Nemzeti Adatvédelmi és
Információszabadság Hatóság

Ügyszám: NAIH-1387-2/2014/J.

Dr. Gulyás Gergely részére
elnök

Törvényalkotási Bizottság

Budapest
Pf.: 2.
1357

Tisztelt Elnök Úr!

A Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 38. § (4) bekezdés a) pontjában meghatározott jogszabály-véleményezési feladatkörében eljárva, a személyes adatok védelméhez fűződő jog érvényesülésének elősegítése érdekében a sportról szóló 2004. évi I. törvény módosításáról szóló T/156. számú törvényjavaslattal (a továbbiakban: Javaslat) kapcsolatban az alábbi észrevételeket teszi.[1]

1. A Javaslat 1. §-át a Hatóság nem kifogásolja.

2. A Javaslat 2. §-a értelmében a sportról szóló 2004. évi I. törvény (a továbbiakban: Stv.) 72/A. § (1) bekezdése helyébe a következő rendelkezés lép: *„Beléptető rendszer alkalmazása esetén a szervező személyazonosításra alkalmas,* ***fényképpel ellátott****, kedvezményekre jogosító kártya (a továbbiakban: klubkártya) kiváltását is kötelezővé teheti."*

Az Infotv. 4. § (2) bekezdése tartalmazza az adatminimalizálás elvét. Eszerint csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulása szempontjából elengedhetetlen, a cél elérésére alkalmas, kizárólag a cél megvalósulásához szükséges mértékben és ideig. Ezen alapelv figyelembe vétele szavatolja, hogy az adatkezelés céljára tekintettel csupán a legszűkebb, indokolt adatkör kezelésére kerül sor. Az adatminimalizálás elve továbbá kizárja a készletezésre történő adatkezelést, azaz hogy olyan adatok felvételére kerüljön sor, amelyeket csak később meghatározásra kerülő célból gyűjtenek.

A Javaslat 1. §-a értelmében beléptető rendszer alkalmazása esetén a szervező – a rendező útján – ellenőrzi a belépőjegy vagy a bérlet birtokosának személyazonosságát, és a személyazonosság igazolására alkalmas igazolványban szereplő személyes adatait egybeveti a névre szóló belépőjegyhez vagy a bérlethez hozzárendelt egyéb személyes adatokkal. A Javaslat 2. §-a szerint szervező a klubkártya kiváltásának a feltételeként meghatározhatja továbbá azt is, hogy a klubkártya tulajdonosa személyazonosítása céljából bizonyos biometrikus adatokból generált, „vissza nem fejthető, titkosított, algoritmizált alfanumerikus kód" kezelését is, amelyet szintén az a belépőjegy vagy a bérlet birtokosa személyazonosságának ellenőrzése céljából használna fel.

Az érintett azonosítására tehát három – eltérő adatkörön alapuló – lehetőséget is biztosít a törvény a szervező számára. Ebben a tekintetben tehát nem érvényesül megfelelő módon az adatminimalizálás elve. Amennyiben ugyanis az érintett rendelkezik az azonosításához szükséges okirattal, feleslegessé válik a további azonosítási módok kötelező előírása.

[1] Az iromány elérhető: www.parlament.hu/irom40/00156/00156.pdf.

1125 Budapest,
Szilágyi Erzsébet fasor 22/C.
Tel.: +36 1 391-1400
Fax: +36 1 391-1410
ugyfelszolgalat@naih.hu
www.naih.hu

Az adatminimalizálás elvének figyelembe vétele természetesen nem zárja ki azt, hogy a törvény további azonosítási módokat biztosítson az érintett adatkezelők részére. A fényképes azonosítás lehetővé tétele azonban jelen esetben ellentétes az Infotv. 4. § (2) bekezdésében foglaltakkal. A szervezők ugyanis az érintettek arcmását az állami hatóságok által kiállított fényképes okmányok segítségével ellenőrizhetik. Egy további felvétel bemutatása így – a Javaslat 1. és 3. §-aiban foglalt azonosítási módok mellett – felesleges, és ezért cél nélküli, készletező adatkezelésnek minősül.

A Hatóság ezért javasolja a „fényképpel ellátott" szövegrész elhagyását a Javaslat vonatkozó rendelkezéséből.

