Nemzeti Adatvédelmi és
Információszabadság Hatóság

Ügyszám: NAIH/2018/6413/3./J
Ügyintéző: dr. Vass Norbert József
dr. Bíró János

Telefon: +36-1/391-1453
Hiv.szám: BM/16335- /2018

Dr. Felkai László részére
közigazgatási államtitkár

Belügyminisztérium

Tisztelt Közigazgatási Államtitkár Úr!

2018. október 15-én Hatóságunkhoz érkezett BM/16335- /2018. iktatószámú megkeresésével kapcsolatban *az okos város központi platformszolgáltatás létrehozásáról és működtetéséről szóló kormány-előterjesztéshez* kapcsolódó *kormányrendelet* tervezetével (a továbbiakban: Előterjesztés) kapcsolatos álláspontomról az alábbiakban tájékoztatom.

1.) Magyarország Alaptörvénye (a továbbiakban: Alaptörvény) I. cikk (3) bekezdés alapján az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Az Alaptörvény VI. cikk (3) bekezdés ilyen alapvető jogként határozza meg a személyes adatok védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez való jogot. Mivel az általános adatvédelmi rendelet (a továbbiakban: GDPR) rendelkezéseit az Alaptörvénnyel összhangban kell alkalmazni, a fenti magyar jogrendszerbeli sajátosságból adódóan Magyarországon a GDPR 6. cikk (1) bekezdés c) pont szerinti adatkezelési jogalapot legalább törvényi szintű jogszabályban kell meghatározni. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 5. § (3) bekezdése határozza meg az adatkezelést elrendelő törvényben minimálisan szabályozandó tárgyköröket. Ebből adódóan az okos város működéséhez kapcsolódóan szükséges kötelező adatkezeléseket kormányrendelet nem rendezheti, a szabályozás ezen részét egy vagy több törvényben szükséges rendezni. A törvényben szükséges pontosan megjelölni minden egyes adatkezelési célt, és célonként az ezek eléréséhez minimálisan szükséges kezelendő adattípusokat és azok jogalapját, valamint a megfelelő garanciákat a személyes adatok kezelésével kapcsolatban.

2.) Az okos város projekt érdekében szükséges jogszabály-módosításoknak figyelembe kell venniük a tagállami szabályozás korlátait. A projekt megvalósíthatósági tanulmány 348. oldalán tett alábbi megállapítás emiatt adatvédelmi szempontból aggályos megfogalmazást tartalmaz:

„Különös tekintettel az EU általános adatvédelmi rendeletére, valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezéseire kiemelten fontos a személyes, különleges és egyéb adatok védelme, ugyanakkor fontos az is, hogy ez ne hátráltassa a projekt eredményességét, a megvalósuló rendszerek, alkalmazások

széleskörű használatát. Meg kell vizsgálni, hogy a fenti szabályzók tekintetében szükséges-e jogszabályi korrekciók elvégzése akár állami, akár helyi szinten, továbbá vizsgálni kell, hogy az egyéb közjogi szabályozók, dokumentumok kellően igazodnak-e a jogszabályi elvárásokhoz."

A GDPR számos területen szűkítette a tagállami jogalkotó mozgásterét. Amennyiben a magyar tagállami szabályozás a GDPR-től el kíván térni, akkor kifejezetten javaslom a megfelelőség átláthatósága érdekében annak pontos megjelölését, hogy a GDPR mely rendelkezése engedi az adott konkrét esetben az eltérést, és mely ott felsorolt feltételek hogyan teljesülnek ezzel kapcsolatban.

Szintén kiemelendő, hogy uniós tagállami szintű egyeztetés alatt van az elektronikus hírközlési irányelvet felváltani hivatott, eredetileg a GDPR-el együtt elfogadni tervezett ePrivacy Rendelet. Ez közvetlen hatállyal tovább szűkíti majd a tagállami jogalkotó mozgásterét, és minden valószínűség szerint a projekt megvalósítása előtt hatályba lép. Az ePrivacy Rendelet nagyon sok hatással bírhat az okos berendezésekre, OTT szolgáltatásokra és egyéb elektronikus kommunikációra, de a szabályai még nem véglegesek. Emiatt célszerű lenne megvárni az említett uniós jogi szabályozási aktus véglegesítését, mert ellenkező esetben lehetséges, hogy a projekt megvalósítása közben kell majd abban lényeges módosításokat eszközölni.

Az adatvédelmi követelmények sorában kifejezetten hangsúlyozni szeretném a GDPR 25. cikk szerinti beépített és alapértelmezett adatvédelem elvét, amely minden adatkezelőre kötelezően irányadó. Ennek megfelelően egy ilyen volumenű projektnél a lehető legkorábbi fázisban szükséges elvégezni az adatvédelmi hatásvizsgálatot, és a projektet eleve annak megfelelően szükséges megtervezni. Ennek elmaradása miatt előfordulhat, hogy a rendkívüli mértékű beruházással kivitelezett rendszert jelentős költségekkel utólag kell átalakítani ahhoz, hogy a jogszabályokkal összhangban tudjon működni. Az adatkezelés nem kezdhető meg anélkül, hogy a jogszabályi megfelelés biztosítva lenne. Ehhez segítségként a **jelen irat mellékleteként** található azon adatkezelések listája, amelyekre az okos város projekt megvalósíthatósági tanulmánya alapján rendelkezésre álló információk szerint különösen, de nem kizárólag szükséges részletesen kitérni az adatvédelmi hatásvizsgálat és az adatkezelést rendező törvényjavaslat(ok) előkészítése során.

