmi törvény adatminőségi elve szerint a személyes adatok felvételének és kezelésének tisztességesen kell történnie [Avtv. 7. § (1) bekezdés a) pont]. Ebből, valamint a tájékozott hozzájárulás követelményéből [Avtv. 2. § 6. pont] következően az adatkezelő tájékoztatni köteles az érintettet az adatkezelés részleteiről. Az érintettet – egyértelműen és részletesen – tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat [Avtv. 6. § (2) bekezdés]. E szabályozásra tekintettel eleve nem, illetve csak rendkívüli esetekben (titkos információszerzés, nemzetbiztonsági indok, stb.), törvény által elrendelten használhatók az olyan biometrikus azonosító rendszerek, amelyek az érintettek tudta nélkül gyűjtik a biometriai adatokat, mint például a távolról is működő arcfelismerő rendszer, az ujjnyomatok gyűjtése vagy az

emberi hang analizálása.

a biometriai adatok kezelésének jogalapja

Személyes adatok, így biometriai adatok is csak akkor kezelhetők, ha az érintett ehhez hozzájárul, vagy törvény ezt elrendeli [Avtv. 3. § (1) bekezdés]. A biometrikus azonosítás valójában automatizált egyedi döntéseket foglal magában, mivel számítástechnikai eszközzel hajtják végre és az érintett személyes jellemzőinek értékelése történik, ilyenre pedig csak akkor kerülhet sor, ha ahhoz kifejezetten hozzájárult, vagy azt törvény lehetővé teszi [Avtv. 9/A. § (1) bekezdés]. A hozzájárulás esetében kiemelendő az a magyar adatvédelmi törvényben is megfogalmazott követelmény, hogy a hozzájárulás csak akkor tekinthető érvényesen adott hozzájárulásnak, így csak akkor szolgálhat megfelelő jogalapként az adatkezeléshez, ha az az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez [Avtv. 2. § 6. pont]. Az adatkezelés jogellenes volta a célhozkötöttségi szabályok áthágása mellett a legtöbb esetben az önkéntes hozzájárulás hiányára vezethető vissza, bizonyos helyzetekben ugyanis eleve kizárt az önkéntesség. Erre mutatott rá a magyar adatvédelmi biztos is akkor, amikor megnyilvánult a biometrikus azonosító rendszerekkel összefüggésben. Állásfoglalása szerint az önkéntes hozzájárulás „annyit jelent, hogy az érintetteknek teljesen szabadon kell dönteniük arról, hogy megadják-e hozzájárulásukat, vagy sem. Nem beszélhetünk valódi önkéntességről, ha a hozzájárulás megtagadása esetén az érintetteknek munkájuk elvesztésével kell számolniuk.” (832/K/2000) Az önkéntesség kérdésének részletesebb vizsgálata nélkül is megállapíthatjuk, hogy bizonyos élethelyzetekben tényleg nem várható el az önkéntesség. Különösen igaz ez a munkahelyre, ahol a leggyakrabban alkalmaznak biometrikus azonosító rendszereket, és ugyanez a helyzet a közigazgatás által kibocsátott azonosító igazolványok biometriai adattal történő felszerelésekor is. Az önkéntesség fontosságának alátámasztására az adatvédelmi biztos azt is hozzáteszi, hogy „a biometria előnyeiről szóló ’Biometrikus Fehérkönyv’ – amely az egyik biometrikus azonosítóeszközöket forgalmazó cég honlapján

olvasható – 9. fejezetében említést tesz arról, hogy a felhasználók önkéntessége, a módszer általuk történő elfogadása szükséges a rendszer eredményes működtetéséhez is."

adatbiztonsági követelmények

Az adatbiztonság az adatvédelemmel összefüggésben annyit jelent, hogy az adatkezelő köteles gondoskodni az adatok biztonságáról, köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat a törvény szerint védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik [Avtv. 10. §]. A biometrikus azonosító rendszerek adatkezelési műveletei szinte kivétel nélkül elektronikusak. Adatbiztonsági intézkedések szükségesek minden biometriai adatkezelési mozzanatnál: a felvételkor, a sablonná alakításkor, a tárolással összefüggésben, az összehasonlításnál, stb.

Az adatkezelés első, a biometriai adatok felvételének fázisa az adatbiztonság szempontjából a legérzékenyebb fázis, ekkor alakítják ugyanis sablonokká a biometriai adatokat. A személyes és nem személyes adatok (például az átalakításhoz használt algoritmus) sérülése, vagy jogosulatlan megismerése ebben a fázisban nem pusztán az azonosító rendszer megbízhatatlanságát eredményezi, hanem az érintettek jogainak sérelmét is. Ha például egy ujjnyomatot a rendszer nem a hozzá tartozó személlyel kapcsol össze ebben a fázisban, akkor a továbbiakban ez a személy fog hozzáférni mindahhoz, amihez az ujjnyomat tulajdonosának kellene. Az ilyen hibák pedig elvezethetnek az úgynevezett személyiséglopáshoz is, hiszen a meglopott személy ujjnyomata a későbbiekben nem lesz használható, megbízhatatlan azonosítóvá válik, ennélfogva az érintettnek bizonyos korlátozásokkal kell szembenéznie.

A biometrikus azonosító rendszerek működése során felmerülő adatbiztonsági hibáknak számos hátrányos következménye lehet mind az érintettekre, mind pedig a rendszer üzemeltetőire nézve, különösen ha azok azt eredményezik, hogy a megfelelő személyt a rendszer elutasítja, az pedig, akit vissza kellene utasítania, tévesen azonosítja és átengedi. Azt gondolnánk, hogy a biometrikus azonosító rendszerek használata csökkenti a téves azonosítás valószínűségét. Valójában azonban azt a látszatot keltik, hogy az azonosítás és a személyazonosság-megállapítás csalhatatlan módszerét alkalmazzák. Hiba esetén az adatalanynak rendkívül nehéz vagy akár lehetetlen bizonyítania, hogy az azonosítás hibás. Ha például egy azonosító rendszer valakiről tévesen azt állapítja meg, hogy ő nem szállhat fel a repülőgépre, vagy nem léphet be egy meghatározott országba, könnyen úgy találja, hogy „megdönthetetlen" bizonyítékok állnak állításaival szemben, valójában nincsenek is igazán eszközei arra, hogy bebizonyítsa az igazát. Ilyen esetekben különösen fontos, hogy minden olyan döntés meghozatala előtt, amelynek valamilyen jogi hatása van az adott személyre nézve, ellenőrizni kell az automatizált egyedi döntések eredményét. Az ilyen automatizált egyedi döntések esetében lehetőséget kell biztosítani az érintettnek álláspontja kifejtésére [Avtv. 9/A. § (1) bekezdés]. Ha pedig az esetből bírósági eljárás lesz, az adatkezelés jogszerűségét (így a kezelt adatok pontosságát is) az adatkezelőnek kell majd bizonyítania [Avtv. 17. § (2) bekezdés].

a biometriai adatok mint különleges adatok

Nem nehéz belátni, hogy bizonyos biometriai adatok különleges adatoknak minősülhetnek, biometriai adatokkal összefüggésben elsősorban faji eredetre vagy nemzetiségi hovatartozásra, esetleg egészségi állapotra utaló különleges adatokra kell gondolnunk. Egy arcfelismerő rendszer például felismeri a felismerni kívánt személy bőrszínét, amelyből egyenes következtetés vonható le arra nézve, hogy melyik rasszhoz tartozik az illető. A különleges adatokat a törvény szigorúbban védi, így az ilyen adatokat is használó rendszerek esetében ezekre a többlet-garanciákra is figyelemmel kell lenni. Az olyan biometriai adatokat használó rendszerek esetében például, amelyek

különleges adatok kezelését is megvalósítják, nem lehet eltekinteni a hozzájárulás írásbeli voltától [Avtv. 3. § (2) bekezdés]. Mindez természetesen nem jelenti azt, hogy a biometriai adatok kezelése minden esetben együtt járna különleges adatok kezelésével. Az, hogy a rendszer tartalmaz-e különleges adatokat, leginkább a biometriai adatok felhasználási céljától, és attól függ, hogy a rendszer képes-e értékelni a különleges adatokra utaló speciális jellegzetességeket. A különleges adatok kezelése sokkal valószínűbb a képeket, tehát a nyers adatokat használó rendszerek esetében, tekintettel arra, hogy ezek ezeket a felismerhető jellegzetességeket szükségképpen tartalmazzák, míg a letisztított sablonok már nem feltétlenül, és a sablonokból az eredeti, nyers adatok már nem helyreállíthatók.

a biometriai adatok mint univerzális azonosítók

A biometriai adatokat egyedi adatokként definiáltuk, és ebből következően állíthatjuk azt is, hogy az azokból generált sablonok is egyediek. Egy adat, vagy egy sablon csupán egyetlen személyhez tartozhat. E jellemzőjük miatt az ilyen adatok könnyen válhatnak univerzális azonosítóvá, ha széles körben használják őket, ez pedig különösen akkor veszélyes, ha nemcsak a felhasználás köre tág, hanem az érintettek köre is, ha a lakosság nagy része ugyanazzal a biometriai adatával azonosítja magát. Ha végiggondoljuk mindazt, amit az Alkotmánybíróság a korlátozás nélkül használható, általános és egységes személyazonosító kódról, azaz a minden állampolgárnak és országlakosnak ugyanazon elv szerint kiosztott személyi szám alkotmányellenességéről mondott, akkor könnyen belátható, hogy ha ugyanazt a biometriai adatot használjuk az élet számos területén önmagunk azonosítására, akkor nem állunk messze a személyi szám korától, pláne akkor, ha ezt az adatunkat valamelyik személyazonosító okmányunkban is rögzítik. Az egységes személyazonosító szám, kód, jel, vagy más adat értelme az, hogy egy olyan rövid, technikailag könnyen kezelhető kód segítségével, amely megváltoztathatatlan és összecserélhetetlen, könnyedén és biztosan lehet azonosítani, illetve ugyanazon személy adatait összegyűjteni. (Lásd az Alkotmánybíróság 15/1991. (IV. 13.) AB határozata indokolásának III. 3. pontját, ABH 1991. 51.) Erre tekintettel mondja ki az adatvédelmi törvény, hogy korlátozás nélkül használható, általános és

egységes személyazonosító jel alkalmazása tilos [Avtv. 7. § (2) bekezdés].