3. A Javaslat 2. §-a értelmében az Stv. 72/A. § (2) bekezdése helyébe a következő rendelkezés lép: *„A szervező a klubkártya kiváltásának a feltételeként meghatározhatja, hogy a szervező a klubkártya tulajdonosa személyazonosítása céljából, e személy képmásából, íriszképéből vagy vénalenyomatából generált, vissza nem fejthető,* ***titkosított***, ***algoritmizált*** *alfanumerikus kódot (továbbiakban:* ***HASH-kód****) kezelhessen."*

3.1. Az Infotv. 3. § 2. pontja értelmében személyes adat az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. Érintett lehet bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy [Infotv. 3. § 1. pont].

A személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelv (a továbbiakban: Adatvédelmi Irányelv) 29. cikke alapján létrehozott Adatvédelmi Munkacsoport (a továbbiakban: Munkacsoport) által elfogadott, a biometrikus technológiák fejlődéséről szóló 3/2012. számú vélemény (WP193)[2] olyan biológiai jellegzetességekként, pszichológiai sajátosságokként, életvitelként vagy olyan ismétlődő tevékenységekként határozza meg a biometrikus adatokat, amelyek során e jellegzetességek, illetőleg tevékenységek egyedülállóak az érintett egyén vonatkozásában, továbbá mérhetőek, még ha a gyakorlatban a technikai mérésükhöz alkalmazott mintákat bizonyos fokú valószínűség jellemzi is. Példaként említhető az ujjlenyomat, a DNS- vagy írisz minta, a hangmintázat vagy a tenyérben lévő erek elhelyezkedése. Ezek az információk – tekintettel arra, hogy az érintett fiziológiai azonosságára jellemző ismeretek – személyes adatoknak minősülnek.

A biometrikus beléptető rendszerek alapvetően két eltérő módszer, következésképpen két eltérő adatkör alapján működhetnek. A hagyományos biometrikus beléptető rendszerek a működésük során az érintett biometrikus adatáról készített felvételt hasonlítják össze az ugyanarról az adatról korábban rögzített és eltárolt felvétellel. Ebben az esetben a technológia személyes adatokat dolgoz fel.

A fejlettebb biometrikus beléptető rendszerek ezzel szemben a nyers formában lévő biometrikus adatból kinyert kulcsfontosságú jellemzők alapján ún. biometrikus sablonokat képeznek. Ebbe a körbe tartoznak például a különböző logikai művelettel létrehozott digitális adatcsomagok. A biometrikus sablon képzése egyirányú folyamat, amely lehetetlenné teszi a biometrikus adatok ismételt előállítását vagy visszafejtését. Az ilyen biometrikus beléptető rendszerek kétféle biometrikus sablon alapján működnek: az egyik a letárolt formában lévő, a másik pedig a rendszer működése során keletkezett adatcsomag. A rendszer mindig utóbbit hasonlítja az előbbihez. A két sablon teljes mértékig megegyezhet, vagy – egyes esetekben – előre meghatározott százalékos mértékig eltérhet egymástól.

Biometrikus sablon – szemben a biometrikus adattal – csak akkor nem minősül személyes adatnak, ha azok tárolása oly módon történik, hogy az érintett azonosítására semmilyen ésszerű eszköz nem áll az adatkezelő vagy harmadik személy rendelkezésére. Amennyiben tehát a letárolt sablont megszemélyesítik, ahhoz

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_hu.pdf#h2-2

további adatokat (a továbbiakban: azonosító adat) rendelnek, az adatcsomag személyes adatnak fog minősülni. Ellenkező esetben viszont nem valósul meg adatkezelés. Megjegyzendő azonban, hogy az esetek nagy többségében a biometrikus sablont azonosító adatokkal, illetve az érintettre vonatkozó következtetésekkel párosítják.

A Hatóság felhívja szíves figyelmét arra, hogy a Javaslat 2. §-a, illetőleg a Javaslat részletes indokolása között ellentét áll fenn. Az Stv. javasolt szövege három különböző biometrikus adatot, a személy képmását, íriszképét vagy vénalenyomatát sorolja fel. Ezzel szemben viszont az indokolásban az „ujj- vagy tenyérnyomat" kifejezés szerepel. Utóbbi biometrikus adatok közül azonban a javaslat egyiket sem említi meg: az ujjlenyomat egyáltalán nem szerepel a szövegben, a tenyérlenyomat pedig nem azonos az érintett vénalenyomatával.