3.) Az Előterjesztés a Kormányzati Adatközpont (a továbbiakban KAK) kizárólagos feladatkörébe kívánja utalni az okos városok számára nyújtandó platformszolgálatások egy részének nyújtását és ezzel összefüggésben megtiltanák a települési önkormányzatok számára, hogy ezekkel párhuzamos vagy alternatív szolgáltatásokat tartsanak fenn. A platformszolgáltatások kötelező igénybevétele az adatkezelés kormányzati centralizációjával járna, hiszen elvonná a polgárok helyi közösségeitől azt az önkormányzati autonómiából levezethető jogot, hogy eldöntsék, vállalják-e a központi platformszolgáltatásoktól való függőséget, valamint az adataik KAK-ban történő kezelését, vagy inkább maguk kívánnak gondoskodni a település működésével és a helyi ügyekkel összefüggő adataikról. Véleményem szerint indokolt lenne széleskörű társadalmi vitát folytatni arról, hogy elfogadhatónak tartják-e az állampolgárok és a helyi közösségeik a centralizált kormányzati platformszolgáltatások ex lege monopolizált bevezetését.

4.) Ha az okos városok adatainak kezelése a terveknek megfelelően bekerül a KAK-ba, úgy egy országosan uniformizált és centralizált informatikai infrastruktúra fog létrejönni, illetve tovább épülni. Az egységesítésnek és a centralizációnak számos előnye mellett vannak árnyoldalai is, így például az, hogy a központtal való kapcsolat megszűnése esetén, illetve a központ bármilyen módon történő kiiktatásával (pl. üzemzavar, természeti katasztrófa, szabotázs stb.) megbénítható a

rendszer működése. Véleményem szerint már csak ezért is indokolt lenne a monolitikus, centralizált architektúra alternatíváit, így különösen a decentralizált, heterogén és osztott információs rendszermodelleket is számításba venni az okos városok informatikai infrastruktúrájának koncepcionális tervezése során.

5.) Rendkívül problematikusnak tartom a biometrikus arcképadatok kezelésére vonatkozó terveket, ugyanis a biometrikus személyazonosítás és ellenőrzés azon technológiák közé tartozik, amelyek jellegüknél fogva különösképp veszélyesek az állampolgárok alapvető jogaira. Az automatikus arcfelismerésen alapuló azonosítás és személyazonosság ellenőrzés nem igényli az érintett közreműködését, ezért rejtett megfigyelést tesz lehetővé. Az arcfelismerési és hasonló jellegű biometrikus technológiák kiterjedt, tömeges alkalmazása ahhoz vezethet, hogy a települési közterületek, a nyilvánosság számára nyitva álló egyéb közterületek és a tömegközlekedési eszközök megszűnnek a magánélet színterei lenni. A biometrikus azonosításra épülő szolgáltatások alkalmazásának kiterjesztése ellentétbe kerülhet a magyar alkotmányos jogfejlődés már elért eredményeivel, így különösen azzal, hogy az Alaptörvény a magán- és családi élet, az otthon és kapcsolattartás tiszteletben tartását egyaránt alapvető jogokként ismeri el, továbbá a magánélet védelméről szóló 2018. évi LIII. törvényben a magánélet fokozottabb védelme érdekében deklarált elvekkel és szabályokkal.

Előzetes véleményem szerint a helyi „okos városi" önkormányzati feladatkörben nem merülhet fel olyan biometrikus adatfelhasználási igény, amely alkotmányos keretek között megvalósítható lenne. Tovább fokozza az aggodalmat, hogy az okos városok közterületi megfigyelő rendszereit integrálnák a KAK-ban létrehozandó, az ország valamennyi településén, valamint a tömegközlekedési eszközökön és a közutakon jelenlévő, több tízezer közterületi kamera képfolyamatit folyamatosan gyűjtő és tároló, biometrikus azonosítást is alkalmazó, titkos megfigyelést lehetővé tevő képi megfigyelőrendszerbe. Jelenleg még beláthatatlan, hogy hosszabb távon milyen hatásai lennének egy ilyen totális megfigyelőrendszer létrehozásának az állam működésére és a magyar társadalomra. Ismét hangsúlyozom, hogy minél előbb el kell készülnie a tervezett adatkezelések adatvédelmi hatásvizsgálatának, amelyet a hatóságom konzultáció keretében meg kíván vizsgálni. Véleményem szerint célszerű lenne az adatvédelmi hatásvizsgálat főbb megállapításait ismertetni majd a törvényhozással is, hogy az okos városok fejlesztésének előnyei mellett a lehetséges kockázatokról és veszélyekről is tudomást szerezve megfelelő információkon alapuló, felelősségteljes döntés születhessen a kapcsolódó adatkezelések törvényi szintű szabályozását illetően.