A biometriai adatok korlátozás nélkül használható, általános és egységes személyazonosító jellé válása azonban elkerülhető, és ennek érdekében álláspontunk szerint az államnak kell lépéseket tennie. Az univerzális személyazonosító adat természeténél fogva különös veszélyt jelent a személyiségi jogokra, az államnak pedig az alapjogok védelmére vonatkozó elsőrendű kötelességéből [Alkotmány 8. § (1) bekezdés] következik, hogy ezt a kockázatot a legkisebbre kell csökkentenie: az általánosan használható egyedi azonosítók használatát – ugyanúgy, mint a személyi szám használatát is – garanciális szabályokhoz kell kötnie. Ennek érdekében két feltételnek kell teljesülnie. Egyrészt kerülendő a népesség-nyilvántartáshoz hasonló központi állami nyilvántartásba való felvétele az olyan biometriai személyes adatnak, amely széles körben történő használatára természeténél fogva számítani lehet, ezzel elkerülhető az Alkotmánybíróság által a hivatkozott határozatában a személyi számmal kapcsolatban kifogásoltak egy része. Az általánosan használt személyazonosító adat azonban az állami nyilvántartások nélkül is alkalmas lehet több adat összekapcsolására, ezért az államnak a jogi szabályozás útján intézkedéseket kell tennie annak érdekében, hogy ugyanazon fizikai jellemző átalakítása más és más matematikai manipuláción (titkosításon, zavaráson, maszkoláson) essen át az egyes biometriai eszközökön, vagyis a visszaalakíthatatlan sablonok előállítása más eljárással történjen az egyik adatkezelőnél, mint a másiknál, annak érdekében, hogy a sablonok ne legyenek összehasonlíthatók egymással.

adatvédelmi követelmények összefoglalása

A fentiek alapján a biometriai adatok felhasználása azonosítási célokra csak bizonyos követelmények teljesülése esetén engedhető meg a magánszféra kímélete, a veszélyek minimalizálása, valamint a biometriai adatokkal való visszaélés elkerülése érdekében. Az előzőekben kifejtettek szerint az alábbi tételek vázolhatók fel.

1. A nyers biometriai adatokat (például képeket) használó biometrikus

azonosító rendszerek sok veszélyt hordoznak magukban, ezért velük szemben előnyben részesítendők azok, amelyek az ilyen adatokból visszafordíthatatlanul képzett sablonok alkalmazásán alapulnak.

sablont használó rendszer

2. Azok a biometrikus azonosító rendszerek, amelyek nem járnak a biometriai adatok vagy sablonok adatbázisban történő kezelésével, adatvédelmi szempontból sokkal kevésbé lehetnek aggályosak, ezért az olyan megoldások fogadhatók el adatvédelmi szempontból, amelyek esetében a biometriai adat vagy sablon kizárólag az érintett birtokában van, olyan adathordozó eszközön, amelyhez kizárólag ő férhet hozzá, és az adatokat sehol máshol nem tárolják.

központban tárolás kerülendő

3. Ha elengedhetetlen az adatbázisok használata, mert az adatkezelés célja a személyazonosság megállapítása, vagy ha a biometriai adatokat az érintett által hagyott nyomokból gyűjtik össze, esetleg ha az érintett tudta nélkül történik az adatok felvétele, akkor az adatkezelés alapvető jogot érint, ezért csak olyan körülmények között lehetséges, ahol az érintettek valóban önkéntes hozzájárulásával történik mindez, vagy pedig a szükségesség és az arányosság követelményének figyelembevételével törvény rendeli el a biometriai adatok használatát. Ilyen, törvény alapján kötelező biometriai adatkezelést csak különleges biztonsági célok indokolhatnak.

megfelelő biometriai adat kiválasztása

4. Az általánosan használható személyazonosító adattá válás elkerülése érdekében népesség-nyilvántartásba biometriai adatot kötelezően felvenni nem szabad, ebből következően az állami azonosító rendszerek csak úgy támaszkodhatnak biometriai adatokra, ha azokat adatbázisban nem tárolják (lásd a 2. pontot).

népességnyilvántartás nem tartalmazhatja

5. Ugyanezen cél érdekében nem szabad megengedni, hogy a különböző célú biometrikus azonosító rendszerek ugyanazon fizikai jellemzőből ugyanazt a sablont állítsák elő.

sablonképzési variációk

2.3. Az ügyféloldali adatszolgáltatás és személyes részvétel minimalizálása

kitűzött célok

Mind az e-Közigazgatás 2010 Stratégia, mind az e-Közigazgatás 2010 Programterv munkaanyagai, mind pedig az egyes további háttéranyagok tartalmazzák az ügyféloldali adatszolgáltatás és személyes részvétel minimalizálásának követelményét. A Stratégia által a szolgáltatási folyamatok egyszerűsítése érdekében megfogalmazott kiemelt cél *„...az ügyféligények által vezérelt folyamatok kialakítása, az ügyfél oldali adatszolgáltatás és az ügyfél részvétele szükségességének minimalizálása az ügyintézési folyamatokban, valamint az élethelyzethez, vagy egymáshoz kapcsolódó folyamatok összekapcsolása."*

adatösszekapcsolási igények

Amennyiben feltételezzük, hogy a közigazgatás személyesadat-igénye nem csökken, sőt a jövőben tovább növekedhet, akkor e követelmény teljesítéséhez természetszerűleg az szükséges, hogy az érintettek adatait a szervek az érintett minimális közreműködésével, avagy közreműködésük nélkül, egymástól szerezzék be. A Stratégia és a Programterv ide kapcsolódó célkitűzései egyrészt a fejlettebb adatmenedzsment, vagyis *„[a]z adatok formai és tartalmi egységesítésének, standardizációjának megoldása, valamint az ágazati rendszerek közti, az adatvédelem követelményeivel összhangban álló adatintegrációs lehetőségek felmérése és interoperábilis adatkapcsolatok megteremtése",* másrészt a fejlettebb információmenedzsment, azaz *„[a]z informatikai rendszerek közti rendszer szintű együttműködési képesség megteremtése, a leggyakrabban keresett szolgáltatásokat működtető szervezetek között az együttműködés előmozdítása annak érdekében, hogy az információ megosztása és az együttműködés az egész közigazgatáson belül hatékonyabban történjen."* Noha fenti két idézet nemcsak személyes adatok kezelésére vonatkozik, a célok megvalósítása lényegileg érinti az érintettek személyes adatainak automatikus kezelését, főként megosztását, továbbítását.

Korábban többször hivatkoztunk az adatvédelem azon alapvető elveire és

törvényi rendelkezéseire, amelyekből következően az érintetteknek képesnek kell lenniük arra, hogy átlássák adataik sorsát, adataik kezelése (a törvényi felhatalmazással végzett adatkezelések kivételével) csak az ő tájékozott hozzájárulásuk esetén lehet jogszerű, a célhozkötöttség követelményeinek pedig az automatikus adattovábbítás körülményei között is teljesülniük kell. Könnyen belátható, hogy ezeknek az adatvédelmi követelményeknek az érvényesülését az automatizált személyesadat-csere vagy adattovábbítás alapvetően megnehezíti. A korszerű közigazgatás igényei ugyanakkor igénylik az ügyintézés elektronizálását, és erre ösztönöznek egyes EU elvárások is; emellett az érintettek számára is kézzelfogható előnyökkel járhat az ügyintézés ily módon történő egyszerűsítése. Ezért olyan adatkezelési megoldásokat kell találni, amelyek megőrzik a tervezett gyakorlati előnyöket, teljesítik a közigazgatás általános stratégiai célkitűzéseit, ugyanakkor elkerülik vagy minimalizálják az adatvédelem szintjének gyengítését.

adatvédelmi követelmények e körben figyelembe veendők

Az érintettek közreműködése nélküli személyesadat-szolgáltatás technikailag két módon képzelhető el; mindkettő koncepcionális szinten felbukkan a háttéranyagokban. Az egyik koncepció központosított adattárolást valósítana meg, ide fordulnának az adatigénylők a tevékenységükhöz szükséges személyes adatok bekérésére. (Megjegyezzük, hogy az alapvető személyazonosító adatok tekintetében ma is ezt a funkciót nyújtja a KEK KH, illetve e tekintetben elődszervezetei, a KÖANYVH és az ÁNH. Ezeket az adatokat ugyan más adatkezelők is kezelik, de a központi nyilvántartás az etalon, amellyel szükség esetén adategyeztetést végeznek. Fontos különbség azonban e központi nyilvántartás és más, személyes adatok központosított nyilvántartását célzó koncepciók között, hogy a KEK KH e funkciójában csupán a lakosság személyi és lakcímadatait tárolja, amelyek – eltérő mennyiségben és mértékben, de – minden adatkezeléshez szükségesek; ezen adatok adatminőségét, rendelkezésre állását és ellenőrizhetőségét biztosítja.)

központosított, többcélú adattárolás egyértelműen elvetendő

A másik koncepció szerint az adatkezelők a meglévő külön célú és adattartalmú nyilvántartásokból hívnák le a tevékenységükhöz szükséges

a célhozkötött adatkapcsolatokon alapuló adatlehívások megvalósíthatók

adatokat. Az eddigiekből következően adatvédelmi szempontból ez a megoldás, vagyis a meglévő rendszerek közötti adatkapcsolat kiépítése és megfelelő garanciákhoz kötése a kedvezőbb. Ez a koncepció jobban megfelel az osztott információrendszerek elvének, kielégítheti a célhozkötöttség követelményeit, tükrözi a közigazgatás szerveinek eltérő feladatait és felelősségi rendszerét, ellenőrizhetőségük kritériumait. Azonban egy ilyen megoldásnak is számos adatvédelmileg kritikus követelményt kell teljesítenie ahhoz, hogy már koncepciójában is megfeleljen az adatvédelmi elveknek és a hatályos jogszabályi rendelkezéseknek. Az alábbiakban olyan adatkapcsolati eseteket, illetve javaslatokat vázolunk fel, amelyek figyelembe veszik ezeket a követelményeket és adatvédelmi szempontból kívánatos szemléletet tükröznek.

a kívánt célt megvalósító egy lehetséges megoldás logikai modellje

Tegyük fel, hogy egy ügyfélnek egy közigazgatási ügyéhez szükséges adatai A, B, C és D szervnél vannak nyilvántartva, ő pedig a példa kedvéért az E szervnél indít eljárást (de természetesen indíthatna az A, B, C, D szervek bármelyikénél is). Az E szervnek tehát be kell szereznie az ügyfél adatait az A, B, C és D szervektől. E szervek némelyike ugyanazokat a személyes adatait kezeli az ügyfélnek, tehát az A, B, C és D szervek nyilvántartásai átfedőek az ügyfél tekintetében. Első lépésben eldöntendő, hogy az E szerv melyik adatkezelőtől kérjen be egy személyesadat-fajtát, ha az több szerv nyilvántartásában is szerepel. Ilyen esetben az adatkérést ahhoz az adatkezelőhöz kell címezni, amely vagy alapfunkciója miatt, vagy az adott ügyben játszott szerepe miatt az adatok elsődleges kezelője, és/vagy rendszeresen gondoskodik az adatok minőségéről, vagyis pontosságáról, teljességéről és időszerűségéről. (Az egy időpillanatra vagy feltétel bekövetkeztére, avagy cél teljesülésére vonatkozó személyes adatok önmagukban nem változnak, de vannak olyan személyes adatok, például családi állapot, tanulói jogviszony, adótartozás stb., amelyek rendszeres aktualizálása szükséges.)