További probléma forrása lehet az, hogy a Javaslat a „vissza nem fejthető, titkosított, algoritmizált alfanumerikus kód" generálására épülő technológiát privilegizálja, ezáltal pedig kizárhat olyan piaci szereplőket, akik magánszféra-barát rendszerek fejlesztésében és forgalmazásában lehetnek érdekeltek. Ez amellett, hogy a tisztességes verseny érvényesülését is korlátozza, ahhoz vezethet, hogy az adatkezelők a személyes adatok védelme szempontjából kevésbé megfelelő, adott esetben akár elavult rendszert kénytelenek használni. Ráadásul a HASH-kód mint kifejezés idegen a magyar jogi szaknyelvtől.[3]

Egyértelmű, és a Munkacsoport már említett véleményében is az áll, hogy a Javaslat szövegében is említett HASH-kódolásra épülő biometrikus technológiákat kell előnyben részesíteni az érintettek magánéletének és személyes adatainak védelme érdekében. A Javaslat szövegében található „titkosított" és „algoritmizált" kifejezések ugyanakkor nem értelmezhetőek. A HASH-kód ugyanis már önmagában is egy egyoldalú leképezést végző algoritmussal előállított alfanumerikus kód, amelyből a kód képzéséhez felhasznált adattartalom nem fejthető vissza. E kódot azonosítási célú felhasználás esetén nem szükséges külön titkosítani, mivel már eleve nem utal a kódképzéshez használt kiinduló adatokra. Természetesen a HASH-kód titkosítása – figyelemmel az Infotv. 7. §-ában foglalt adatbiztonsági előírásokra is – az érintettek magánszférájának védelme szempontjából további garanciát jelenthet, azonban ebben az esetben a titkosítás módját a jogszabály szövegében pontosan meg kell határozni.

A Hatóság a fentiekre való tekintettel javasolja a „titkosított", az „algoritmizált" és a „HASH-kód" kifejezések elhagyását a szövegből, és a „vissza nem fejthető biometrikus sablon" kifejezés alkalmazását. Ez továbbá szükségessé teszi a biometrikus sablon fogalmának technológia-semleges meghatározását akár az Stv. 72/A. §-ának keretében, akár az Stv. értelmező rendelkezéseit tartalmazó 77. §-ában.

3.2. Végezetül a Hatóság felhívja szíves figyelmét arra, hogy a Javaslat vonatkozó rendelkezésének megfogalmazása nehézkes, nem egyértelmű. Az adatvédelemmel kapcsolatos olyan jogszabályokban, ahol meghatározott adatok kezelése az adatkezelő mérlegelésétől függ, jellemzően azzal a megfogalmazással él a jogalkotó, hogy az adott személy „jogosult kezelni" bizonyos adatokat. Nem egyértelmű továbbá, hogy a törvényi felhatalmazás csupán a HASH-kódokra, vagy esetleg az említett biometrikus adatokra is vonatkozik.

Az Infotv. 3. § 10. pontja tágan, vagyis az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összességeként határozza meg az adatkezelés fogalmát. Ennek megfelelően a biometrikus beléptető rendszerek vonatkozásában három önálló adatkezelési művelet különböztethető meg. A biometrikus adatok felvétele mindazokat a folyamatokat magában foglalja, amelyeket annak érdekében végeznek egy biometrikus beléptető rendszer működtetése során, hogy egy biometrikus forrásból biometrikus adatot nyerjenek ki, abból esetleg letárolt sablont képezzenek, és ezt az adatot hozzákapcsolják az

[3] Ezzel kapcsolatban hangsúlyozandó, hogy a Hatóság vonatkozó állásfoglalásaiban is a „biometrikus sablon" kifejezést alkalmazza.

érintetthez. A biometrikus adatok tárolása a felvétel során nyert adatok vagy a letárolt sablon és az esetlegesen hozzárendelt egyéb személyes adatok vagy technikai azonosítószám tárolását jelenti a leolvasók által hozzáférhető központi adatbázisban. A biometrikus adatok párosítása során pedig a rendszer a felvételkor nyert biometrikus adatokat/sablonokat hasonlítja össze a biometrikus beléptető rendszer működése során keletkezett biometrikus adatokkal/sablonokkal.

Lényeges, hogy a biometrikus adatok felvétele során, amennyiben azokból biometrikus sablont képeznek, ha rövid időre is, de létrejön a biometrikus adatok kezelése a szervező által. Ezen nem változtat az sem, hogy a Javaslat 3. §-a értelmében a biometrikus adatok felvételét – a biometrikus sablonok tárolásától és párosításától eltérően – a szervező megbízásából eljáró adatfeldolgozóként, harmadik személy is végezhet.