Kérem, az előzőekben jelzett észrevételeimet az előterjesztésben foglalt módosítási javaslatok, valamint az okos város projekttel kapcsolatos egyéb jogszabályok kialakítása során szíveskedjen figyelembe venni.

Budapest, 2018. október „31"

Üdvözlettel:

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG 1

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár

Melléklet a NAIH/2018/6413/J. iktatószámú irathoz

Az okos város projekt megvalósíthatósági tanulmánya alapján felmerülő legfontosabb adatkezelések, amelyekre különösen, de nem kizárólag szükséges részletesen kitérni az adatvédelmi hatásvizsgálat és az adatkezelést rendező törvényjavaslat előkészítése során

1.) KAK (Kormányzati Adatközpont) felhő szolgáltatása, ahol a szolgáltató a NISZ lenne

- IaaS (Infrastructure as a Service), szerverek, virtuális gépek, tárhely stb.

- PaaS (Platform as a Service), adatbázis, webszerver, futtatási környezet stb.

- SaaS (Software as a Service), e-mail, kommunikáció, programok stb.

A NAIH/2018/6413/J. iktatószámú irat 5. pontban kifejtettek szerint az önkormányzati adatkezelőtől az adatkezelés átvétele, elvétele számos kérdést vet fel, amelynek szükségességét, arányosságát, céljait és a célok elérésére alkalmasságát megfelelően dokumentálnia szükséges az adatkezelőnek.

2.) Városkártya

- beléptetés

- kafeteria

- iskolakártya

- fizetés szerződött partnereknél

- stb.

Megvalósítás fizikailag: e-személyigazolványon belül, illetve e-diákigazolványon belül, saját kártya akiknek nincs e-személyi, vagy mobiltelefonos applikáció formában is lehessen regisztrálni.

Ennek megfelelő elválasztása szükséges egyéb adatkezelésektől, továbbá annak minden részletre kiterjedő szabályozása, hogy ki, milyen célból, milyen feltételekkel jogosult a kártyán tárolt egyes személyes adatokhoz hozzáférni.

3.) Intelligens Vizesblokk

Ha a tervek szerint a használati díj levásárolható a környező boltokban, akkor ennek megvalósítása felvethet adatvédelmi kérdéseket, ennek részletes leírása és rendezése szükséges az átlátható és jogszerű adatkezelés alapvető feltételeként.

4.) Okos Iskola

- okos-eszközök

- tanuló azonosító – szülő értesítő rendszer (városkártyán, e-diákigazolványon, mobilapplikáción keresztül)

- e-számlázás

Az okos eszközökkel kapcsolatban jó lenne a tudatos internethasználat, eszközhasználat oktatása, ennek várható pozitív hatásaival és konkrét terveivel is bővíthető a hatásvizsgálat. A pozitív oldalon kívül le szükséges írnia kockázatokat az egyes adatkezelésekkel kapcsolatban és azok mérséklésére tervezett megfelelő intézkedéseket.

5.) Várostárca mobiltelefonos applikáció

A kivitelezésen múlik a ténylegesen kezelt adatok és jogalapok, kezelési módok, hozzáférési jogok, adatbiztonság. Mivel okostelefonon keresztül lesz használható, vizsgálandó a mobiltelefonos applikációt futtatni képes operációs rendszert használó okostelefonok adatbiztonsága is, mivel ha a végberendezés nem biztonságos, az az adatkezelést jelentősen veszélyeztetheti adatvédelmi szempontból.

6.) Térfigyelő rendszer korszerűsítése

- arcfelismerő funkció rendezvény beléptetésre
- tiltott parkolás, hulladék lerakás automatikus észlelése
- stb.

Kérdés, hogy az arcfelismerés funkció mindig be van-e kapcsolva, és azt mire használják, milyen megőrzési idővel, milyen biztosítékai vannak. Az elérni kívánt célok és azokkal arányos és minimálisan szükséges adatkezelés vizsgálata szükséges, de ezt a jelenlegi fázisban még nem lehetséges vizsgálni. A koncepcióban szereplő statisztika szerint 2017-ben összesen 3 db bűnügy és 0 egyéb (szabálysértési, közlekedési stb.) ügyben volt szükség a kamera felvételére, ezért a rendkívül invazív, központi arcfelismerős rendszer indoklásához önmagában a bűnmegelőzés, mint absztrakt indok kevés.

Amennyiben élő városkép sugárzása történik az internetre, akkor fontos, hogy ne legyenek az egyes emberek kivehetőek (távolság, szög stb.), de mindezen technikai részletek csak az adatvédelmi hatásvizsgálat alapján minősíthetőek.

A különböző adatkezelési rendszerek összekapcsolása csak komoly garanciák és megfelelő átláthatóság mellett, konkrétan megjelölt, világos célból lehetséges, a szükségesség és arányosság követelményének betartásával. Ennek részletes bemutatása is fontos része az adatvédelmi hatásvizsgálatnak.