Tekintettel arra, hogy az érintettet egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről [Avtv. 6. § (2)

bekezdés] még az adatkezelés megkezdése előtt, valamint hogy a tájékoztatás megadásának jogszerűsége és etikus volta elektronikus környezetben (távkapcsolatban) nehezebben biztosítható, javasoljuk, hogy a személyes adatok elektronikus úton történő bekérése minden esetben az ügyfél kezdeményezésére történjen, függetlenül attól, hogy az eljárás az érintett kérelmére indul-e (ahol adatainak – az ügyhöz szükséges – kezeléséhez való hozzájárulását vélelmezni kell), hiszen az elektronikus adatkapcsolat az ügyhöz nem elengedhetetlenül szükséges más adatokra is kiterjedhet, és függetlenül attól is, hogy az ügyfél hol és milyen azonosítási módszert, illetve eszközt használ.

mindg az ügyfél kezdeményezésére

A tájékoztatás megadása után az ügyfél kezdeményezésére E szerv elektronikus úton bekéri az ügyhöz szükséges adatokat. Az adatbekérés logikájának követnie kell a célhozkötöttség elvét. Nem arra kell tehát törekednie az adatkérő szervnek, hogy az ügyfél minél több adatát bekérje, hátha egy másik ügyben is szükség lesz rá, vagy netán több, az ügyben nem érintett adatalany adatait is bekérje, hanem pontosan az adott célhoz szükséges és elégséges adatok körére kell szorítkoznia, mivel a készletező adatgyűjtés tilalma elektronikus környezetben is fennáll. A szükséges és elégséges adatkör meghatározása természetesen nem informatikai, hanem közigazgatási feladat, bár informatikai eszközökkel támogatható. Például olyan esetben, ahol az eljáráshoz annak az adatnak az ismerete szükséges, hogy az ügyfél felsőoktatási intézmény nappali szakos aktív hallgatója-e, akkor az adatbekérés voltaképpen állapotlekérés: nem azt kell tudnia az E szervnek, hogy az ügyfél milyen intézményben milyen kurzust hallgat, hanem azt, hogy érvényes-e a hallgatói jogviszonya. Hasonlóképpen, ha csupán azt kell igazolni, hogy az ügyfél nagykorú-e, akkor elvben nem azt az adatot kell bekérni, hogy az ügyfél hány éves (és majd E szervezet megállapítja, hogy a kapott életkor nagyobb vagy egyenlő 18 évvel), hanem egy nagykorúságra irányuló kérdést kell intézni a nyilvántartó szervhez.

gyakran nem részletes adat, csak állapotlekérés szükséges

Az adatkérés jogalapját az adatkérőnek természetesen meg kell jelölnie (ez ügytípustól függően lehet fél-automatikus, de mindig számonkérhető formájú

és tartalmú), de az érintettre vonatkozó más személyes adat, például az ügy fejleményeivel összefüggő adatok nem továbbíthatók az átadó szerveknek; az adatáramlás tehát egyirányú. (Az adatkapcsolat technikai visszaigazolását célzó adatok cseréje lehetséges, azonban nem szükségképpen az alanyt azonosító formában.)

Az adatátadóknak – esetünkben A, B, C és D szerveknek – nyilvántartást kell vezetniük az átadott adatokról, azonban a célhozkötöttség követelményeiből következően ezeket az adatokat csak az érintett esetleges tájékoztatási igényének kielégítésére, az adatkapcsolat technikai ellenőrzésre használhatja fel, és nem például az ügyfél profiljának építésére (pl. hogy milyen szervtől hányszor kértek adatot róla).

Egy további szervnek, a példa kedvéért F-nek – amennyiben F nem tartozik ugyanannak a szoros értelemben vett eljárásnak a résztvevői közé, például fellebbviteli fórumként –, nem továbbíthatók az E szerv által az A, B, C és D szervektől bekért adatok.

Felvethető a kérdés, hogy ha az E szerv újból hasonló adatigényű eljárást indít ugyanazzal az ügyféllel kapcsolatban, vajon használhatja-e a korábban más adatkezelőktől begyűjtött adatokat (előkeresheti-e ezeket az adatokat az archívumából, ahol a korábbi ügy elektronikus aktáit tárolja). Álláspontunk szerint a példabeli E szerv ilyen esetben mindig újból kérje be az eljáráshoz szükséges személyes adatokat más adatkezelőktől, az ügyfél személyazonosító adatai kivételével (bár azokkal is végezhet eleve adategyeztetést a központi nyilvántartással). Ez az eljárás nemcsak a célhozkötöttség szempontjából előnyös, hanem az adatminőség biztosítása szempontjából is, mivel az adatok naprakészsége csak az elsődleges adatkezelőknél, vagyis a megfelelő adatátadó szervnél biztosított. Az újbóli bekérés kötelezettsége alól csak a többé már nem változó (egy időpillanatra vagy feltétel bekövetkeztére, cél teljesülésére vonatkozó) személyes adatok esetében lehet célszerű kivételt tenni.

Az E szerv birtokában lévő, az alany korábbi ügyeire vonatkozó származtatott adatok, például szabálysértési határozatok is csak akkor kapcsolhatók össze a jelenlegi ügyével vagy valamiféle „ügyfélprofillal", ha annak a jogszerűsége minden egyes esetben biztosított. Az átvett adatok esetében is érvényesülnek a célhozkötöttség követelményei: az átvett adatokat csak az előre meghatározott (és az adatkérésben megjelölt) cél teljesítéséhez és az ahhoz szükséges mértékben lehet csak felhasználni, valamint figyelemmel kell lenni a cél teljesülésének időpontjára, illetve az azt kiterjesztő jogszabályi rendelkezésekre; ezt követően pedig biztosítani kell az E szervnél az adatok helyreállíthatatlan törlését (vagy ha az adatokra statisztikai vagy más adatelemzési célból a későbbiekben szükség lehet, anonimizálását).

Végül általános követelményként gondoskodni kell az ilyen elvek alapján felépített és üzemeltetett adatkapcsolati rendszer adatvédelmi szempontú auditálhatóságáról.

2.3.1. Egyablakos adatváltoztatás és igazolásbekérés

A Megbízó által átadott dokumentumok az elektronikus ügyintézést lehetővé tevő elektronikus azonosítás mellett, mintegy másik megvalósítandó célként az adatváltozások bejelentése és átvezetése, valamint az ügyintézéshez szükséges igazolások beszerzése eljárásának egyszerűsítését jelölik meg. E cél az előzőekben, a 2.1. és 2.2. pontokban tárgyaltakhoz képest más jellegű megfontolásokat tesz szükségessé.

A cél az, hogy elegendő legyen az állampolgárnak az adatváltozást egyetlen hivatalban bejelentenie, amennyiben ő úgy akarja, a hivatal továbbítsa az adatváltozás bejelentését minden olyan szervezetnek, amelyhez jelenleg az állampolgárnak külön-külön is fordulnia kell. Az általunk jelenleg ismert szándékok szerint ez önkéntes alapon történne, vagyis nem lenne kötelező az egyablakos adatváltozás-bejelentés, a más szerveknek szóló változásbejelentést csak akkor venné fel a közigazgatási szerv, és azt csak

a kitűzött cél

akkor továbbítaná a címzetteknek, ha az állampolgár ezt kifejezetten kéri.

Az egyablakos adatváltoztatás adatvédelmi problémái az alábbiakban foglalhatók össze:

- Az adatváltozást és az igazoláskérést felvevő és továbbító szerv olyan adatokat is megismer (és esetleg megőriz), amelyek kezelésére ő nem jogosult, például az általa nem használt szektorális azonosítót, vagy az olyan más adatot, amely a nála vezetett nyilvántartásnak nem része, de a változással együtt más szervnél be kell jelenteni, vagy az igazoláskéréskor szükséges ennek is megadása (például ha a lakcímváltozással egyidőben megváltozik a polgár társadalombiztosítási jogállása is, akkor az ezzel összefüggő adatokat csak a társadalombiztosítás szerveinek kell bejelenteni, az okmányirodának, ahol a lakcímváltozást a polgár bejelenti, nem.).

jogalap problémája

- Az adatváltozást, igazoláskérést felvevő és továbbító hatóságoknál az egyes polgárokra vonatkozó olyan adatok gyűlnének így össze, amelyek az adott szerv feladatai ellátásához nem szükségesek, az adatkezelés ellentétes lenne a célhozkötöttség elvével, az osztott információs rendszerek doktrínájával, végső soron személyiségprofil kialakítására lennének alkalmasak. Az adatkezelés tehát nem felelne meg a célhozkötöttségi szabályoknak sem.

célhozkötöttség problémája

Ezek kiküszöbölésére az átadott anyagokban találunk megoldásokat, ezeket némi kiegészítéssel alkalmazhatónak és bevezethetőnek tartjuk. A legkidolgozottabb megoldást az MTA Információtechnológiai Alapítvány 2007. júniusi, Elektronikus azonosító bevezetése: elvárások és igének, következtetések és javaslatok című anyagában, annak a 42-43. oldalán találjuk.

A kidolgozott megoldás lényege, hogy az állampolgár számára a kliens program felajánlja az ügyfélnek, hogy az adatközlést a szükséges további

egy jó megoldás leírása

nyilvántartásokban is átvezeti, ha ezt szeretné, de elintézheti külön, önállóan is. A kliens által felsorolt hatóságok közül az ügyfél maga választja ki, melyeknél kíván így élni a bejelentés lehetőségével. A kliens a kiválasztott hatóságok listája alapján összeállít egy elektronikus űrlapot, amelyben a szükséges adatokat kell megadnia a polgárnak, ideértve a szakazonosítókat is. Az összegyűjtött adatok nem kerülnek semmilyen nyilvántartásba, azok megadása után a kliens az alkalmazás-címnyilvántartás alapján összeállítja az üzenetcsomagot, a kényes információt (a javaslat szerint ilyenek a szakazonosítók) az illető szakrendszer nyilvános kulcsával külön-külön titkosítja (az adószámot az APEH kulcsával, a TAJ számot az OEP-évl stb.), esetleg az egész bejelentést az ügyféllel elektronikusan aláíratja. Az üzeneteket a felvevő-továbbító szervnek adja át, amely azt az alkalmazás címnyilvántartás szerint címzettekre szétszedi, és a dokumentum-továbbító rendszerrel eljuttatja a célalkalmazáshoz.