A Hatóság javasolja ezért a Javaslat vonatkozó szövegrészének a fentieknek megfelelő átfogalmazását, illetőleg annak egyértelmű megfogalmazását, hogy az adatkezelő mely személyes adatokat kezelheti.

4. A Javaslat 2. §-a értelmében az Stv. 72/A. § (2) bekezdése helyébe a következő rendelkezés lép:
„(4) A szervező a beléptetéskor
a) az (1) bekezdésben meghatározott esetben rendező útján a belépőjegy vagy a bérlet birtokosának személyazonosságát úgy ellen őrzi, hogy a személyazonosság igazolására alkalmas igazolványban szereplő személyes adatait egybeveti a belépőjegy vagy a bérlet birtokosa által bemutatott klubkártyához hozzárendelt, a szervező által nyilvántartott, 72/B. § (2) bekezdésében meghatározott személyes adatokkal,
*b) a (2) bekezdés szerinti esetben — **az a) pontban meghatározottakon túl** — a belépőjegy vagy a bérlet birtokosának személyazonosságát **úgy is ellenőrzi**, hogy a belépőjegy vagy a bérlet birtokosa 72/A. § (2) bekezdésében meghatározott biometrikus adatát rögzíti, abból HASH-kódot képez és azt összeveti a klubkártya tulajdonosa szervező által nyilvántartott HASH-kódjával."*

A személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvény (a továbbiakban: Szaztv.) 4. § (1) bekezdése értelmében a polgárt természetes személyazonosító adataival, vagy a természetes személyazonosító adatokból kiválasztott, az adatkezelés célja szerint szükséges és megfelelő mértékű adattal vagy törvényben meghatározott esetben családi és utónevével, valamint az e törvényben meghatározott azonosító kóddal (a továbbiakban együtt: azonosítási módok) kell azonosítani. Természetes személyazonosító adat a polgár családi és utóneve, születési családi és utóneve, születési helye, születési ideje és anyja születési családi és utóneve [Szaztv. 4. § (4) bekezdés].

A Szaztv. 4. § (2)-(3) bekezdése szerint a polgárt saját maga azonosítása céljából csak egy azonosítási mód alkalmazására lehet kötelezni. Törvény eltérő rendelkezése hiányában a polgár az adatok igazolásának módját szabadon megválaszthatja.

Példaként említendő, hogy a Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) 29. § (2) bekezdése is csupán annyit ír elő, hogy a rendőr által igazoltatott személy *„köteles a személyazonosító adatait hitelt érdemlően igazolni. A személyazonosságot – a személyazonosító igazolványon túl – minden olyan hatósági igazolvány igazolja, amely tartalmazza a személyazonosításhoz szükséges adatokat. Az igazoltatott kizárólag ezen okmányok egyikének bemutatására kötelezhető. A rendőr más jelen lévő, ismert személyazonosságú személy közlését is elfogadhatja igazolásként"*. A hivatalos nyomozóhatóság tagjai tehát bármelyik olyan okmányt kötelesek elfogadni, amely alkalmas az érintett azonosítására.

Az Stv. tervezett módosítása ugyanakkor nem biztosítja a Szaztv. 4. § (2)-(3) bekezdésében foglalt lehetőséget a klubkártya tulajdonosok részére, mivel a „hagyományos" azonosításon túl a biometrikus beléptető rendszer révén is azonosítani kell az érintetteket. A törvény ezáltal, összehasonlítva egy rendőrségi intézkedés hatálya alá vont személlyel, sokkal szigorúbb követelményeket támaszt a klubkártya

tulajdonosokkal szemben az azonosítás céljából, ami nyilvánvalóan sérti az érintettek részére a Szaztv.-ben biztosított jogokat.

A Hatóság ezért javasolja, hogy az Stv. 72/A. § (4) bekezdés a) és b) pontjában foglalt azonosítási módok vagylagossá tételét.

5. A Javaslat 3. §-a értelmében az Stv. „A beléptetés" alcíme kiegészül egy 72/A. §-szal, amelynek (2) bekezdése a következőket tartalmazza:
*„A belépőjegy, bérlet, valamint klubkártya eladásakor a sportrendezvényre ezekkel belépésre jogosult személy nevét, **anyja nevét**, születési helyét és idejét, valamint **lakcímét** a szervező, valamint a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet vagy sportszervezet a belépőjegy, a bérlet, illetve a klubkártya érvényességének lejáratát követő **3 munkanapig nyilvántartja**. Ezeket az adatokat a szervező, valamint a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet vagy sportszervezet **a belépőjegyen, a bérleten, illetve a klubkártyán feltüntetheti**."*

A Hatóság a NAIH-4941-3/2014/V. számon kelt állásfoglalásában korábban már kifejtette, hogy *„a néző azonosításához sem a néző lakcímére, sem pedig az anyja születési családi és utónevére nincs szükség, így ezeket nem lehet felhasználni"*. Az említett dokumentum értelmében továbbá nem szükséges a lakcím feltüntetése sem a belépőjegyen, sem a bérleten, sem pedig a klubkártyán. Ennek oka az, hogy a személyes adatok védelméhez fűződő jog szempontjából további veszélyforrást jelenthet ezen adat megismerése, amennyiben a belépésre jogosult személy a belépőjegyét, a bérletét vagy a klubkártyáját elveszíti vagy eldobja.

A Javaslat szövege továbbá nem rendelkezik arról, hogy mi történjen a személyes adatokkal a belépőjegy, a bérlet, illetve a klubkártya érvényességének lejártát követő három munkanapon túl. Az Infotv. 4. § (2) bekezdéséből, illetőleg 17. § (2) bekezdés d) pontjából ugyanakkor az következik, hogy az adatkezelést lehetővé tevő jogszabályban egyértelműen rendelkezni kell az adatok sorsáról azt követően, hogy az adatkezelés célja már megvalósult.

A Hatóság – a korábbi állásfoglalásában foglaltakra tekintettel – ezért javasolja a belépésre jogosult anyja nevének és lakcímének elhagyását a Javaslat szövegéből, továbbá a „„ majd azt követően törli" szövegrész felvételét az adatkezelés határideje vonatkozásában.

6. A Javaslat 3. §-a értelmében az Stv. „A beléptetés" alcíme kiegészül egy 72/A. §-szal, amelynek (3)-(4) bekezdése a következőket tartalmazza:
*„(3) A szervező, valamint a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet vagy sportszervezet a klubkártya eladásakor rögzíti a 72/A. § (2) bekezdésében meghatározott **biometrikus adatot**, amelyből haladéktalanul HASH-kódot képez.*
(4)A HASH-kódot
*a) szervező a (2) bekezdés szerinti személyes adatokkal együtt nyilvántartásba veszi, ezt követően a **biometrikus adatot** haladéktalanul törli, vagy*
*b) a szervező által megbízott, sportesemény-szervező tevékenységet folytató szervezet vagy sportszervezet haladéktalanul továbbítja a szervező részére nyilvántartásba vétel céljából, ezt követően a HASH-kódot és a **biometrikus adatot** haladéktalanul törli."*

A Hatóság a fenti rendelkezésekkel kapcsolatban felhívja szíves figyelmét arra, hogy biometrikus adat fogalma nincsen a javaslatban egyértelműen megfogalmazva. A Javaslat 2. §-ában foglalt biometrikus adatok továbbá nem tekinthetők e fogalom meghatározásának, mivel a taxatív felsorolás túlságosan szűkítő.

Célszerű lenne ezért a Javaslat szövegének a jelen vélemény 3.1-3.2. alpontjaiban foglaltaknak megfelelő módosítása.

7. A Javaslat 3. §-a értelmében az Stv. „A beléptetés" alcíme kiegészül egy 72/A. §-szal, amelynek (5)-(6) bekezdése a következőket tartalmazza:
„(5) Az (1) és (2) bekezdésben foglaltak alapján kiadott belépőjegy, bérlet, valamint klubkártya, illetve az ezekhez hozzárendelt, a szervező által nyilvántartott ***HASH-kód*** *és személyes adat csak a sportrendezvény helyszínén vagy a sportrendezvény helyszínének megközelítése, illetve az onnan való távozás során elkövetett* ***bűncselekmény vagy szabálysértés miatt indult büntető- vagy szabálysértési eljárás, továbbá a sportrendezvényről való eltiltás céljából használható fel****.*
A (2) bekezdésben meghatározott határidőn belül az (5) bekezdés szerinti személyes adatot megkeresésre a nyomozó hatóság, az ügyészség, illetve a bíróság részére büntető- vagy szabálysértési eljárásban bizonyítási eszközként való felhasználás céljából továbbítani lehet."