Az MTA Információtechnológiai Alapítvány anyaga ugyanezt a módszert ajánlja a polgár ügyintézéséhez szükséges adatainak, igazolásainak beszerzésére is. Az ügyintéző készítené össze a bekérendő adatok listáját, amihez az ügyfél az űrlapon a fentiekhez hasonlóan megadná a szükséges azonosítókat is (pl. TAJ, adóazonosító), amelyek a kérésbe már az érintett szakrendszer kulcsával titkosítva kerülnek be. Itt az üzenet visszajelzési címet is tartalmazna, ez a cím az előbbiekben említett alkalmazás-azonosítási rendszerben használt alkalmazást, s azon belül a konkrét tranzakciót azonosítaná. A szakrendszerek automata alkalmazásai itt is ellenőrzik, jogosult programtól érkezett-e kérés, szerepel-e rajta az ügyfél (képviselő) beleegyező aláírása, és ha igen, a kívánt címre küldik a válasz üzenetet, az adatok tartalmától függően a kívánt titkosító kulccsal kódolva. Ez a javaslat kidolgozói szerint lehet az ügyintéző szakrendszer kulcsa, de speciális esetben lehet a felhasználó kulcsa (például különleges egészségügyi, bűnügyi adatoknál, amikor az összegyűjtött adatok megtekintését a felhasználó csak jelenlétében engedi meg, a saját kulcsával feloldva a titkosítást).

A vázolt módszer messzemenően figyelembe vesz az érintett önrendelkezési

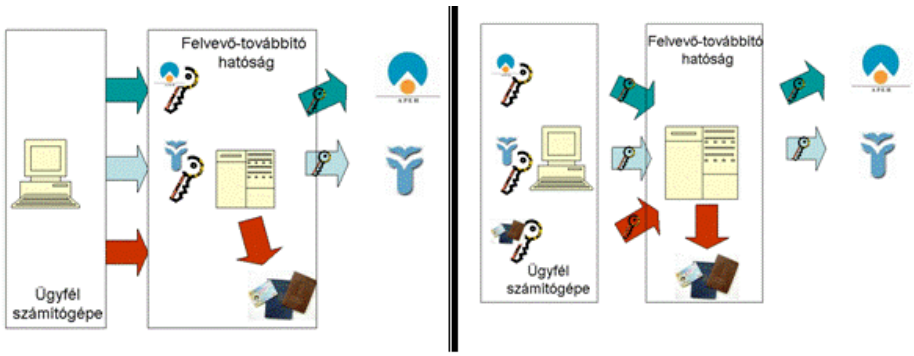
jogát, és fontos garanciákat tartalmaz az adatbiztonság érdekében, azonban az alábbi kiigazításokat tartjuk fontosnak:

1. Az ügyintézés ezen formája elsősorban az online ügyintézés során alkalmazható, nevezetesen ha a polgár otthonról, munkahelyéről, vagy nyilvános ügyfélterminálról intézi a saját ügyeit. Ha papír alapon indítja az ügyet, amit az ügyfélfogadó helyiségben az ablak mögött ülő ügyintéző rögzít és indít el elektronikusan (például az okmányirodában), akkor már megdől az az elv, hogy az adatokat felvevő és továbbító szervezet nem ismeri meg azokat az adatokat, amelyekhez neki semmi köze, csak postázza őket. Az offline (személyes, ügyintéző segítségével történő) ügyintézés ezért más jellegű garanciákat igényel (polgár pozitív hozzájárulása, a felvett adatok megőrzésének kizárása, stb.).

a javaslat csak online ügyintézésben értelmezhető

2. Online ügyintézés esetén csak akkor elfogadható a fenti megoldás, ha a kliens úgy van kialakítva, hogy a kitöltött űrlap adatai nem titkosítottan utoljára csak az ügyfél számítógépén vannak, onnan már eleve a címzett szervek nyilvános kulcsaival titkosítottan kerülnek elküldésre, a szükséges szkriptek az ügyfél számítógépén kerülnek lefuttatásra, nem pedig az adatok elküldése után a felvevő-továbbító hatóság számítógépén. Ezzel kerülhető ugyanis el, hogy a felvevő-továbbító hatóság olyan adatokat is megismerjen, amelyeket nem kezelhet. Ezt hivatott ábrázolni az alábbi két ábra:

titkosítás a polgár felületén



Rossz megoldás **Jó megoldás**

3. A felvevő-továbbító szerv a titkosított adatokat sem tárolja. A titkosítás a

mai ismereteink szerint ésszerű erőfeszítéssel nem visszafejthető, de nem is szabad módot adni arra, hogy ha esetleg ez megváltozik, az adatokat a felvevő-továbbító szerv megismerje.

a továbbított adatok nem tárolhatók

4. A fent leírt megoldáshoz képest fontosnak tartjuk, hogy az ügyfél számítógépéről ne csak az érzékeny, és ne is csak a felvevő-továbbító hatóság által nem kezelhető adatok kerüljenek titkosítva elküldésre. A kliensnek az ügyfél számítógépén címzett hivatalonként olyan adat-csomagokat (dokumentumokat) kell létrehoznia, amely az egyes címzettekhez eljuttatandó valamennyi adatot tartalmazza, és mindegyiket a címzett nyilvános kulcsával titkosítania kell, mielőtt az adatokat elküldi a felvevő-továbbító szervnek. Ennek elsősorban adatbiztonsági okai vannak.

minden elküldött adatot titkosítani indokolt

5. A javaslat nem dönt abban a kérdésben, hogy szükséges-e az ügyfél elektronikus aláírása a művelethez, azt csupán egy esetleges kelléknek tekinti. Álláspontunk szerint az aláírás minden esetben indokolt, ez biztosítja ugyanis, hogy az érintett valóban önrendelkezési jogát gyakorolva indítja meg ezt az eljárást, és nem valaki más, illetéktelen teszi ezt helyette. A Ket. 36. § (3) bekezdése szerint egyébként is írásban kell kérnie az ügyfélnek, ha azt akarja, hogy a hatóság maga szerezze be más hatóságtól a különféle adatokat, igazolásokat. A kidolgozott eljárás alkalmas lehet különleges adatok továbbítására is, amelyek kezeléséhez írásban adott hozzájárulást kíván meg a törvény [Avtv. 3. § (2) bekezdés], ez pedig szintén az aláírás megkövetelése mellett szóló érv.

ügyfél aláírása szükséges

6. Az ügyintézéshez szükséges adatok, igazolások különböző hatóságoktól történő beszerzésére javasolt megoldás nyitva tartja azt a kérdést, hogy az adatkérésre válaszul érkező adatok az adatkérést felvevő és továbbító szerv, vagy az adatalany nyilvános kulcsával titkosítva érkezzenek vissza. Álláspontunk szerint az adatalany (ügyfél) nyilvános kulcsával titkosított válaszadás indokolt, hiszen ő jogosult a visszaérkező adatok ismeretében eldönteni, hogy akarja-e folytatni az általa megindított

a válasz érkezzen titkosítva

eljárást, függetlenül attól, hogy különleges adatokról van-e szó, vagy sem (a különleges adatokon kívüli személyes adatok is lehetnek érzékenyek, az adatalany a visszaérkező igazolás ismeretében még elállhat eredeti eljárás-kezdeményezésétől). Indokolt, hogy az eljáró szerv a másik szervtől az adatalany kérésére érkező adatokat addig ne ismerje meg, amíg azt az adatalany maga meg nem engedi. Ez önrendelkezési jog gyakorlásának fontos garanciája, ugyanakkor nem érinti az így beszerzett adatok és igazolások tartalmának hitelességét.

A javasolt megoldást tehát – a fenti kiegészítésekkel – megvalósíthatónak tartjuk, nemcsak azért, mert tiszteletben tartja az érintettek információs önrendelkezési jogát, hanem bizonyos mértékben a jelenlegi állapothoz képest ki is terjeszti azt, további döntési jogokat ad az adatalanyok kezébe adataik sorsát illetően. Hangsúlyozzuk azonban, hogy a javasolt megoldás csak kiegészítő jelleggel működhet, az adatalanyok hozzájárulása alapján (amennyiben nem bíznak a hatóságokban, a kliensek titkosító funkciójának működésében, stb., akkor nem ezt választják), és akkor is csak online környezetben, amikor ő maga adja meg elektronikusan az adatokat, és nem ügyintéző segítségével teszi ezt. Érdemes gondolni arra is, hogy a közigazgatás bármely szerve csak akkor tesz valamit (például vesz fel adatokat, gondoskodik azok továbbításáról), ha számára előírnak ilyen feladatot, egyéb esetben nem. Az ügyintézéshez szükséges adatok, igazolások beszerzésével összefüggésben a közigazgatási szerveknek a törvény előír ilyen feladatot (Ket. 36. §), az adatváltozások tekintetében azonban nem, ezért e körben szükséges lehet – ha nem is adatvédelmi, hanem közigazgatási jogi okokból – a törvénymódosítás.

a megoldás csak alternatív eljárás lehet

A fenti technikai megoldás adaptálható az „e-Közigazgatás Programterv 2001” című dokumentum 24. pontjában említett azon eljárásokra, amelyek az ügyfél élethelyzetéhez igazítva egyszerre indítják el az egymástól függetlenül folyó eljárásokat (one-stop-shop). Hangsúlyozni kell azonban, hogy az ilyen eljárás-kezdeményezés, csak nagyon részletes tájékoztatás mellett történhet.

tájékoztatás szükséges

2.3.2. Személyes adatok, dokumentumok központi tárolása, adatletét

A Megbízó által feltett kérdések között, a „Kapcsolódó további kérdéskörök" kategóriájában szerepelt egy központi szolgáltatásként kialakított – állami vagy privát üzemeltetésű – adattár elképzelése, amelyben az érintett személyek saját kulcspárjuk nyilvános felével kódolva tárolhatnák a rájuk vonatkozó adatokat, dokumentumokat. Hasonló elképzelések az áttanulmányozott háttéranyagokban is felvetődtek.

Megítélésünk szerint az elektronikus közigazgatás korszerű, ügyfélbarát szolgáltatásává válhatna egy ilyen tárhely, ehhez azonban az szükséges, hogy a szolgáltatás kielégítse az alábbi adatvédelmi követelményeket.

1. Az állam által biztosított tárhely a hozzá kapcsolódó informatikai szolgáltatásokkal nem lehet kötelező vagy kvázi-kötelező használatú az ügyfelek számára, csupán opcionális lehetőség.

használata csak önkéntes lehet

2. Az állam nem monopolizálhatja e szolgáltatás nyújtását; az üzleti szektor szolgáltatói számára is lehetővé kell tenni ilyen szolgáltatás nyújtását, amennyiben megfelelnek az adatkezeléssel szemben támasztott informatikai (funkcionális és biztonsági) követelményeknek.

állami monopólium kerülendő

3. Akár állami, akár magánszervezet nyújtja a szolgáltatást, meg kell határozni a szolgáltatásra vonatkozó adatbiztonsági követelmények minimális szintjét, valamint a kulcskezeléssel kapcsolatos követelményeket, és ezek gyakorlati megvalósulását rendszeresen ellenőrizni kell. Gondoskodni kell arról, hogy az adattárban tárolt adatok, illetve dokumentumok kizárólag az érintett személy számára legyenek értelmezhetők, visszafejthetők. A szolgáltatás ezért nem képzelhető el titkosításra alkalmas kulcsok használata nélkül

az adatbiztonsági követelményeket rögzíteni és ellenőrizni kell

titkosító kulcsot feltételez

4. Tekintettel arra, hogy nem lehet kizárni azt a lehetőséget, hogy az adatalany kulcspárjának titkos feléhez is hozzájuthat illetéktelen fél, a

időben korlátozott érvényességű adatok

kulcskezelés követelményei közé tartozik a kulcsok rendszeres cseréje (lásd a 2.1.1. pont alatt a 3. észrevételben az 54.oldalon is). Amennyiben például az adatalany önként vagy valamilyen vélt előny fejében önként a központi nyilvántartó tudomására hozza a titkos kulcsát, akkor a központi szolgáltató által megismert adatok kezelésének jogalapja esetleg igazolható lenne, az adatok célhozkötött kezelése azonban nem biztosítható. Ha pedig az adatalany környezetéből valaki megismeri az adatalany titkos kulcsát, akár egy teleház személyzete, akár egy rosszindulatú felhasználó, akkor egyszerre számos személyes adathoz, illetve személyes adatot tartalmazó dokumentumhoz juthat hozzá.

5. Biztosítani kell azt is, hogy az adatalany a tárhellyel biztonságos csatornán keresztül kommunikáljon, függetlenül az általa használt végberendezés fajtájától.

biztonságos kommunikáció a tárhellyel

6. Tárhely szolgáltatást e követelmények mellőzésével is lehet nyújtani – ahogy azt ma is nyújtanak egyes szolgáltatók – de ezek megnevezését meg kell különböztetni a fenti biztonságos tárolási szolgáltatástól, és gondoskodni kell arról, hogy reklámozásuk ne tévessze meg a felhasználókat. Kifejezetten kerülendő olyan tárhely szolgáltatás alkalmazása, amelynél az adatalany valamilyen függő viszonyban áll a szolgáltatóval; ilyen lehet például a munkahely, illetve a munkáltató által nyújtott szolgáltatás.

más tárhelyek

7. A biztonságos tárhely célja az, hogy a polgárok maguk – és csakis ők – helyezzék el itt elektronikus irataikat és maguk – és csakis ők – férhessenek hozzá az itt tárolt irataikhoz. Ebből következően más, akár állami, akár üzleti, akár egyéb adatkezelő e tárhelyre nem küldhet adatokat, illetve dokumentumokat, illetve innen nem olvashat ki, még az adatalany felhatalmazásával sem.

a tárhellyel csak az adatalany kommunikál, más nem helyezhet el ott adatot, és nem is kérdezhet le

8. Az ilyen tárhely nem lehet hiteles elektronikus adat-, illetve iratforrás. Ha az lenne, akkor a polgárok egy idő után mégis arra kényszerülnének,

nem társulhat hozzá a hitelesség, mint jogkövetkezmény

hogy minden hivatalos iratukat itt helyezzék el, mivel később csak azt a dokumentumot tudják hitelesként elfogadtatni, amit innen töltenek le. A hitelességet más úton kell biztosítani – erre a megvizsgált koncepciók több bevált megoldást tartalmaznak, amelyek adatvédelmi vonatkozásait a 2.1. pont alatt elemezzük.

9. A tárhely ne válhasson egy személy összes személyes adatának, illetve személyes adatokat tartalmazó iratainak őrzőjévé. Az adattárolás lehetőleg legyen mindig az adatkezelési célhoz illeszkedő, legalább is adatkezelési szektoronként: az orvosi leleteket például ne ugyanott tárolják, mint az adóbevallásokat.

10. A tárhely a fentiek miatt nem alkalmas személyazonosítók, főként szakazonosítók hiteles tárolására (a hangsúly itt a hitelességen van). Az ugyanakkor nem zárható ki, hogy az adatalany itt (is) tárolja ilyen adatait.

11. A személyes adatok, illetve személyes adatokat tartalmazó iratok biztonságos tárhelyen történő tárolása természetesen digitális másolatok tárolását jelenti. Ha a tárhely az adatalany számára valamilyen ok miatt korrumpálódik, például az adatalany elveszíti a magánkulcsát, vagy az más tudomására jut, az adatalanynak képesnek kell lennie arra, hogy az ott tárolt adatait helyreállíthatatlanul törölje. Amennyiben maga a tárhely megy tönkre helyreállíthatatlanul, akkor – mivel másolatokról, ráadásul nem hiteles másolatokról van szó – az adatalany újból összeszedheti az adatokat, dokumentumokat az eredeti adatkezelőktől (egyes speciális, például a hivatal és az ügyfél közötti kommunikációt bizonyító üzenetek, visszaigazolások kivételével).

törlés biztosításának lehetősége

2.3.3. Adatösszekapcsolás egyszer használatos kapcsolati kóddal

Az 1.2. pont alatt ismertetett, „hagyományos”, a hatályos jogszabályokban szabályozott kapcsolati kódot egy ideiglenes számsorként definiáltuk, amely ugyanakkor alkalmas arra, hogy rendszeres adatszolgáltatás történjen egy-

hagyományos kapcsolati kód

egy adatalany személyes adatai tekintetében. Használata lehetővé teszi az eltérő célú és adattartalmú nyilvántartások célhozkötöttségen alapuló, jogszerű kapcsolatát. A kapcsolati kód természetesen technikailag nem teszi lehetetlenné a külön célú nyilvántartások jogellenes összekötését, de megnehezíti azt, és egyben világos informatikai és adminisztratív korlátot testesít meg a közigazgatási adatkezelők és dolgozóik számára. A kapcsolati kód azonban arra is alkalmas, hogy csupán az egyes adatkezelőknél legálisan kezelt kapcsolati kódok alapján, a kapcsolati kódok segítségével végrehajtott adatkapcsolatok naplózásával olyan adatok kerüljenek az egyes adatkezelők kezelésébe, amelyek nem tartoznak a feladatukhoz (például hogy kiről milyen adatkezelő milyen gyakorisággal milyen adatokat kér), és így a célhozkötöttség szempontjából mintegy „káros mellékhatást" képviselnek.

Az interoperabilitás jelenlegi követelményei ismét aktuálissá tették a kapcsolati kód kérdéskörének, alkalmazhatóságának vizsgálatát, amit az is indokol, hogy értesüléseink szerint a hagyományos kapcsolati kódok rendszere nem működik kielégítően, vagy legalább is nem illeszkedik az elektronikus közigazgatás fejlesztési elképzelései közé.

egyszer használatos kapcsolati kód

Olyan elképzeléssel is megismerkedtünk, amely szerint a közigazgatás adatkapcsolatainak megvalósítása az egyes nyilvántartások között egyszer használatos kapcsolati kód alkalmazásán alapul. Lényege, hogy az adatkapcsolatban a nyilvántartások egyfelől saját nyilvános/titkos kulcspárjaikat használják, másfelől olyan, egyetlen adatkérésben használt kapcsolati kódokat, amelyek két adatkezelő közötti kapcsolatban még az ugyanazon személyre vonatkozó adatkérések illetve -továbbítások esetén is megváltoznak minden kapcsolati kezdeményezésben. Lépései a következők:

az összekapcsolás lépései

Az adatkérő szerv egy véletlen elemet tartalmazó kapcsolati kódot generál, azt saját nyilvános (!) kulcsával kódolva küldi át az adatszolgáltatónak, megjelölve az érintett személy természetes személyazonosító adatait (nevét, születési idejét stb.). Az adatszolgáltató a számára visszafejthetetlen módon titkosított kapcsolati kódot az érintett személy kért adataihoz kapcsolja és ezeket együttesen visszaküldi az adatkérőnek. Az adatkérő saját kulcsával

visszafejti az egy bizonyos adatalanyra vonatkozó, általa generált egyszer használatos kapcsolati kódot, és a megkapott személyes adatokat ennek alapján hozzárendeli a saját nyilvántartásában az érintett személyhez. Amikor az adatkérő a kért adatok megérkeztét visszaigazolja, egyszersmind törli a már felhasznált kapcsolati kódot, generál egy újabbat, és azt hasonlóképpen titkosítva küldi meg az adatszolgáltatónak, aki ugyancsak törli egyszeri adatszolgáltatásra már felhasznált (titkosított) kapcsolati kódot és kicseréli az új (titkosított) kapcsolati kóddal. A visszaigazolás után tehát mind a két szervezet egy új (még fel nem használt) kapcsolati kódot tárol az adott személyre vonatkozóan, amelyet a következő adattovábbításkor fognak felhasználni, azt követően pedig újból lecserélni.

előnyös, mert kapcsolati profil nem jön létre

A vázolt megoldás előnye, hogy a nyilvántartásokban szereplő személyek adatainak összekapcsolása egyedi, és így ellenőrizhető adatkéréseken és válaszokon alapul, és egyik szervnél sem keletkezik csupán az adatkapcsolatok naplózásából származó „kapcsolati profil" az érintett személyek vonatkozásában. Ebből adódó előny, hogy a történeti adatok felhasználásával sem állítható elő utólag a nyilvántartások adatainak összegyűjtése az érintett személyről a kapcsolati kódok alapján.

a naplózást ellehetetleníti

A „kapcsolati profil" felépíthetőségének elkerülése adatvédelmi szempontból előnyös, ugyanakkor hátrányt is jelent abból a szempontból, hogy az Avtv. által előírt adattovábbítási naplózás [12. § (1) bekezdéséből következő kötelezettség] nem valósítható meg vagy tartalmát tekintve kiüresedik. Ez a naplózási kötelezettség ugyanis nemcsak az adatkezelő védelmét szolgálja olyan esetekben, amikor bizonyítania kell az adattovábbítás megtörténtét vagy annak jogszerűségét, hanem az adatalany védelmét is: e naplózott adattovábbítási adatok segítségével tudja utólag is követni személyes adatainak sorsát. A fenti adatvédelmi előnyök és hátrányok mérlegelésnél azonban a profilépítés megakadályozását tartjuk fontosabbnak. A naplózás elmaradásából származó járulékos hátrányok csökkentésére az alábbi megoldást javasoljuk: minden adattovábbításnál az érintett személy kapjon automatikus értesítést az adattovábbító szervtől, amelyből kiderülnek az

más garanciával pótolható

adattovábbítás legfontosabb jellemzői. Amennyiben az érintett ezeket az értesítéseket archiválja (például a másutt elemzett adattári szolgáltatás igénybevételével), a későbbiekben képes a róla szóló adatok sorsát követni. Ha nem archiválja (vagy egyáltalán nem rendelkezik az elektronikus ügyintézésben felhasználható eszközökkel, például nincs e-mail címe), ez a lehetősége természetesen elveszik.

titkos kommunikáció szükséges

Az ismertetett elképzelés az adatszolgáltató részéről a személyes adatok titkosítatlan formában történő elküldését tartalmazza (a titkosított kapcsolati kóddal együtt). Megítélésünk szerint további biztonsági garanciát nyújtana, ha az adatszolgáltató az átküldött adatcsomagot (benne a másik szerv által generált, titkosított kapcsolati kóddal) a saját titkos kulcsával kódolná, amit a fogadó fél természetesen ki tud nyitni.

központi szolgáltató által generált egyszer használatos kapcsolati kód

Az ismertetett elképzelésnek van központi szolgáltatást is magában foglaló, kiterjesztett változata is. Ebben az egyszer használatos kapcsolati kódokat egy központi szerv (az elképzelés szerint a KEK KH) generálná és küldené meg az adatkérőnek, illetve az adatszolgáltatónak. Mindkét megoldást, a két adatkezelő közötti közvetlen kapcsolaton alapuló, és a központi szolgáltató igénybevételével megvalósított adatkapcsolatot adatvédelmi szempontból kielégítőnek tartjuk, sőt, előnyösebbnek a „hagyományos” kapcsolati kód alkalmazásánál. A központi szolgáltató bevonása esetén azonban teljesülnie kell annak a követelménynek, hogy a központi szolgáltató – amennyiben nem közvetlenül teljesít adatkérést, hanem két, egymással adatkapcsolatba lépni kívánó szervezet számára generál kapcsolati kódokat – ne kerüljön olyan személyes adatok birtokába, amelyek a két adatkezelő között kapcsolatból származnak vagy arra vonatkoznak. A központi szolgáltató bevonásával, egyszer használatos kapcsolati kódok segítségével történő adattovábbítások esetében is javasoljuk az érintettek automatikus értesítését adataik továbbításáról, a fentebb ismertetett módon.

3. Néhány további szempont a személyesadat-kezelő rendszerek informatizálásához

A Megbízó előtt is ismeretes, hogy a háttéranyagokból megismert tervek, megoldási alternatívák számottevő része tisztán informatikusi szemléletet tükröz, amelynek jellemzője, hogy az informatikai rendszerek tervezésének és üzemeltetésének egyszerűsítése, az alapkoncepcióban kitűzött célok megvalósításának hatékonysága elsőbbséget – gyakran kizárólagosságot – élvez más, köztük adatvédelmi szempontokkal szemben. Ennek egyik következménye az, hogy az interoperabilitás és az egyablakos ügyintézés követelményét a javaslatok egy része megfelelő adatvédelmi garanciák nélkül, centralizált adatkezelési rendszerek alkalmazásával kívánja megoldani.

3.1. Információtechnológiai szempontok

Noha a dokumentumok elemzése során találkoztunk adatvédelmileg kielégítő, sőt kifejezetten előnyös megoldási javaslatokkal is, amelyek korszerű adatvédelmi szemléletet tükröznek (és amelyekre korábban kitértünk), szükségesnek ítéljük, hogy a jövőben a közigazgatás személyesadat-kezelési rendszereit érintő informatikai fejlesztésekben a Megbízó gondoskodjon arról, hogy már a koncepció kialakításánál, és azt követően a tervezés minden fázisában jelen legyen az adatvédelmi szakértelem. Azzal, hogy e jelenlét egyaránt megkíméli a Megbízót és fejlesztőt attól, hogy esetlegesen megvalósítási akadályokba ütköző koncepciókat dolgozzanak ki, nemcsak a kifejlesztett rendszer adatvédelmi színvonalának biztosítását eredményezi, hanem a tapasztalatok szerint erőforrás-megtakarítást is.

adatvédelmi szempont érvényesítése a koncepcióalkotáskor

Ezen túlmenően szemléletileg is kívánatos, hogy az adatvédelmi követelményeket se a Megbízó, se az informatikai fejlesztő és kivitelező ne értelmetlen külső korlátozó feltételnek, hanem az adatkezelés integráns részének tartsa. Ennek érdekében javasoljuk, hogy a rendszertervezők és

fejlesztők vegyék figyelembe azokat a sajátos, nemzetközileg ismert információs technológiákat, amelyeket egyfelől az adatkezelők, másfelől az adatalanyok alkalmazhatnak, és amelyek célja az adatvédelmi követelmények gyakorlati teljesítése az informatikai rendszerekben. Ilyen információtechnológiai megoldások lehetnek például az elkülönítendő adatkezelések közös hardveren és szoftveren futtatásánál az adatbázisok struktúrájának megfelelő felépítése, egyes adatkezeléseknél adatvédelmi célú alkalmazásokat támogató jelölő nyelvek (pl. EPAL) rendszerbe illesztése, adatkezelő-centrikus identitásmenedzselés helyett felhasználó-centrikus identitásmenedzselés bevezetése, stb. A jövőbeli rendszerek tervezésénél érdemes figyelembe venni a jelenleg folyó nemzetközi felhasználóbarát identitásmenedzselési (IDM) rendszerek fejlesztését, például a PRIME projektet, és felkészíteni a fejlesztendő rendszereket a PRIME vagy hasonló IDM rendszerekhez való csatlakozás lehetőségére. Ezen túlmenően, az elektronikus ügyfélkapcsolatok részeként, jellemzően a személyazonosítást nem igénylő tájékoztatási funkciók nyújtásánál, kívánatos a Privátszférát Erősítő Technológiák (Privacy Enhancing Technologies, PET) – például anonim böngésző vagy üzenetküldő szolgáltatások – használatának lehetővé tétele.

adatvédelmi szempontú információtechnológiai megoldások

privátszférát erősítő technológiák

A nem speciálisan adatvédelmi technológiai megoldások között kiemelt szerepet játszhatnak az informatika mai fejlettségi szintjén általánosan ismert, kipróbált és tömeges alkalmazásra kifejlesztett, ugyanakkor nem túlzott számításigényű eljárások, amelyek egyirányú adat-átalakításon alapulnak. Ezek lényege személyesadat-kezelési szempontból, hogy megbízhatóan képesek személyes adatokból kódolt, önmagukban értelmezhetetlen adatokat előállítani oly módon, hogy azonos kiinduló adatokból bizonyíthatóan mindig azonos eredményt, vagyis átalakított, önmagukban értelmezhetetlen adatokat eredményezzenek. Akárhányszor ismételjük meg az eljárást a kiinduló adatokon (esetünkben személyes adatokon), mindig ugyanazt az átalakított adatot kapjuk eredményül; ha viszont bármilyen kis változás történik a kiinduló adatokban, az eredmény, vagyis az átalakított adat lényegesen eltérő lesz. Az ilyen eljárásokat azért

egyirányú adat-átalakítások

nevezik egyirányúnak, mert az átalakítást egyik irányban könnyű elvégezni, a visszaalakítás pedig gyakorlatilag lehetetlen, vagy legalább is ésszerű erőfeszítéssel nem lehetséges. A személyes, illetve különleges személyes adatokon végzett egyirányú adat-átalakítási eljárások eredményeképpen kapott adatok egyedi, anonimizált adatoknak tekinthetők olyan adatkezelők kezelésében, akiknek vagy amelyeknek sem jogi, sem technikai lehetőségük nincs megismerni a kiinduló adatokat.

3.2. Logikai, szervezési szempontok

személyes adatok kérése helyett állapotlekérdezések

A célhozkötöttség azon követelménye, amely szerint csakis a szükséges és elégséges – az adatkezelés céljának megvalósulásához elengedhetetlen – mértékű adatkezelés jogszerű, esetenként úgy is teljesíthető az adatkezelő rendszerek között kapcsolatban, hogy az adatkérő szerv állapotlekérdezéseket, feltételek, igazolások meglétére vonatkozó információkat igényel, és nem egyéb személyes adatok átadását kezdeményezi.

adatvédelmi hatásvizsgálat

Az adatvédelmi szempontokat természetesen nemcsak az informatikai fejlesztésben és a rendszerek koncepcionális megtervezésében, hanem a jogi elemzésben, a döntési szempontrendszer kialakításában is érvényesíteni kell; ennek egyik nemzetközileg elfogadott módszere az adatvédelmi hatásvizsgálat lefolytatása, amit a későbbiekben, a 3.3. pont alatt részletesebben ismertetünk.

a közigazgatás nem egységes adatkezelő

Már a koncepcionális alapok kidolgozásánál figyelembe kell venni mind adatvédelmi, mind pedig közigazgatási szempontból, hogy az állam nem egységes, monolit adatkezelő (különösen nem tekinthető annak az állami szervek és a magánszektor szervezeteinek szövetsége), amely egységesen áll szemben az adatalannyal. A hatalmi ágak alapvető megosztása mellett a közigazgatás szervezeteinek egymáshoz való viszonya is tükrözi sajátos feladataikat és felelősségüket, amelyet személyesadat-kezelési tevékenységük és jogosítványaik terén is érvényesíteniük kell. Az

informatizálás elősegítheti e szervek adatkapcsolatainak hatékonyabbá tételét, az ügyfelekkel való kapcsolattartásuk egyszerűsítését, de nem moshatja össze feladatkörüket és felelősségüket, sem a közigazgatás belső rendszerében, sem az ügyfelekkel szemben, sem pedig a társadalom általi átláthatóságuk és elszámoltathatóságuk általános szempontjából. Az elektronizálás nem változtatja meg lényegileg a közigazgatás alapvető szervezeti tagozódását, a szervek egymás közti viszonyainak rendszerét; ezeknek világosan kell tükröződniük az új elektronikus szolgáltatásokban is. Ennek az elkülönülő feladatbeli és felelősségbeli meghatározottságnak a jogi és közigazgatási jelentősége megítélésünk szerint nem mindig egyértelmű az informatikusok számára.

az elektronikus ügyintézés, elektronikus közigazgatás is legyen átlátható

Fontos szempont, hogy az adatalany továbbra is, sőt egyre könnyebben tájékozódhassék az elektronikus ügyfélkapcsolat keretei között, az egyablakos felület ne fedje el az adatalanyi/adatkezelői viszonyok sajátosságait; enélkül nem várható a tájékozott, öntudatos állampolgári viselkedés kialakulása, hosszabb távon a közigazgatás – és ezen belül az elektronikus ügyfélkapcsolat – iránti bizalom növekedése. Az ügyintézés folyamatának átláthatóságát az elektronikus közegben is biztosítani kell. A bonyolult elektronikus folyamatoknak a laikus ügyfél számára könnyen érthetővé kell válniuk, ugyanakkor a mélyebben érdeklődő számára több szinten is ellenőrizhetővé, megmagyarázhatóvá. Az e-szolgáltatások felhasználóinak körében tapasztalható divergencia egyrészt az egyre figyelmetlenebb és felületesebb laikus, másrészt a tájékozott, a szolgáltatások technikájában és gyakorlatában járatos érdeklődő között megkívánja a szolgáltatások ergonómiai tervezésében, hogy az elektronikus ügyintézés mindkét réteget megfelelően tudja kiszolgálni, s ezzel az ügyfelek széles körének biztosítsa személyes adataik sorsának átláthatóságát.

Ehhez kapcsolódó – nem adatvédelmi, hanem inkább az adatkezelés etikáját érintő – kérdés, hogy a szolgáltató állam koncepciója, minden előnyével együtt, nem keltheti azt az illúziót, hogy az állam kizárólag „szolgáltatna” állampolgárainak, különösen egyéni szinten. Az ügyfél életét meg lehet és

meg kell könnyíteni az egyre bonyolódó adatkezelési viszonyok között, de ez csak a felületet, a kapcsolatteremtés és bonyolítás könnyítését jelenti, ettől még az érintetteknek mindenkor tisztában kell lenniük azzal, hogy az ügyfélbarát, szolgáltatás-centrikus ügyintézés mögött milyen hatósági funkciók állnak.

alternatív eljárások

Az elektronikus ügyfélkapcsolaton alapuló közigazgatási rendszerekben eleve gondoskodni kell a személyes adatokat érintő alternatív eljárások kidolgozásáról, alternatív azonosítási módok elfogadásáról, egyfelől a centralizálás elkerülésére és az adatalanyi önrendelkezés lehetőségének technikai biztosítására, másfelől rendszerhibák, leállások esetére. A közigazgatás működőképességét az informatikai rendszer rendelkezésre állásának átmeneti hiánya esetén is biztosítani kell, a rendkívüli üzemmód – például manuális adatkezelési műveletek alkalmazása – azonban nem jelentheti az adatvédelmi követelmények figyelmen kívül hagyását, az adatvédelmi szint gyengítését, legfeljebb a követelményeket más technikai körülmények között kell teljesíteni. Ehhez kapcsolódóan a személyesadat-kezelő informatikai rendszerek minden lényeges funkcionális elemére előzetesen ki kell dolgozni a visszaélés, rendszerhiba, identitáslopás stb. esetén alkalmazandó rendkívüli (manuális, javító-helyreállító, ellenőrző) eljárást, amelynek azonban adatvédelmi szempontból hasonló kritériumokat kell teljesítenie, mint az üzemszerű működés adatkezelési eljárásainak.

kiszervezés, adatfeldolgozó igénybevétele

A tervezett elektronikus szolgáltatások egy részét célszerű, sőt néha szükséges is központilag biztosítani. Itt azonban figyelemmel kell lenni arra, hogy az adatkezelési funkciók szervezeti különválasztása fontos adatvédelmi és biztonsági garanciákat tartalmazhat. A gazdaságosság és a rendelkezésre álló szakértelem vonzóvá teheti piaci szolgáltatók bevonását a rendszerek fejlesztésébe és üzemeltetésébe. Megítélésünk szerint a közigazgatás egészét érintő alapvető adatkezelési szolgáltatásoknak állami hatáskörben kell maradniuk, akkor is, ha az állam egyes technikai részfeladatokat kiszervez. Személyes adatokat érintő tevékenység esetében a kiszervezés adatfeldolgozói jogviszonyt hoz létre.

Külön ügyelni kell arra, hogy a közigazgatásból a magánszektorba, illetőleg a magánszektorból a közigazgatásba, csupán az elektronizálás következményeként, ne folyhassanak át személyes adatok jogalap nélkül. Adatfeldolgozás esetén a lánc-adatfeldolgozás tilalmát kell szem előtt tartani. [Avtv. 4/A. § (2)] Gondoskodni kell arról is, hogy az informatikai fejlesztő és üzemeltető szervezetek, különösen a versenyszféra szervezetei, csak a legszükségesebb mértékben ismerhessék meg a rendszerben tárolt személyes adatokat, lehetőleg az „éles" ügyféladatok ismerete nélkül végezzék feladataikat.

a lánc-adatfeldolgozás tilalma

Fontosnak tartjuk a köztisztviselő azonosításához, jogosultságainak elektronikus leképezéséhez és használatához kapcsolódó eszközök és módszerek elkülönítését az ügyfél hasonló eszközeitől és adatkezelési módszereitől. Más szóval, a hivatalnoknak más típusú kártyája, aláírása, jogosultsága legyen, mint az állampolgároknak; ez tükrözi és egyben ellenőrizhetőbbé teszi köztisztviselői feladatkörüket és felelősségüket. Ebből következően a köztisztviselői elektronikus eszköztár mellett az ilyen feladatot ellátó személyeknek külön állampolgári vagy ügyfél-eszköztárral is rendelkezniük kell – hasonlóképpen ahhoz, ahogy a köztisztviselő a magánéletben nem érvényesíti köztisztviselői kiváltságait.

a hivatali-köztisztviselői oldal eszközeinek elkülönítése az állampolgár eszközeitől

Amennyiben a jövőben megvalósul akár az elektronikus TAJ-kártya, akár egy elektronikus közigazgatási kártya kiadása, a hivatalnokoknak speciális kártyát kell készíteni. Állampolgári „közigazgatási" kártyával csakis közigazgatási ügyeket lehessen intézni, de annak ne legyen akadálya, hogy ilyen ügyeket az állampolgárok más kártyával is intézhessenek. A hivatalnoki kártya nem lehet azonos a hivatalnok eTAJ (vagy állampolgári közigazgatási) kártyájával. Elektronikus aláírás alkalmazása esetén a hivatalnoki kártyán szereplő magánkulcs párja mindenki számára nyilvános legyen, az állampolgárok eTAJ (vagy közigazgatási) kártyájának nyilvános kulcsát azonban csak a közigazgatás használja, és a kapcsolódó hitelesítési , illetve letiltási funkciókat az állam végezze.

Itt említjük meg, hogy az az elképzelés (ami a szerződés mellékletében is szerepel), miszerint az ügyintézés elektronizálása során egységes központi közigazgatási jogosultság-kezelő rendszert kellene kiépíteni, álláspontunk szerint nem megvalósítható, sem elvi, sem gyakorlati szempontból. Az egyes közigazgatási szervek, illetve az egyes ügyintézők által kezelt ügytípusok köre olyan szerteágazó, és olyan elemeket tartalmaz, hogy azok nem szabványosíthatók teljes körűen; de ha erre mégis kísérlet történne, az ügytípusok és aleseteik, az ügyintézői jogosultságok meghatározása, módosítása, a kivételek elbírálása stb. olyan bürokráciához vezetne, ami ellentétes lenne a számítógépesítés deklarált céljaival.

központi egységes jogosultságkezelés futurisztikus elképzelése

3.3. Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálat (a jogirodalomban használatos elnevezése szerint Privacy Impact Assessment) a személyes adatok kezelését érintő kormányzati és közigazgatási intézkedések és tervek minőségbiztosítását jelenti. Kanadában, Új-Zélandon, az Egyesült Államokban, Ausztráliában és Hong-Kongban minden személyesadat-kezelést érintő projekt kezdeti fázisától, annak befejezéséig kötelező adatvédelmi hatásvizsgálatot lefolytatni.

A kötelező adatvédelmi hatásvizsgálat a kormányzati és a közigazgatási szervek új adatkezelési megoldásaira, az adatkezeléssel érintett tervek, jogszabály-módosítások folyamatos ellenőrzését jelenti. Azokban az országokban, ahol kötelező a hatásvizsgálat elvégzése, a projektek kezdeti szakaszától annak lezárásáig elemzik a javaslatokat. Ennek során kialakításra kerülnek projekttel kapcsolatos követelményrendszerek, amely a jogszerűséget hivatott biztosítani. Az adatvédelmi hatásvizsgálat, amellett hogy az állampolgárok alapjogának védelmét tartja szem előtt, egyidejűleg biztosítja a projekt sikerességét, az átláthatóságot és a társadalmi elfogadottságot is.

A fenti országok erre az OECD által kidolgozott adatkezelési elveket (OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980) kérik számon a hatásvizsgálat során független szervezetek, de ez elképzelhető más adatvédelmi normarendszer számonkérésével is, így biztosítva védelmet az esetlegesen alkotmányellenes szabályozási javaslatokkal szemben. A hatásvizsgálat növeli az állampolgárok bizalmát is. Egy hazai adatvédelmi hatásvizsgálatban az adatvédelmi törvény és a szektorális szabályok figyelembe vétele az elsődleges, de a projektek jogszerűsége csak úgy biztosítható, ha az uniós irányelveknek és a nemzetközi dokumentumoknak is megfelel. Kollízió esetén mindig a nemzeti szabályozás az irányadó.

a hatásvizsgálat célja

Az adatvédelmi hatásvizsgálatot már a döntés-előkészítési szakaszban érdemes elkezdeni. A vizsgálat amellett, hogy felbecsüli a lehetséges negatív hatásokat, a problémák kiküszöbölésére is megoldási javaslatokat nyújt. Egy ilyen jellegű vizsgálat képes kimutatni, hogy az egyes projektek milyen adatvédelmi kockázattal járnak, és milyen megoldás harmonizál a nemzeti és nemzetközi szabályozással, az Alkotmánybíróság és az adatvédelmi biztos gyakorlatával. Éppen emiatt a hatásvizsgálat eredményeként olyan megoldások születhetnek, ami minimális jogalkotással is megvalósítható, hiszen a jogszabály-módosítási javaslat nem kockázatcsökkentő megoldás; az a probléma kiküszöbölésének végső eszköze lehet csak, ehelyett technikai, adatkezelési, adatgyűjtési, adattörlési javaslatokat nyújt a vizsgálat.

a döntés-előkészítés szakaszában is

Az adatvédelmi hatásvizsgálat arra vonatkozik, hogy a javaslat milyen hatással van az állampolgárok magánszférájára, milyen kockázati tényezők mutathatók ki és milyen módosításokat kell végrehajtani ahhoz, hogy ezeket a negatív hatásokat ki lehessen küszöbölni. A hatásvizsgálat eredményeinek beépítése a kormányzati és közigazgatási szervek feladata, célja a jogszerű adatkezelési rendszerek felállítása. A negatív hatások kiküszöbölése mellett, a megfelelő kormányzati kommunikáció és az állampolgári bizalom megszerzésének is eszköze.

a vizsgálat szempontjai

Az adatvédelmi hatásvizsgálat az adatvédelmi problémákat definiálja a projekt kezdeti lépései során, lehetőleg már a koncepció kidolgozásának szintjén, az elfogadás és a finanszírozás tervezését megelőzően. Az előzetes hatásvizsgálat olyan korai szakaszban képes kimutatni az egyes adatvédelmi kockázatokat, amivel a projekt sikerének kockázata jelentősen csökkenthető. Az adatvédelmi és alkotmányos követelményeknek megfelelő projekt kialakítása megfelelő biztonságot jelent, ami későbbi módosítási követelmények kockázatát is csökkenti.

kockázatelemzés

Azokban az országokban, ahol kötelezően bevezetésre került az adatvédelmi hatásvizsgálat, tipikusan az alábbi esetekben kötelező elvégezni:

- egészségügyi adatok (egyéb különleges adatok) adatbázisba rendezésére kerül sor;
- meglévő adatbázisok összekapcsolása;
- a nemzetbiztonsági és bűnüldözési jogszabályok módosítása, amennyiben az megfigyeléssel, adatkezelés bővítésével jár;
- biometrikus azonosítás bevezetése;
- a végrehajtó és s bűnüldöző szervek adatbázisokhoz való hozzáférésére vonatkozó jogszabályok változása;
- adatkezelés megváltozása;
- új azonosítók bevezetése;
- új adatbázisok felállítása;
- megfigyelő kamerák üzembe helyezése;
- elektronikus fizetés bevezetése;
- adattovábbítás.

Az adatvédelmi hatásvizsgálat a döntés-előkészítéstől a projekt végig tart, hogy az újabb megoldási módok vizsgálata is megtörténjen. Fontos garanciális elem, hogy a vizsgálatot független szervezetek végzik, biztosítva ezzel a hitelességet és az objektivitást.

Az adatvédelmi hatásvizsgálat eredménye minden esetben az adatvédelmi

kockázatok felmérése és a szükséges módosítások végrehajtása a projekt tervben. A kockázatokat és a lehetséges kiküszöbölő eszközöket a kormányzati és közigazgatási szerveknek kötelezően figyelembe kell venniük. Formálisan egy jelentést készítnek a végzők. Bár projektenként változik a jelentés tartalma, fontos, hogy az alábbiakat magába foglalja:

jelentés

- áttekintés az adatvédelmi elvekről és hatásokról;
- a kezelt személyes adatok körének meghatározása;
- az adatkezelők körének meghatározása;
- annak az elemzése, hogy a vizsgált rendszernek milyen hatása lesz a személyes adatok védelmére;
- kockázatelemzés, és annak hatásai;
- kockázatcsökkentési javaslatok;
- javaslatok a megfelelő technikai és eljárási megoldásokra.

A hatásvizsgálat szakmai színvonalát és annak eredményeit figyelembe vevő döntést a tanulmány nyilvánosságra hozatala biztosíthatja. Vizsgálatot végző szervezettől elvárás, hogy a tanulmány speciális szakmai ismeret hiányában is érthető legyen. A hatásvizsgálat publikálását követően közmeghallgatást tartanak. A nyilvánossággal - a polgárok, civil szféra bevonása - az egyes személyes adatok kezelését igénylő kormányzati projektekben a bizalmat és a társadalmi elfogadottságot növeli.

nyilvánosság

A jogalkotásról szóló 1987. évi XI. törvény (Jat.) kimondja, hogy a jogszabály megalkotása előtt - a tudomány eredményeire támaszkodva - elemezni kell a szabályozni kívánt társadalmi-gazdasági viszonyokat, az állampolgári jogok és kötelességek érvényesülését, az érdekösszeütközések feloldásának a lehetőségét, meg kell vizsgálni a szabályozás várható hatását és a végrehajtás feltételeit. [Jat. 18. § (1)] Az adatvédelmi hatásvizsgálat kötelezővé tétele megfelelő eszköz lenne a személyes adatok védelmét érintő egyes projektek és jogalkotási feladatokat megelőzően, összhangban a Jat. szabályaival. A döntés-előkészítéshez szükséges adatok hozzáférhetőségének biztosításáról szóló 1997. évi CI. törvény kimondja, hogy „kötelessége az

a hatásvizsgálat elvégzésének szükségessége Magyarországon a jogalkotásban

államnak és az államigazgatási szerveknek, hogy a gazdaságra és a társadalmi folyamatokra kiható döntéseiket előzetesen mérlegeljék, eredményüket utólagosan vizsgálják. […] Empirikus kutatásokkal alátámasztott hatásvizsgálatok nyújthatnak segítséget a döntési alternatívák közötti választásban, a hatékonyság és a célszerűség érvényesítésében." Az adatvédelmi hatásvizsgálatok elvégzésére vonatkozó kötelezettség tehát a jogalkotás tekintetében a hatályos jogszabályokból is kiolvasható.

az adatvédelmi biztos előzetes ellenőrzése

Az Avtv. hatásvizsgálatot előíró rendelkezését pedig az adatvédelmi biztos előzetes ellenőrzés-hatáskörének szabályai között találjuk. Az Avtv. 31. §-a szerint az adatvédelmi biztos az adatvédelmi nyilvántartásba vételt megelőzően nyilvántartásba vételt megelőzően előzetes ellenőrzést végezhet. Új adatállomány feldolgozását vagy új adatfeldolgozási technológia alkalmazását megelőzően – az adatvédelmi nyilvántartásba vételtől függetlenül előzetes ellenőrzést végezhet a következő adatkezeléseket végző adatkezelőknél:

- országos hatósági, munkaügyi és bűnügyi adatállományok;
- pénzügyi szervezetek és közüzemi szolgáltatók ügyfelekre vonatkozó adatkezelései;
- távközlési szolgáltatóknak a szolgáltatást igénybe vevőkre vonatkozó adatkezelései;
- külön törvényben meghatározott egyedi statisztikai adatokat tartalmazó adatállományok.

Az adatkezelőnek az új adatállomány feldolgozására vagy az új adatfeldolgozási technológia alkalmazására irányuló szándékát a tevékenység megkezdését megelőzően 30 nappal be kell jelentenie az adatvédelmi biztosnak. Az adatvédelmi biztos az előzetes ellenőrzésre vonatkozó igényét a bejelentéstől számított 8 napon belül köteles jelezni az adatkezelőnek, és az ellenőrzést 30 napon belül köteles elvégezni. Az adatkezelő a feldolgozást csak az adatvédelmi biztos előzetes ellenőrzésének befejezése után kezdheti meg.

Az ellenőrzés alapján az adatvédelmi biztos a kezelendő adatok körének,

illetőleg az adatfeldolgozás módszerének megváltoztatására hívhatja fel az adatkezelőt. Ha az adatvédelmi biztos az adatkezelést elrendelő jogszabályt kifogásolja, ajánlást tehet a jogszabály módosítására.

A tapasztalatok szerint az adatvédelmi biztos ezt a hatáskörét nem gyakorolja, ezért az előzetes ellenőrzés nem tölti be valódi rendeltetését.

A hatásvizsgálatok nyilvánosságra hozatalának biztosítékai egyébként ugyancsak megtalálhatóak az a személyes adatok védelmének alapelvei között: az Avtv. biztosítja az átláthatóságot és a nyilvánosságot. Az érintettek tájékoztatáshoz való joga [Avtv. 11. § (1) b)], a betekintési [Avtv. 11. § (2)] és tiltakozási joga (Avtv. 16/A. §), az adatvédelmi nyilvántartás (Avtv. 28. § (1) mind ezt a célt szolgálja. Az információs önrendelkezési jog lényege éppen az, hogy az érintett tudhatja és követheti személyes adatai felhasználásának útját és körülményeit. [15/1991. (IV. 13.) AB határozat]. Az adatkezelés átláthatósága az önrendelkezési jog gyakorlásának előfeltétele, ezért a hatásvizsgálat eredményének nyilvánosságát is biztosítani kell.

a jelentés nem döntés-előkészítő adat

A hatásvizsgálatot, bár döntés-előkészítési szakaszban kell elkezdeni, nem lehet döntés-előkészítő adatnak tekinteni. A hatásvizsgálatot lezáró jelentés közérdekű adat, amelynek nyilvánosságát biztosítani kell a projekt végső tervének nyilvánosságra hozatalával egyidejűleg.

A fentiek alapján javasoljuk a következőket a tanulmányt érintő adatkezelések körében.

1. Kötelezővé kell tenni az adatvédelmi hatásvizsgálatok elvégzésének követelményét valamennyi kormányzati programban, amely személyes adatok kezelését érinti, illetve ha az intézkedés az adatvédelmi szabályozás módosításával jár.

2. Garanciális elemként érdemes bevezetni a független szervezetek által

készített vizsgálati eredményt, amelyet az adatvédelmi biztosnak kötelező lenne megküldeni.

3. A hatásvizsgálatokat nyilvánosságra kell hoznia mind az azt végző szervezetnek, mind a kormányzati/közigazgatási szerveknek.

4. . A nyilvánosságra hozott tanulmányt az érdekelt társadalmi szervezetek és érdekképviseleti szervek véleményezhetik.

5. Szükséges kidolgozni az adatvédelmi hatásvizsgálat követelményrendszerét és annak figyelembe vételére vonatkozó kötelezettséget.