A Hatóság felhívja szíves figyelmét arra, hogy a HASH-kód „felhasználása" a fent megjelölt célból megkérdőjelezhető. Az érintett biometrikus adata, de az abból generált biometrikus sablon ugyanis nem alkalmas arra, hogy az adatalany beléptetéskori azonosításán kívül más eljárásban is felhasználható legyen. A magyar jogszabályok pontosan meghatározzák, hogy a nyomozóhatóságok mely adatokat kezelhetik a büntető vagy szabálysértési eljárások keretében. Példaként említhető a bűnügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bűnügyi és rendészeti biometrikus adatok nyilvántartásáról szóló 2009. évi XLVII. törvény (a továbbiakban: Bnytv.), amely az érintettek ujj- és tenyérlenyomata, valamint DNS-kódján kívül nem teszi lehetővé más biometrikus adatok kezelését, és az azokra épülő nyilvántartások létrehozatalát. Törvényi felhatalmazás, illetőleg a megfelelő nyilvántartások hiányában azonban az eljáró hatóságok nem jogosultak a sportrendezvényre látogatók – Bnytv.-ben meghatározott biometrikus adatain kívüli – egyéb biometrikus adatainak kezelésére.

A fentieknek megfelelően a Hatóság javasolja a „HASH-kód" szövegrész elhagyását a Javaslat vonatkozó rendelkezéséből.

8. A Hatóság felhívja szíves figyelmét arra, hogy az ún. privacy by design szemléletnek megfelelően az adatkezelő köteles a működését, struktúráját az adatvédelmi szempontok maximális figyelembevételével kialakítani. Az Infotv. 7. § (1) bekezdése ezzel összhangban úgy rendelkezik, hogy az adatkezelők kötelesek az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsák az érintettek magánszférájának védelmét. Az Stv.-ben foglalt biometrikus beléptető rendszer kialakításával kapcsolatban ez azt jelenti, hogy az adatkezelőknek olyan rendszerek bevezetésére kell törekednie, ennek megfelelően pedig a törvényalkotónak olyan jogszabályi környezetet kell kialakítania, amelyek szem előtt tartják az érintettek magánélet tiszteletben tartásához és személyes adatok védelméhez fűződő jogát.

Figyelembe véve a korábbi adatvédelmi biztosi gyakorlatot, a Hatóság álláspontja szerint az biztosítaná a legmagasabb szinten az említett alapjogok érvényesülését, amennyiben az érintettek biometrikus sablonjait az általuk birtokolt klubkártyán elhelyezett adathordozón tárolnák. A biometrikus beléptető rendszer pedig a kártyán lévő letárolt biometrikus sablont helyben hasonlítaná össze az érintett tenyeréről képzett sablonnal.

Ez a megoldás több ok miatt is különösen előnyös. Egyrészt az érintett nemcsak a biometrikus adata, hanem a biometrikus sablon felett is gyakorolhatja információs önrendelkezési jogát. Másrészt az adatkezelő egyetlen adatkezelési műveletet leszámítva nem kezelné fizikailag a biometrikus sablonokat, hiszen azokat a biometrikus beléptető rendszer dolgozná fel automatikusan. Emiatt viszont az adatkezelőnek sem kellene külön nyilvántartást fenntartani a biometrikus sablonok számára, és így jelentős mértékben csökkenteni lehetne az adatvédelmi és adatbiztonsági követelményeknek való megfelelés szempontjából rá háruló anyagi

és más terheket is. Harmadrészt pedig az érintett és a klubkártyán tárolt személyes adatok közötti kapcsolatot az összepárosított biometrikus sablonok teremtenék meg, azaz a rendszer biztonságának szintje nem csökkenne, hiszen az érintett biometrikus adata, vagy a letárolt biometrikus sablont tartalmazó klubkártya hiányában továbbra sem lenne lehetséges belépni a sportlétesítmény területére. A klubkártya esetleges elvesztése továbbá nem jár azzal a –hagyományos mágneskártyás beléptető rendszerek esetében gyakran hangoztatott – veszéllyel, hogy az érintett helyett, annak személyes adataival visszaélve egy harmadik személy lép be az adott területre. Az adatalany biometrikus adatából képzett biometrikus sablon ugyanis annyira egyedi és hamisíthatatlan, hogy a rendszer nagy pontossággal meg tudja különböztetni a belépésre nem jogosult személyt az arra jogosulttól. Végezetül megjegyzendő, hogy az adathordozó programozása és elhelyezése a klubkártyákon nem jár jelentősebb többletmunkával, illetőleg kiadásokkal.

A Hatóság ezért javasolja a fentebb vázolt biometrikus beléptető rendszer jogi szabályozásnak, illetőleg bevezetésének megfontolását és előnyben részesítését más rendszerekkel szemben.

10. Végezetül a Hatóság megjegyzi, hogy a Javaslat indokolása csupán általánosságban határozza meg azt a célt („a sportesemény szervezők a modern technológia segítségével már beléptetésnél kiszűrhessék azokat, akik korábbi rendzavarásukkal veszélyeztették a fair play szellemét a lelátókon"), amelynek érdekében a biometrikus beléptető rendszer bevezetésre kerülhet.

Az Infotv. 4. § (1) bekezdése értelmében ugyanakkor személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. A Munkacsoport a célhoz kötöttségről szóló 03/2013. számú véleményében (WP203)[4] kifejtette, hogy az adatkezelés céljának meghatározása a személyes adatok védelme jogi szabályozásának középpontjában áll. Azon cél meghatározása ezért, amelynek érdekében az adatkezelés történik, szükséges előfeltétele annak, hogy megállapítható legyen az adatkezelés jogszerűsége, illetőleg az alkalmazandó adatvédelmi garanciák. Az adatkezelés célját világosan és egyértelműen meg kell határozni: részletesen meg kell adni ahhoz, hogy megállapítható legyen, hogy milyen típusú adatkezelési művelet kapcsolódik az adott célhoz, és hogy melyik nem.

Továbbá a Munkacsoport 3/2012. számú véleménye szerint biometrikus adatok felhasználása – az adatkezelés céljának fényében – felveti az arányosság problémáját. Mivel a biometrikus adatok csak akkor kezelhetők, ha megfelelőek, relevánsak és nem túlzott mértékűek, a kezelt adatoknak meg kell felelniük a szükségesség és az arányosság követelményének, illetőleg mérlegelni kell, hogy a biometrikus rendszer üzemeltetése által elérni kívánt cél megvalósítható lenne-e egyéb, a magánszférát kevésbé érintő módon. A biometrikus rendszer arányosságának elemzésekor az alábbi szempontokat kell megfontolni:

- A rendszer működtetése szükséges-e a meghatározott cél eléréséhez (***szükségesség***). Azaz a rendszer használata elengedhetetlen-e az adott igény kielégítéséhez, vagy csupán annak kényelmes és költséghatékony módja.
- A rendszer működtetése mennyire lesz hatékony az adott cél elérése érdekében (***hatékonyság***).
- A magánszférának a rendszer működtetéséből eredő korlátozása vajon arányban áll-e a várható előnyökkel (***arányosság***). Amennyiben viszonylag kisebb az előny, például a kényelem növekszik a rendszer működtetése által vagy az csak egy minimális költségmegtakarítást eredményez, akkor a magánszféra korlátozása nem arányos az elérendő célokkal.
- A kitűzött célt vajon el lehet-e érni a magánéletet kevésbé korlátozó módon (***megfelelő alternatívák hiánya***). Amennyiben egyes alternatív intézkedések ugyanolyan hatékonyak lennének a kitűzött célra tekintettel, a rendszer üzemeltetője köteles az alternatívák közül választani.

[4] ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf#h2-2

E szempontok mérlegelését az adatkezelő, illetőleg – kötelező adatkezelés esetén – a jogalkotó köteles elvégezni. Ennek keretében többek között megfelelő módon fel kell mérni, hogy a Javaslat részletes indokolásában említett személyiséglopás (a korábban rendbontást elkövető személyek más személyazonosságával lépnek a stadionok területére) valóban olyan konkrét, folyamatos és jelentős kockázatot jelent, amely megalapozza a biometrikus beléptető rendszer alkalmazásának szükségességét. Amennyiben nincsen ilyen, az adatkezelés szükségességét és arányosságát alátámasztó indok, a Javaslat nem feltétlenül felelne meg az alkotmányossági követelményeknek.

Tekintettel arra, hogy a biometrikus adatok kezelése jelentős beavatkozást valósít meg az érintett személyek magánszférájába, a Hatóság kéri észrevételeinek szíves megfontolását.

Budapest, 2014. június 6.

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár