A digitális korszakkal együtt járó kérdések és válaszok az önkormányzati adatkezeléssel kapcsolatban

Készítette: Dr. Béres László

A tanulmány elkészítését és megjelenését a Demokratikus Helyi Közigazgatás Fejlesztéséért Alapítvány támogatta.

2022

Tartalom

A digitális korszakkal együtt járó kérdések és válaszok az önkormányzati adatkezeléssel kapcsolatban

Béres László[1]

Bevezetés

> *Az interneten valójában nagyon is megfizetünk dolgokért, méghozzá a lehető legfontosabb fizetőeszközzel: a személyes adatainkkal. Miközben az interneten olvasgatunk, az internet is olvasgat bennünket.* (*Frank Schätzing*)

A helyi önkormányzatok működésük, az önkormányzati feladatok ellátásuk során nagy számban kezelnek személyes adatokat. A teljes önkormányzati szektort egy nagy egésznek tekintve az egyik legnagyobb adatkezelő szervezetnek tekinthetjük, tekintettel arra, hogy az ország valamennyi lakosa érintett lehet az adatkezelés által.

A képviselő-testület szerveként működő polgármesteri hivatal, közös önkormányzati hivatal által végzett adatkezelési műveletek nagyságrendjét és típusait, feladataik ellátását befolyásolja a lakosságszám, az önkormányzat vagy társulás által fenntartott intézmények száma, rendelkezésre álló személyi és dologi erőforrások. Az adatvédelmi előírásoknak ugyanúgy eleget kell tennie egy pár száz fős község polgármesteri hivatalának, mint egy megyei jogú városának. Az ügyfélnek az ország bármely pontján ugyanolyan szinten kell, hogy érvényesüljön a személyes adatok védelméhez való joga, függetlenül attól, hogy éppen valamelyik budapesti kerületi önkormányzati vagy egy vidéki polgármesteri hivatalban intézi ügyeit.

Pozitívumként említhető, hogy egyre több önkormányzati honlapon elérhető a GDPR-konform adatkezelési tájékoztató a különböző ügyekhez, pályázatokhoz kapcsolódóan, egyre több település jelenti be az adatvédelmi tisztviselőjét a hatósági nyilvántartásba. Az átláthatóság és a szabályszerűség követelményének betartását többféle, interneten fellelhető módszertani kiadvány (szabályzatminták, felülvizsgálathoz útmutatók), elemzések, állásfoglalások, valamint informatikai fejlesztések egyaránt segítik. A hivatali munka minél magasabb színvonalon történő ellátásához számos önkormányzatokat érintő, rendezvényen, workshopon, szakmai konferencián vehetünk részt, ahol nyomon követhetjük a nemzetközi trendeket, hazai jó gyakorlatokat is.

A módszertani anyag iránytűként szolgál az adatvédelem tengerében az önkormányzati adatkezelés területén, a gyakorlati életben jól hasznosítható ajánlásokat fogalmaz meg, így az

[1] A szerző adatvédelmi és adatbiztonsági szakjogász, egy önkormányzati informatikai rendszerek fejlesztése területén évtizedes múlttal rendelkező, debreceni székhellyel rendelkező vállalkozás (eKÖZIG Zrt.) munkatársa, továbbá több önkormányzat esetében lát el adatvédelmi tisztviselői feladatokat.

adatvédelemmel foglalkozó önkormányzati köztisztviselők, adatvédelmi tisztviselők számára is hasznos olvasmány lehet.

1. Digitális korszakváltás a közigazgatásban

Az igazgatási folyamatok informatikai támogatása, kiszolgálása egyáltalán nem újkeletű dolog, ezzel a közigazgatásban évtizedes tapasztalattal rendelkező kollégák tisztában vannak, a közszolgák új generációja pedig már egy – valamilyen szinten – digitalizált közigazgatási rendszerbe csöppent bele az önkormányzati igazgatás területén is. Az 1990-es években már elektronikusan, DOS-os környezetben futtatott programok segítségével vezettek különböző nyilvántartásokat a központi közigazgatási szervek, majd hamarosan – ahogy egyre elérhetőbbé váltak az információtechnológiai eszközök – az önkormányzatoknál is elterjedtek az elektronikus népességnyilvántartó rendszerek, számlázó programok, iktatórendszerek. Ezek használhatósága a maiakéhoz képest lehet, hogy limitáltnak tűnik, de alkalmazásukkal abban az időpontban a közigazgatás is belépett az úgynevezett digitális korszakba. A szolgáltatások és a működés technológiai alapú megújítása nem csak a versenyszférában, hanem a közigazgatásban is stratégiai jelentőségűvé vált.

A technológiaalapú megújulás a digitalizáció és a digitális transzformáció fogalmához vezet. A *digitalizáció* kifejezés olyan folyamatok, eljárások vagy megoldások digitálissá válását jelenti, amelyek korábban (elsősorban vagy teljesen) fizikaiak vagy analógok voltak. Ilyen például, hogy egy eddig papíron végzett adminisztratív feladatot immár szoftveres segítséggel, vagy automatizálva végzünk el.

A *digitális transzformáció* ennél többet takar, egy folyamatos és összetett vállalkozást jelent a szervezet működésének átalakítására, nemcsak szervezeti szinten, hanem a teljes közigazgatási rendszerre kiterjedően valósult meg az elmúlt évtizedekben. A digitális transzformációhoz nemcsak egy innovatív technológia fejlesztése és implementálása szükséges, hanem komplex környezetváltás. A transzformáció fontos eleme az új képességekbe való befektetés és az erőforrások, folyamatok újraszervezése, újraelosztása is.[2]

Nem szabad elfelejteni, hogy a digitalizáció csak eszköz a közigazgatási rendszer átalakításában, olyan magasabb rendű célok elérése érdekében, mint például a hatékonyság növelése vagy az ügyféligények modern megoldásokkal történő kielégítése. Utóbbi cél egyre nagyobb hangsúlyt kapott az évek során, ami természetesen nem volt véletlen, hanem hosszú tervezési és fejlesztési folyamat eredményeként valósult meg. Valójában emiatt beszélhetünk digitális korszakváltásról a közigazgatásban, mert a közigazgatási szervek és az ügyfelek, a lakosság interakciója egy új szintre lépett a közelmúltban és több további nagyszabású fejlesztés is napirenden van. A klasszikus közfeladatok informatikai támogatása mellett pedig egyre gyakrabban kerül sor egyedi fejlesztések alkalmazására – ez a helyi önkormányzatok esetében jellemző –, illetve akár meglévő piaci megoldások igénybevételére is a közszféra szereplői által.

[2] Ld. http://unipub.lib.uni-corvinus.hu/4141/1/VT_2019n0708p88.pdf honlapot. (Letöltve: 2022.08.22.)

A technológia fejlődése és a közigazgatás átalakítása mellett a személyes adatok védelme és az információbiztonság meghatározó változáson ment keresztül az utóbbi években, nemzetközi és hazai szinten egyaránt. Manapság sokan megfogalmazták már azt a véleményt, hogy a 21. század aranya az *adat,* hiszen a modern világban az adat bír a legnagyobb jelentőséggel a versenyszférában és a közszférában. Sőt, talán a közigazgatásban van a legfontosabb szerepe az adatoknak, hiszen hazánkban a legnagyobb adatkezelők valószínűleg az állami szervek és az önkormányzatok, akik feladataik ellátása során nagy mennyiségű személyes adatok, különleges személyes adatot és nem személyes adatot (melyek között lehetnek üzleti titok tárgyát képező adatok, illetve minősített adatok is) kezelnek.

Mivel ezek az adatok a szerv működése szempontjából kiemelt fontossággal bírnak, megfelelő védelmükhöz – amely kiterjed az adatok bizalmasságára, sértetlenségére és rendelkezésre állására – kiemelt érdek fűződik, ugyanakkor biztosítani kell azt is, hogy az állam és más, az adatok kezeléséből és feldolgozásából előnyt szerző fél ne élhessen vissza a birtokába került információkkal, az adatok megszerzésére és felhasználására mindig jogszerű eljárás keretében kerüljön sor.

A következő részben röviden bemutatom a hazai közigazgatás digitalizációjának eddigi folyamatát, valamint azokat az aktuális trendeket, amelyeket érdemes figyelembe venni a helyi közigazgatás szereplőinek saját működésük digitális eszközökkel történő továbbfejlesztése során.

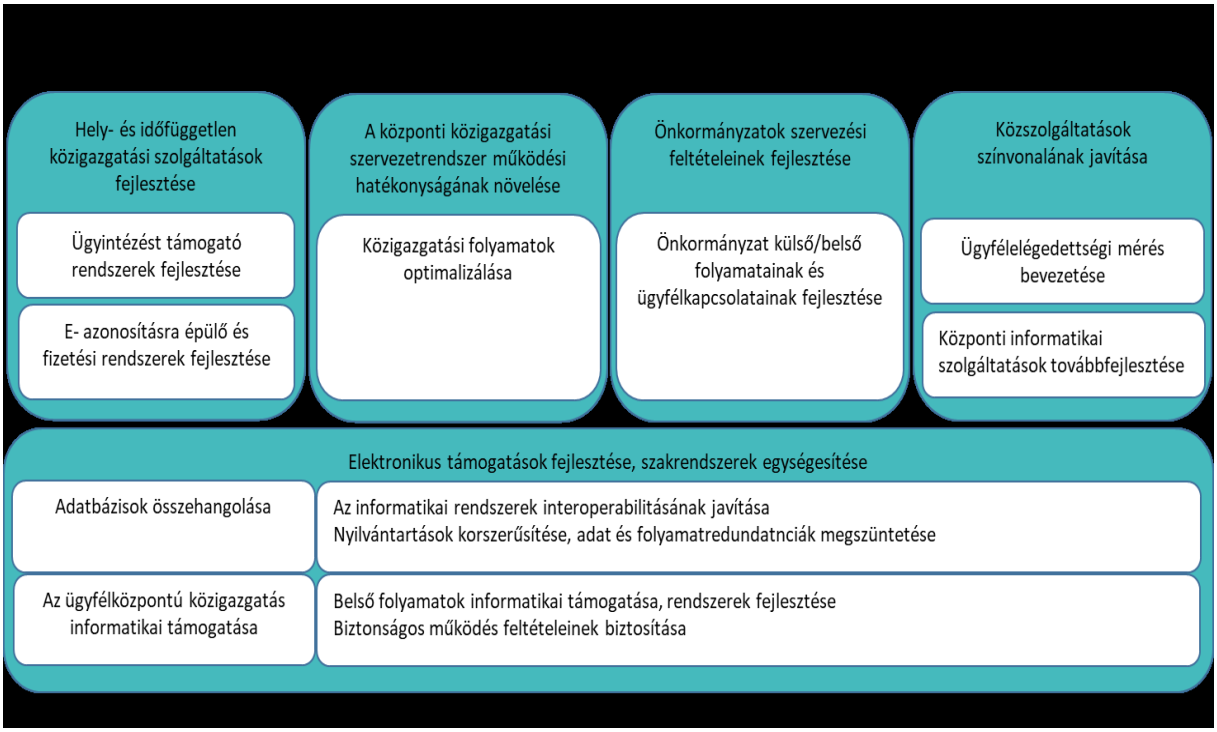
1.1 A közigazgatási rendszer megújulása

A közigazgatási rendszer átalakítását 2011-ben a Kormány a **Magyary Zoltán Közigazgatás-fejlesztési Program** elfogadásával alapozta meg. A névadó, a magyar közigazgatás egyik nemzetközileg is elismert legnagyobb tudósa Magyary Zoltán. Magyary és iskolája a maga korában, az első pontban már említett amerikai közigazgatás-tudomány korabeli tudományos üzemszervezési irányzatát próbálta összehangolni az Európai kontinens bürokrácia elveire épülő közigazgatásával. 2011. június 17-én mutatták be a közigazgatás-fejlesztési program első (MP11.0) változatát. Ennek és a **2012-ben elfogadott módosított változatának** a végrehajtása azonban olyannyira elhúzódott, hogy mára már egy egészen új program az, mely az államreform keretében 2015 elején elfogadásra került.[3]

A **Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia (KKFS)** a magyar közigazgatás 2020-ig elérendő céljait fogalmazza meg. Célja egy olyan szolgáltató állam létrehozása, amely professzionális, vagyis kiszámítható, jogszerű, szakszerű, etikus, költséghatékony és szervezett, azaz korszerű, optimális működésű, ügyfélközpontú. A szolgáltató állam megteremtése érdekében – többek között – kiváló szolgáltatási minőségű, biztonságos, költséghatékony e-

[3] Bővebben ld. Prof. Dr. Balázs István CSc.: A „JÓ KÖZIGAZGATÁS" ILLÚZIÓJÁRÓL című cikkét, 8. oldal. http://real.mtak.hu/73066/1/a_jo_kozigazgatas_illuziojarol.pdf . A letöltés ideje: 2022. szeptember 2.

közigazgatás megteremtését célozza meg, valamint fejlesztési területeket (és azokon belül beavatkozásokat) jelöl ki. A legfontosabb célokat az alábbi ábra szemlélteti.[4]



1. számú ábra: Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia legfontosabb céljai

Az **OECD 2017 decemberében** tette közzé **értékelését**[5] a magyar kormány 2015 februárjában elfogadott közigazgatás- és közszolgáltatás-fejlesztési stratégiájáról. **A „Közigazgatás- és Közszolgáltatás-fejlesztési Stratégia 2014-2020”** (továbbiakban: ***Stratégia*)** című dokumentumot a Miniszterelnökség készítette és terjesztette elő. Az OECD értékelésére a magyar Kormány kérésére került sor, azzal a céllal, hogy más OECD-tagországok tapasztalataira építve a szervezet tanácsokat fogalmazhasson meg a fenntarthatóság és az átfogó jelleg érvényesülése érdekében. Célja, hogy olyan közigazgatást formáljon, amely segíti Magyarország versenyképességének erősítését, erősíti a közintézményekbe vetett bizalmat azáltal, hogy ügyfélközpontú szolgáltatásokat biztosít az állampolgároknak és vállalkozásoknak, mindeközben hatékonyabbá teszi a kormányzati működést.

A jelentés ugyanakkor rámutat kritikus hiányosságokra is. Ilyen a korábbi sikerek és kudarcok részletes elemzése, valamint a fő célokhoz rendelt teljesítménymutatók hiánya. Az ajánlásokat is megfogalmazó OECD-dokumentum *három fő területre* fókuszál elemzési szempontként: az

[4] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 13. oldal. A letöltés ideje: 2022. szeptember 3.

[5] Az OECD értékelése a magyar Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiáról (2014-2020), I. rész https://hirlevel.egov.hu/2018/01/01/az-oecd-ertekelese-a-magyar-kozigazgatas-es-kozszolgaltatas-fejlesztesi-strategiarol-2014-2020-i-resz/ A letöltés ideje: 2022. szeptember 2.

emberi erőforrás menedzsmentre, a digitális kormányzásra és a költségvetési gyakorlatra. Az OECD értékelése szerint a Stratégia két fontos fókuszterülettel kellő mértékben foglalkozik: az emberi erőforrás menedzsmenttel és a „digitális állam" fejlesztésével. Mindkettő kulcsfontosságú a közszolgáltatások minőségének és elérhetőségének javítása szempontjából. A költségvetési gyakorlat felülvizsgálatát és reformját ugyanakkor hiányolja a jelentés. Bár a 2010 és 2013 között megvalósított **Magyary reformprogramok mélyreható változásokat eredményeztek**, magas szinten központosított közigazgatási rendszert hozva létre az ország minden területén, az elérhető magas színvonalú szolgáltatások és költségvetési megtakarítások érdekében, nem olvashatunk mélyelemzést arról, hogy miért nem érzékelhetőek eleddig számottevő nyereségei a reformoknak, a jelentős áramvonalasítás és egyszerűsítés ellenére sem. Az OECD dokumentuma kitér arra, hogy 114 intézkedés történt a vállalkozások adminisztratív terheinek mérséklése érdekében, ami 500 milliárd forintos megtakarítást jelent az üzleti szféra számára. A cégregisztráció egyszerűsítésében és az e-közigazgatás jogi kereteinek megalkotásában ugyanakkor további előrelépésre van még szükség. Az emberi erőforrás menedzsment területén szintén kulcsfontosságú eredmények születtek új értékelési rendszerek bevezetésével. További lépéseket szükséges tenni a valóban egyablakos ügyintézés megvalósítása érdekében is. A költségvetés tervezési folyamat megújítása kulcsfontosságú lehet a további eredmények szempontjából, ahogy a fő beavatkozási területekhez rendelt, részletes teljesítménymutatók bevezetése is.

A **Nemzeti Digitalizációs Stratégia 2021-2030** felhívja a figyelmet arra, hogy nagy hangsúlyt igényel az információbiztonság, a jelenleg is működő rendszer további fejlesztésével biztosítva az állami és önkormányzati szervek elektronikus információs rendszereinek biztonságos kialakítását, üzemeltetetését, továbbá a rendszer teljes életciklusára kiterjedő kockázatokkal arányos védelmét, minimalizálva a magyar kibertér biztonságát érintő károkat, különös tekintettel a létfontosságú rendszerek és az alapvető szolgáltatásokat biztosító rendszerek védelmére. [6]

1.2 Jogszabályi háttér

A digitalizáció folyamatával szorosan összefüggő első jogszabály elfogadására hazánkban több mint két évtizeddel ezelőtt került sor, ez volt **az elektronikus aláírásról szóló 2001. évi XXXV. törvény**. A jogalkotó felismerte az információs társadalom fejlődésének irányát, és kiemelt jelentőséget tulajdonított annak, hogy eleget tegyen az ezzel járó kihívásoknak. A törvény elfogadásának célja az volt, hogy megteremtse a **hiteles elektronikus nyilatkozattétel, illetőleg adattovábbítás jogszabályi feltételeit** az üzleti életben, **a közigazgatásban** és az információs társadalom által érintett más életviszonyokban. A hiteles elektronikus nyilatkozattétel alapvető fontossággal bír az elektronikus ügyintézés megteremtésében, így a jogszabály mérföldkőnek tekinthető ezen a téren.

[6] Nemzeti Digitalizációs Stratégia 72. oldal. Ld. https://2015-2019.kormany.hu/download/f/58/d1000/NDS.pdf honlapot. A letöltés ideje: 2022. szeptember 5. Készítette: Innovációs és Technológiai Minisztérium, Belügyminisztérium.

További lépcsőfok volt az állami digitalizáció folyamatában a nyilvánosság széleskörű tájékoztatása érdekében elfogadott **az elektronikus információszabadságról szóló 2005. évi XC. törvény,** amely többek között elektronikus közzétételi kötelezettséget írt elő a közfeladatot ellátó szervek számára, illetve biztosította a jogalkotás folyamatának és a bírósági határozatoknak a nyilvánosságát. A jogszabály jelentősége, hogy kötelező erővel megvalósította az elektronikus tájékoztatást a nyilvánosság számára a közérdekű adatok tekintetében, amely a közvélemény gyors és pontos tájékoztatását tette lehetővé, ezzel pedig javította a közigazgatási szervek működésének átláthatóságát.

Az **Alaptörvény XXVI. cikke** garanciális szabályként rögzítette, hogy az állam - a működésének hatékonysága, a közszolgáltatások színvonalának emelése, a közügyek jobb átláthatósága és az esélyegyenlőség előmozdítása érdekében - törekszik az új műszaki megoldásoknak és a tudomány eredményeinek az alkalmazására. Az Alaptörvény hivatalos indokolása szerint az államnak törekednie kell arra, hogy lépést tartson a modern kor technológiai fejlődésével és lehetőség szerint felhasználja azokat az új műszaki megoldásokat és más tudományos vívmányokat, amelyek az állam működésének hatékonyságát, a közszolgáltatások színvonalának emelését, a közügyek jobb átláthatóságát és a polgárok esélyegyenlőségét szolgálhatják.

Az elektronikus aláírásról szóló törvényben foglalt szabályokat végül 2016. július 1-jétől felváltotta **az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (E-ügyintézési tv.)**, amely szabályokat tartalmaz az elektronikus ügyintézésre (pl.: ügyfélként eljáró önkormányzat, jegyző, költségvetési szerv részére történő kötelező e-ügyintézés), az elektronikus kapcsolattartásra, illetve az elektronikus ügyintézést biztosító szervek működésére vonatkozóan. Az elektronikus ügyintézésről szóló törvény elfogadásával egyébként is az a célja a jogalkotónak, hogy az elektronikus működés felé terelje a hatóságokat, így az adatok ilyen formában történő tárolása csak egyre hangsúlyosabb lesz.[7]

Az Eüsztv. végrehajtási rendelete, **az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) Korm. rendelet** 2017. január 1-jétől a szolgáltatások és a központi szolgáltatások részletszabályait tartalmazza, ezzel egyidejűleg a 2012. évben elfogadott végrehajtási rendeletekből kettőt hatályon kívül helyezett. A 2012. évi végrehajtási rendeletek közül a kijelölő rendelet maradt hatályban, mely által **kijelölésre kerültek a hazai elektronikus közszolgáltatások működéséért felelő szervek**, a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., a Magyar Posta Zrt. és az IdomSoft Zrt., továbbá az e-közigazgatásért felelős miniszter és a KOPINT-DATORG Informatikai és Vagyonkezelő Kft.

2018. január 1-je a magyar közigazgatás fejlődéstörténetének fontos dátuma, ettől kezdődően hivatalosan is **elindult az e-közigazgatás Magyarországon**. Az államigazgatási szervek, helyi önkormányzatok, a törvény vagy kormányrendelet által közigazgatási hatósági jogkör gyakorlására feljogosított egyéb jogalany, a bíróságok, az alapvető jogok biztosa, az

[7] 2015. évi CCXXII. törvény- az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól - Preambulum

ügyészségek, közjegyzők, a bírósági végrehajtó, a köztestületek – kivéve a hegyközségeket – és a közüzemi szolgáltatók kötelesek voltak immár biztosítani az elektronikus ügyintézést[8]

2016-tól kezdődően több nagy jelentőségű és széles felhasználói kört érintő központi informatikai rendszerfejlesztés fejeződött be és kialakította az e-közigazgatás feltételeit (ilyen fejlesztés volt pl.: a szabályozott elektronikus ügyintézési szolgáltatások rendszere vagy az Önkormányzati ASP - Application Service Provider – alkalmazásszolgáltató központ). Az **Önkormányzati ASP** az önkormányzati feladatellátást támogató, számítástechnikai hálózaton keresztül távoli alkalmazásszolgáltatást nyújtó elektronikus információs rendszer. Az elektronikus ügyintézési szolgáltatások közül a legfontosabbak működési módját és feltételét – az ügyfelek biztonsága érdekében –az állam szabályozza és egy részét maga is szolgáltatja. Az állam által nyújtott szabályozott elektronikus ügyintézési szolgáltatások kifejlesztése az elektronikus ügyintézéshez szükséges, alapvető infokommunikációs háttérszolgáltatások rendelkezésre állását javította (pl.: e-azonosítás, e-hitelesítés, e-kézbesítés, e-iratkezelés, e-fizetés). Erre épülve egyre nagyobb arányban folytatható le elektronikus formában a belső ügyintézés, illetve az elektronikus úton is igénybe vehető közigazgatási szolgáltatások száma növekedhet. A **szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ)** bevezetésének kiemelt célja az interoperabilitás növelése, vagyis az egyes elektronikus rendszerek közötti együttműködési képesség javítása.

Az **általános közigazgatási rendtartásról szóló 2016. évi CL. törvény** (Ákr) 26. §-a úgy rendelkezik, hogy a hatóság írásban, az Eüsztv-ben meghatározott elektronikus úton vagy személyesen, írásbelinek nem minősülő elektronikus úton tart kapcsolatot az ügyféllel és az eljárásban résztvevőkkel. Ha törvény másként nem rendelkezik, a kapcsolattartás formáját a hatóság tájékoztatása alapján az ügyfél választja meg. Az ügyfél a választott kapcsolattartási módról más - a hatóságnál rendelkezésre álló - módra áttérhet. Életveszéllyel vagy súlyos kárral fenyegető helyzet esetén a hatóság választja meg a kapcsolattartás módját.
Az ügyfél az e-papír szolgáltatáson keresztül valamennyi ügytípusban kezdeményezhetnek eljárásokat 2018-tól kezdve, kivéve azon ügyeket, melyek tekintetében az elektronikus kapcsolattartás kizárt.

A **helyi önkormányzati szint digitalizációja 2019-re teljes mértékben megvalósult**, miután az önkormányzati ASP rendszerhez 2019. január 1-jével további mintegy 200 helyi önkormányzat csatlakozott, így annak szolgáltatásai immár a teljes hazai helyi önkormányzati szervezeti kört lefedik. Összesen **3197 önkormányzat** veszi igénybe a szolgáltatásokat, közülük 3158-an rendszercsatlakozóként, amely nemzetközi szinten is kiemelkedő eredmény. A rendszer 2021-ben európai szintű elismerést kapott. Az önkormányzatok esetében országosan a https://e-onkormanyzat.gov.hu/portálon érhetők el az ügyféloldali elektronikus ügyintézési szolgáltatások.
Lehetővé vált, hogy hazánk összes településére kiterjedően könnyen elérhető információk álljanak rendelkezésre elsősorban a helyi önkormányzatok **tervezési feladatainak információkkal történő támogatásához**, a helyi közszolgáltatásokra kiterjedő ellátás-és

[8] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 8. oldal. A letöltés ideje: 2022. szeptember 3.

finanszírozás-tervezési, valamint rendszerszintű szervezési feladatokhoz. Az **Önkormányzati ASP** elősegíti a hivatali munkavégzés szabványosított belső folyamatokkal történő támogatását, valamint egységes platformot biztosít az állampolgárok és a vállalkozások részére nyújtandó helyi önkormányzati szintű e-közigazgatási szolgáltatások nyújtására. A hazai digitális közszolgáltatásokat a Központi Kormányzati Szolgáltatás Busz (KKSZB) fogja össze, amely az adatbázisok összehangolása, az informatikai rendszerek interoperabilitása érdekében kialakított központi elektronikus ügyintézési szolgáltatás. Legnagyobb igénybe vevője az Önkormányzati ASP rendszer, de számos egyéb rendszer is használja. A KKSZB 2021-ben 234 féle adat-szolgáltatást tett lehetővé a 156 csatlakozott szervezet számára. A rendszerek egymással történő adatcseréje és az ennek kapcsán keletkező adatlekérdezések száma meghaladja a havi 100 millió tranzakciót.[9]

Az önkormányzati ASP kötelező kiterjesztésével nagyban javult az önkormányzatok információbiztonsági felkészültsége, azonban a szervezetek továbbra sem érik el az állami és önkormányzati szervek az **elektronikus információbiztonságáról szóló 2013. évi L. törvényben** (a továbbiakban: **Ibtv**.) eredetileg 2015. év végére elérendő biztonsági szintet, rendszereik pedig az elvárt biztonsági osztályt. Az Ibtv. kötelezővé tette minden önkormányzat, mint szervezet biztonsági szintjének meghatározását, azaz fel kellett mérniük az egyes szervezeti kockázataikat, illetve az elektronikus információs rendszereiknek meg kellett határozniuk az elvárt biztonsági osztályt, vagyis azt, milyen fizikai, logikai és adminisztratív intézkedések szükségesek a rendszerek működéséből adódó kockázatok kezelésére.[10] Az Ibtv. egyik végrehajtási rendelete **41/2015. (VII. 15.) BM rendelet,** amely konkrét biztonsági intézkedéseket határoz meg a címzettek számára.

A magánszférában jogszabályi előírások hiányában a szervezetek ún. **szabványokat** alkalmaznak, amelyeket nagy nemzetközi szabványügyi szervezetek adnak ki, és lényegüket tekintve az adott szakterületen alkalmazott legjobb megoldások egységes szerkezetbe foglalt leírásai. Az információbiztonság területén a legismertebb és leggyakrabban alkalmazott ilyen szabvány az **ISO/IEC 27001:2013**, amelyet az **Európai Uniós Hálózat- és Információbiztonsági Ügynökség** is alapul vett a GDPR adatbiztonsággal kapcsolatos kötelezettségeinek teljesítésére vonatkozó iránymutatásaiban.[11] Ez azért bír nagy jelentőséggel, mert az Ibtv. megalkotása során a jogalkotó nagy mértékben merített ihletet a szabványból, így a törvény rendelkezései nagyon hasonlóak az abban foglaltakhoz, sőt maga a törvény is úgy fogalmaz, hogy a nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat, illetve független, képesített ellenőr által készített ellenőri jelentéseket a hatóság az eljárása során figyelembe veszi.[12]

---

[9] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 10. oldal. A letöltés ideje: 2022. szeptember 3.

[10] Nemzeti Digitalizációs Stratégia 74. oldal. Partnerségi konzultációra bocsátott. Ld. https://2015-2019.kormany.hu/download/f/58/d1000/NDS.pdf honlapot. A letöltés ideje: 2022. szeptember 5. Készítette: Innovációs és Technológiai Minisztérium, Belügyminisztérium.

[11] Handbook on Security of Personal Data Processing, European Union Agency for Network and Information Security (2018)

[12] Ibtv. 4. §

Az Ibtv. szabályozásának középpontjában az elektronikus információs rendszer és az abban tárolt adatok állnak, amelyek között nem csak személyes adatok vannak, hanem a szervezet tevékenységével kapcsolatos bármely egyéb információ. A kezelt személyes adatok mennyisége és típusa **az információs rendszerek ún. biztonsági osztályba sorolásánál** is kiemelt szempontként jelenik meg, amely összhangban van a GDPR 24. cikkében körülírt „kockázatokkal arányos" védelem elvével. Ahogy az a törvény címéből is kiderül, elsősorban az elektronikusan tárolt (a Rendelet szerinti automatizált módon történő adatkezelés) információk védelmét biztosítja a követelmények teljesítése, de a kontrollok között találunk számos olyan előírást is, amelyek általános jelleggel növelik az információbiztonság szintjét, ilyen például a fizikai biztonsági intézkedések köréből a fizikai belépések ellenőrzése vagy a behatolás riasztás.[13]

Az okos város központi platformszolgáltatás létrehozásáról és működtetéséről szóló 252/2018. (XII. 17.) Korm. rendeletet 2018. év végén fogadta el az Országgyűlés. A Korm. rendelet 2. § (1) bekezdése alapján a Kormány okos város központi platformszolgáltatást működtet a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter útján, a helyi önkormányzatokért felelős miniszter közreműködésével. Ezt a platformszolgáltatást a helyi önkormányzatok vehetik igénybe. Monor városa lett jelölve pilot projekt helyszínként.

Komplex informatikai rendszer létrehozására irányult az **Integrált Közszolgáltatási Információs Rendszer (IKIR)** projekt, amelyből olyan adatok és információk nyerhetők, amelyek megalapozott döntések meghozatalát teszik lehetővé helyi szinten. [14]

1.3 Aktuális trendek

Az elektronikusan intézhető ügyek száma folyamatosan nőtt, 2021 szeptemberében már több mint 2400 ügyleírás volt megtalálható a magyarorszag.hu oldalon. A NISZ szolgáltatásai között érhető el a 2020 márciusától működő **Személyes Ügyintézési Felület (SZÜF)**, amely megújult felülettel és megközelítéssel biztosítja az általános e-ügyintézési gyűjtő portál funkciókat. A szolgáltatás keretében elektronikus formában érhető el tájékoztatás az e-közigazgatási szolgáltatásokra vonatkozóan, elérhetővé teszi a **kapcsolódó nyomtatványokat**, mind a központi, mind a területi és helyi közigazgatási szervek szolgáltatásai tekintetében.[15]

Az E-önkormányzat portál **(Önkormányzati Hivatali Portál)** az önkormányzati ASP-rendszerben az elektronikus önkormányzati ügyintézés helyszíne**.**[16] Ügyféloldali szempontból jelentős előrelépés az, hogy ennek révén az önkormányzatok magasabb színvonalon, sztenderdizált, országosan egységes módon képesek az ügyfeleiknek szolgáltatásokat nyújtani.

[13] 41/2015. (VII. 15.) BM rendelet 4. melléklet 3.2 pontja
[14] Bővebben lásd. https://ikir.bm.gov.hu/ honlapot a helyi közszolgáltatás információs rendszerről (IKIR)
[15] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 11. oldal. A letöltés ideje: 2022. szeptember 3.
[16] Ld. a https://ohp-20.asp.lgov.hu/nyitolap honlapot.

A digitalizáció terén fontos előrelépést jelentett, hogy **2020. február 1-jétől** az Eüsztv. alapján az elektronikus ügyintézést biztosító szerv köteles az e-ügyintézési szolgáltatásainak működtetéséhez és az ügyintézésbe bevont társszervekkel való kapcsolattartáshoz szükséges belső működését, **folyamatait teljeskörűen elektronizálni**, ehhez biztosítani az elektronikus információs rendszereket. A fejlődés az ügyféloldali e-szolgáltatások terén is megmutatkozott, hozzájárult ahhoz, hogy a közigazgatás strukturáltabb, átláthatóbb, ügyfélközpontúbb legyen. A szolgáltatási paletta bővülése lehetővé tette, hogy az ügyfelek egyre több e-szolgáltatást igénybe tudjanak venni. [17]

A Kormány döntött a **Mesterséges Intelligencia Stratégia** megalkotásáról, melyben 2030-ig szóló célokat jelöl ki és ezekhez kapcsolódóan **2025-ig tartó intézkedési tervet** vázol fel, amely a technológia által nyújtott előnyök kihasználását célozza. A stratégia államigazgatás vonatkozásában megfogalmazott céljai, a közszolgáltatások elektronikus elérésének, digitalizációjának elősegítése, a közigazgatási folyamatok MI segítségével történő automatizációja által, a chat alapú digitális egyablakos ügyintézés kiépítése, levelezési, chat és telefonos ügyfél kapcsolattartási folyamatok automatizációja, mesterséges intelligenciával támogatott kommunikációs asszisztens, önkiszolgálást lehetővé tevő ügyek számának bővítése, videotechnológiás kapcsolattal történő ügyintézés. A mesterséges intelligencia alapú automatizáció, az elektronikus térben elvégzett, videotechnológián alapuló képazonosítás, a hangazonosításra épülő hangvezérlés, az intelligens dokumentum kezelő rendszerek, hitelesítési folyamatok tehát csak akkor lehetnek hatékonyak, ha minden állampolgár számára elérhetőés kezelhető műveletek, alkalmazások képezik alapjukat. [18]

Ma **Magyarországon több cég** is foglalkozik a helyi önkormányzat feladatainak széles körét érintő alkalmazásfejlesztési tevékenységgel. Az **eKÖZIG Zrt** alkalmazásfejlesztési tevékenysége a helyi közigazgatás feladatainak széles körét költséghatékony, on-line módon támogatja. Tudásalapú megközelítést alkalmaz, többek között a településüzemeltetési feladatok térinformatikai támogatása, a helyi adóügyintézés elektronikus útra terelése, a képviselő-testületi, bizottsági döntés-előkészítés és döntéshozatal folyamatainak elektronizálása területén tekintetében jelentős eredményt értek el. Megvizsgálják a jelenlegi ügyintézési, döntéshozatali gyakorlatot, majd átfogó modell megalkotását követően hívják segítségül az információs technológiák valamely, adott feladat kiszolgálásához illeszkedő eszközét.[19]

A cég ennek eredményeképpen a mindenkori jogszabályi környezetnek megfelelő, az önkormányzati ügyintézési gyakorlathoz illeszkedő, szabványos alapokon építkező rendszer kialakítását valósítja meg. Ennek köszönhetően földrajzi helytől, településnagyságtól független, homogén szolgáltatási színvonal valósítható meg a rendszerüket felhasználó önkormányzatok számára. Fontos kiemelni, hogy **valamennyi fejlesztés üzemeltethető ASP környezetben.**

[17] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 12. oldal. A letöltés ideje: 2022. szeptember 3.

[18] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 30. oldal. A letöltés ideje: 2022. szeptember 3.

[19] Ld. az E-Közig Zrt honlapját: https://www.ekozig.hu/portal/oldal.aspx?azon=4 A letöltés ideje: 2022. szeptember 3. Bemutatkozunk.

További újdonságként az egyes rendszerek (ügyintézés, döntéstámogatás) felé érkező nagytömegű adatok két dimenziós vonalkód technológiával történő feldolgozása emelhető ki.[20]

2. Az önkormányzati adatkezelés sajátosságai és kihívásai a GDPR-ban foglalt általános szabályokkal kapcsolatosan

Az önkormányzati adatkezeléssel közvetlenül összefüggésbe hozható rendelkezése viszonylag kevés van a GDPR-nak, ami nem jelenti azt, hogy ne lenne számos olyan körülmény (jogi és ténybeli egyaránt), amely **jelentős eltérésekhez vezet a magánszféra adatkezeléseihez képest.** Ilyen eltérések megfigyelhetőek az előírt alapvető kötelezettségek teljesítése során is. *Az adatvédelem és az önkormányzati adatbiztonság szorosan egymáshoz kapcsolódó témakörét annak terjedelme miatt most nem tárgyalom.*

Az alábbiakban a GDPR legfontosabb központi fogalmai és az általános kötelezettségek kerülnek vizsgálatra az önkormányzatok szempontjából, kifejezetten a **gyakorlati kérdésekre** koncentrálva.

2.1 Az adatkezelő személye

A GDPR szerint **adatkezelő**[21] az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Az **Info tv**[22]. hatályos rendelkezése alapján az **adatkezelő** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

A szabályozás középpontjában az **adatkezelő** áll, ő az, akit az adatkezeléssel kapcsolatban a kötelezettségek terhelnek és őt terheli a felelősség az adatkezelés jogszerűségének biztosításáért. Az adatkezelő hozza meg **az adatkezelésre vonatkozó érdemi döntéseket,** amelyek magukban foglalják többek között az adatkezelés céljának, jogalapjának, a kezelt adatok körének meghatározását, adatfeldolgozó igénybevételéről és az adatbiztonsági intézkedésekről való döntést.[23]

Az önkormányzati adatkezelések körében több eltéréssel találkozhatunk az adatkezelő személyéhez kötődően. Önmagában az is kihívást jelent, hogy megállapítsuk egy adatkezelés esetén, **ki is minősül adatkezelőnek**. Az adatkezelő fentebb vázolt szerepe miatt látható,

[20] Ld. az E-Közig Zrt honlapját: https://www.ekozig.hu/portal/oldal.aspx?azon=4 A letöltés ideje: 2022. szeptember 3. Bemutatkozunk.
[21] GDPR 4. cikk 7. pont
[22] Az információszabadságról szóló 2011. évi CXII. törvény 3. § 9. pont.
[23] Péterfalvi Attila, Révész Balázs, Buzás Péter (szerk.): Magyarázat a GDPR-ról. 81. oldal.

kulcskérdés az ő személyének azonosítása egy adatkezelési tevékenység kapcsán, hiszen ez fogja meghatározni, hogy kit terhelnek a GDPR-ban előírt feladatok, kicsodán lehet számon kérni, ha az adatkezelés nem felel meg a jogszabályban előírt követelményeknek.

A hétköznapi adatkezelések nagy részében nem jelent problémát az adatkezelő azonosítása, mint pl. egy munkaviszonyban vagy egy webshop esetében. Egy több telephellyel rendelkező multinacionális vállalatcsoport esetében ez már koránt sem ilyen egyszerű, de említhetnénk az Európai Bíróság egyik döntését is, amelyben kimondta, hogy egy Facebook oldal üzemeltetése során nem csak az azt létrehozó személy vagy szervezet minősül adatkezelőnek, hanem maga a Facebook is.[24]

Az **önkormányzatok** nagyon **összetett szervezetrendszerrel rendelkeznek**, összehasonlítva a magánszférába tartozó gazdasági társaságok többségével. Az Mötv. 41. § határozza meg az önkormányzat és szerveinek jogállását.

Az önkormányzati feladatok ellátását a **képviselő-testület és szervei** biztosítják. A képviselő-testület szervei: a polgármester, a főpolgármester, a vármegyei közgyűlés elnöke, a képviselő-testület bizottságai, a részönkormányzat testülete, a polgármesteri hivatal, a vármegyei önkormányzati hivatal, a közös önkormányzati hivatal, a jegyző, továbbá a társulás.

Önkormányzati döntést a képviselő-testület, a helyi népszavazás, a képviselő-testület felhatalmazása alapján a képviselő-testület bizottsága, a részönkormányzat testülete, a társulása, a polgármester, továbbá a jegyző hozhat. A képviselő-testület - e törvényben meghatározott kivételekkel - hatásköreit a polgármesterre, a bizottságára, a részönkormányzat testületére, a jegyzőre, a társulására ruházhatja át. E hatáskör gyakorlásához utasítást adhat, e hatáskört visszavonhatja. [25]

Az itt felsorolt szervek közül gyakorlatilag bármelyik lehet önálló adatkezelő, de akár közös adatkezelés is fennállhat, sőt a **hatáskör átruházásával** akár az **adatkezelői minőség is átszállhat,** ahogy ezt a NAIH egyik állásfoglalása is megerősítette.[26]

Felvetődhet a kérdés, hogy a helyi önkormányzat esetében ki minősül adatkezelőnek: az önkormányzat vagy a polgármesteri hivatal (közös önkormányzati hivatal)?

A NAIH álláspontja alapján **adatkezelőnek a képviselő-testület azon szerve** (például polgármester, a képviselő-testület bizottságai vagy a polgármesteri hivatal) fog minősülni, aki a jogalkotó szerint a **kötelezően ellátandó** önkormányzati vagy államigazgatási **feladat- és hatáskör címzettje**. Az **önként vállalt** önkormányzati feladat- és hatáskörök gyakorlása céljából szükséges adatkezelések esetében pedig az adatkezelő személyéről **a települési önkormányzat képviselő-testülete a rendeletében** dönt.[27]

Bár a törvény kimondja, hogy csak az önkormányzat rendelkezik jogi személyiséggel (illetve az államháztartásról szóló törvény alapján a költségvetési szervek is)[28], az adatkezelő

[24] Az Európai Bíróság C-210/16. sz. ügyben hozott ítélete
[25] Mötv. 41. § (2) - (4) bek.
[26] NAIH/2017/5364/2/V állásfoglalás – letölthető: https://www.naih.hu/files/NAIH-2017-5364-2-V.pdf
[27] NAIH/2017/5364/2/V állásfoglalás – letölthető: https://www.naih.hu/files/NAIH-2017-5364-2-V.pdf
[28] Áht. 7. § (1) bek.

fogalmának GDPR-beli meghatározása szerint erre nincs szükség ahhoz, hogy valaki adatkezelőnek minősüljön. Sőt a személyes adatok kezelésével kapcsolatos bírósági eljárások során az egyébként főszabály szerint perbeli jogképességgel nem rendelkező szerv is lehet fél.[29] Az új közigazgatási perrendtartás alapján szintén lehet fél bármely potenciális önkormányzati adatkezelő szerv, így például egy NAIH határozat megtámadása esetén is.[30]

A helyzetet tovább bonyolítja, hogy a képviselő-testület a feladatkörébe tartozó közszolgáltatások ellátására **költségvetési szerveket** (pl. óvodák, szociális intézmények, könyvtár) **gazdálkodó szervezeteket** (pl. BKK vagy a városi vagyonkezelő cégek) vagy akár egyéb szerveket hozhat létre, amelyek szintén lehetnek adatkezelők.[31]

Közterület-felügyelet létrehozható a polgármesteri hivatal belső szervezeti egységeként, önálló költségvetési szervként vagy költségvetési szerv belső szervezeti egységeként, amely szintén kihatással lehet az adatkezelő személyére.[32] Nem szabad elfeledkezni arról sem, hogy jogszabály önálló feladatokat utalhat a polgármester vagy a jegyző hatáskörébe is.

Mint látható az önkormányzatok esetében különböző szervek vagy személyek nagy számú és eltérő jellegű adatkezelési tevékenységet végeznek, így kérdés, hogy **milyen módon lehetséges azonosítani** az egyes esetekben az **adatkezelőt.** A magánszférában a legtöbb esetben ez az adatkezelő saját elhatározásán alapul, amikor úgy dönt, hogy feladatának ellátásához személyes adatokat kezel, de gyakori eset az is, amikor egy jogszabály meghatározza vagy az abban foglalt rendelkezések értelmezése útján megállapítható, hogy ki minősül adatkezelőnek.[33] Erre maga a GDPR is lehetőséget ad az **adatkezelő** fogalmát meghatározó passzus utolsó fordulatában. Mivel az önkormányzatok alapfeladatait jogszabályok rögzítik, így ezekben az esetekben megállapítható az adatkezelő személye, aki a feladat vagy hatáskör címzettjével lesz azonos.

Segítséget adhat az eligazodáshoz a Belügyminisztérium által negyedévente kiadott és frissített **Önkormányzatok Elektronikus Hatásköri Jegyzéke,** amely az önkormányzatok és szerveik feladat- és hatáskörére vonatkozó hatályos jogszabályi rendelkezések listáját tartalmazza.[34] Az elektronikus dokumentumban a képviselő-testület, a bizottság, a polgármester, a jegyző, a hivatal ügyintézőjének feladat- és hatáskörét ágazatok szerint külön fájlok tartalmazzák.

Az **önkormányzatoknak** nem csak **kötelező,** hanem **önként vállalt feladatai** is lehetnek, valamint vállalkozási tevékenységet is folytathat.[35] A helyi önkormányzat - a helyi képviselő-testület vagy a helyi népszavazás döntésével - **önként vállalhatja** minden olyan helyi közügy önálló megoldását, amelyet jogszabály nem utal más szerv kizárólagos hatáskörébe. Az önként vállalt helyi közügyekben az önkormányzat mindent megtehet, ami jogszabállyal nem ellentétes. Az önként vállalt helyi közügyek megoldása nem veszélyeztetheti a törvény által

[29] Info. tv. 23. § (4) bek.
[30] Horváth E. Írisz – Kalas Tibor – Kárpáti Magdolna – Kurucz Krisztina – Marosi Ildikó – Márton Gizella – Mudráné Láng Erzsébet – Petrik Ferenc – Rothermel Erika – Tóth Kincső: A közigazgatási perrendtartás magyarázata, Budapest, HVG-ORAC (2017) 93. oldal
[31] Mötv. 41. § (6) bek.
[32] 1999. évi LXIII. törvény 1. § (2) bek.
[33] Péterfalvi – Révész – Buzás: i.m. 82. oldal
[34] A Hatásköri Jegyzék a kormany.hu oldalról tölthető le, negyedévente frissül.
[35] Mötv. 10. §

kötelezően előírt önkormányzati feladat- és hatáskörök ellátását, finanszírozása a saját bevételek, vagy az erre a célra biztosított külön források terhére lehetséges.[36]

A feladat- és hatáskör vállalásáról a települési önkormányzat képviselő-testülete - a feladat- és hatáskör eredeti címzettjének előzetes egyetértése esetén - rendeletben, a társulás határozatban dönt a feladat- és hatáskör vállalás tervezett időpontját megelőzően legalább három hónappal korábban. [37] Az önkormányzati rendeletben az Infotv. 5. § (3) bekezdése alapján meg kell határoznia az adatkezelő személyét is, amennyiben az adott közfeladat személyes adatok kezelésével is együtt jár. Ilyen esetben tehát maga a **képviselő-testület jelölheti ki**, hogy az adott tevékenységgel kapcsolatban **ki minősül adatkezelőnek.**

Vannak azonban olyan esetek is, amelyekre nincsenek jogszabályi előírások, hiszen a helyi közügyek intézése, a helyi közélet zajlása akarva-akaratlanul is együtt jár személyes adatok kezelésével, és ezeket nem lehet vagy nagyon körülményes lenne egytől egyig jogszabályban leszabályozni, ezért nem is nagyon találunk rá példát. Ilyen lehet például az önkormányzati tisztviselők vagy képviselők **közösségi médiahasználata.** Több olyan eset is volt a közelmúltban, amikor egy polgármester saját közösségi oldalán jogsértő vagy legalábbis kezdetben jogsértőnek vélt módon tett közzé személyes adatokat, amely alapján NAIH vizsgálat is indult.[38] Kérdés, hogy megállhat-e ilyen esetben a polgármester önálló adatkezelői minősége, és még ha a jogsértő magatartással kapcsolatban az önkormányzat ellen is indul vizsgálat, ettől függetlenül a közösségi oldal üzemeltetése során – amennyiben nincs erre vonatkozó semmilyen belső szabályzat – a polgármester önállóan hozza meg a döntéseket. Célszerű a tevékenységről az **önkormányzat adatkezelési szabályzatában** rendelkezni, amely által a képviselő-testület határozhatja meg az adatkezelési célját és eszközeit, valamint az elvárt magatartási normákat. Hasonló problémát jelenthet, amikor az önkormányzat hivatalos lapját a polgármester szerkeszti, anélkül, hogy bármiféle jogi aktus ezt a hatáskörébe utalná.

Az önkormányzati szervezetrendszernek további sajátossága, hogy az egyes szervek vagy **intézmények nem egymástól függetlenül végzik a tevékenységeiket**, emiatt nem mindig lehet a szerepeket olyan jól elválasztani, mint ahogy azt a GDPR egyébként megkövetelné. Egy önkormányzati fenntartású intézmény (pl. óvoda) esetében a munkáltatói jogokat az intézményvezető gyakorolja, a foglalkoztatási jogviszony az intézménnyel áll fenn, de előfordulhat, hogy a személyi anyagok kezelését, az átsorolásokat a polgármesteri hivatal (közös önkormányzati hivatal) illetékes osztálya végzi, hiszen nem minden költségvetési szerv esetében lehetséges önálló, államháztartási jogban képzett mérlegképes könyvelőt alkalmazni.

Az önkormányzat és az intézmény a gazdálkodással kapcsolatos munkamegosztás és felelősségvállalás rendjéről **munkamegosztási megállapodást** köt **az államháztartásról szóló 2011. évi CXCV. törvény** (a továbbiakban ***Áht.***), valamint az **államháztartási törvény végrehajtásáról szóló 368/2011. (XII.31.) Korm. rendelet** (továbbiakban ***Ávr.***) 9.§ (5) bekezdésében szabályozottak alapján.

[36] Mötv. 10. § (2) bek.
[37] Mötv. 12. § (2) bek.
[38] https://www.magyarhirlap.hu/belfold/20191223-adatvedelmi-vizsgalat-jozsefvarosban (2020.04.23.)

Önkormányzati fenntartású óvoda esetében a megállapodás tárgya általában nem terjed ki a közfeladatként ellátott, közvetlen szakmai tevékenységekre, az óvodai nevelésre és az ehhez kapcsolódó szakmai nyilvántartások vezetésére és adatszolgáltatásokra. A megállapodás célja, hogy a pénzügyi, számviteli rend betartásával a munkamegosztás és felelősségvállalás szakszerű rendjének szabályozása mellett segítse a gazdaságos és hatékony intézményi gazdálkodást, biztosítsa a szervezeti feltételeket és egyértelműen rögzítse a feladat-, hatáskörök megosztását. A megállapodásban rögzíteni kell, mely szervezet (pl. polgármesteri hivatal, közös önkormányzati hivatal vagy egyéb gazdasági szervezet) látja el az intézmény tervezési, gazdálkodási, finanszírozási, adatszolgáltatási és beszámolási, valamint a működtetéssel, üzemeltetéssel, a vagyon használatával, védelmével összefüggő feladatait az óvoda szakmai döntéshozó szerepét. A munkaügyi adatok kezelése, nyilvántartása, továbbítása a Magyar Államkincstár által rendelkezésre bocsátott KIRA Illetmény-számfejtési rendszeren keresztül valósul meg. A megállapodásban egyértelműen rögzíteni szükséges - tekintettel arra, hogy a szerződő felek a szerződés teljesítése során adatvédelmi kötelezettség alá eső adatokat és iratokat is megismerhetnek - önálló kötelezettségükként elfogadják, hogy a megállapodással összefüggő bármilyen tevékenységük végzése során az irányadó adatvédelmi szabályokat betartják és ellenőrzési körükbe tartozóan a munkavállalóikkal is betartatják. Ebben az esetben az **Óvoda adatkezelőként**, míg a **polgármesteri hivatal (közös önkormányzati hivatal) vagy a gazdasági szervezet adatfeldolgozóként**, esetlegesen **közös adatkezelőkként** felel az érintettek irányába.

Az **adatfeldolgozó fogalmát** a GDPR meghatározza, miszerint az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.[39]

A gazdasági szférában, ha egy külső szerv vagy személy végzi a bérszámfejtést, akkor a felek **adatfeldolgozói szerződést** kötnek.[40] A szerződés helyett más jogi aktussal is létrejöhet az adatfeldolgozói jogviszony, de a tartalmi követelmények azonosak ilyen esetben is. Az önkormányzati szervek szoros együttműködése (vagy nagyon egyszerűen úgy is fogalmazhatnánk, hogy a gyakorlatban szinte mindenkinek minden feladatát a polgármesteri hivatal vagy közös önkormányzati hivatal segíti) gyakran felvethetné annak vizsgálatát, hogy a személyes adatok kezelésére mégis milyen formában kerül sor, de egy erről szóló, az adatfeldolgozói szerződés tartalmi követelményeit magában foglaló jogi aktuson alapuló adatfeldolgozás bizonyára nagyon ritka.

Az adatfeldolgozó kötelezettségei:[41]

- a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli,
- titoktartási kötelezettsége van,
- biztonsági intézkedéseket alkalmaz,
- speciális szabályok további adatfeldolgozó igénybevételére,

[39] GDPR 4. cikk 8. pont
[40] GDPR 28. cikk
[41] Ld. Az adatkezelők és az adatfeldolgozók felelőssége című NAIH által készített ppt-t. (STAR projekt). These training materials are based on standard training materials developed in the context of the project "Supporting Training Activities on the Data Protection Reform" – STAR (http://www.project-star.eu/)

- megfelelő technikai és szervezési intézkedésekkel segíti az adatkezelőt abban, hogy teljesítse az érintettek jogaik gyakorlásához kapcsolódó kérelmét,
- az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek,
- az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges.

Az adatfeldolgozó felelőssége az elszámoltathatóság elvének való megfelelésben:[42]

- az adatkezelő utasításai alapján végzi az adatkezelést,
- azonos kötelezettségek terhelik a további alvállalkozókat is,
- nyilvántartást vezet az adatkezelési tevékenységéről,
- az adatkezelés befejezését követően, az adatkezelő utasítása alapján, törli a személyes adatokat,
- segíti az adatkezelőt a GDPR-nak való megfelelésben (pl. adatvédelmi hatásvizsgálat, biztonsági intézkedések, adatvédelmi incidens bejelentések során),
- elősegíti az érintettek joggyakorlását,
- minden adattovábbításról tájékoztatja az adatkezelőt.

A GDPR szerinti **elszámoltathatóság** azt jelenti, hogy az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.[43]

Az elszámoltathatóság eszközeire példák a GDPR-ban[44]**:**

- jóváhagyott magatartási kódexek vagy tanúsítási mechanizmusok betartása (40. cikk, 42. cikk)
- adatvédelemért felelős személy kijelölése (pl. adatvédelmi tisztviselő) (37. cikk)
- rendszeres kommunikáció folytatása az adatvédelmi tisztviselő és az adatvédelemért felelős személyek között (38. cikk)
- adatvédelmi képzések lefolytatása (39. cikk)
- adatvédelmi hatásvizsgálat lefolytatása a meglévő vagy új programok, rendszerek vagy folyamatok bevezetésére vagy módosítására (35. cikk)
- potenciális adatfeldolgozók adatvédelmével és biztonsági intézkedéseivel kapcsolatos kellő gondosság tanúsítása (28. cikk)
- az adatbiztonság szintjének rendszeres ellenőrzése (32. cikk)

[42] Ld. Az adatkezelők és az adatfeldolgozók felelőssége című NAIH által készített ppt-t. (STAR projekt). These training materials are based on standard training materials developed in the context of the project "Supporting Training Activities on the Data Protection Reform" – STAR (http://www.project-star.eu/)

[43] Ld. Az adatkezelők és az adatfeldolgozók felelőssége című NAIH által készített ppt-t. (STAR projekt). These training materials are based on standard training materials developed in the context of the project "Supporting Training Activities on the Data Protection Reform" – STAR (http://www.project-star.eu/) és GDPR 24. cikk

[44] Ld. Az adatkezelők és az adatfeldolgozók felelőssége című NAIH által készített ppt-t. (STAR projekt). These training materials are based on standard training materials developed in the context of the project "Supporting Training Activities on the Data Protection Reform" – STAR (http://www.project-star.eu/)

- az adatkezelési tevékenység önellenőrzése (24. és 29. cikk)
- az adatkezelés jogalapjának dokumentálása (6., 9. és 10. cikk)
- a beépített és az alapértelmezett adatvédelem biztosítása (25. cikk)
- az aktuális adatvédelmi követelmények, például jogszabályok, joggyakorlat, kódexek, stb. azonosítása (39. cikk)
- az érintettek jogainak gyakorlására vonatkozó intézkedések és eljárások végrehajtása (12. és 24. cikk)
- a beépített adatvédelem integrálása a rendszer- és termékfejlesztésekbe (25. cikk)
- az adatvédelem beépítése az információbiztonsági politikába, nyilvántartásmegőrzési-gyakorlatokba (5. és 32. cikk)
- az adatvédelmi kockázatok biztonságikockázat-értékelésekbe történő beépítése (32. cikk)
- adatvédelmi incidensek bejelentése (szabályozó szervek, hitelintézetek, bűnüldözési szervek felé), valamint értesítés az érintettek számára (12., 33. és 34. cikk)
- cselekvési terv kidolgozása adatvédelmi incidens esetére (33. és 34. cikk)
- adatvédelmi szabályzat kidolgozása (5., 24. és 91. cikk)
- adatvédelmi incidensek, valamint szabálysértések nyilvántartása (33. cikk)
- nyilvántartás a kezelt személyes adatokról, milyen személyes adatokat és hol kezelnek (30. cikk)
- tanúsítás, akkreditálás vagy adatvédelmi védjegy a szabályoknak való megfelelés igazolására (42. cikk)
- megfelelés az adatvédelmi követelményeknek a harmadik személyek adatkezelése során - pl. ügyfelek, adatfeldolgozók (28. és 32. cikk)
- a megfelelést, elszámoltathatóságot igazoló bizonyítékok dokumentációja (5. és 24. cikk)
- adatvédelmi hatásvizsgálatra vonatkozó iránymutatások és minták követése (35. cikk)
- a gyermekek és a kiskorúak személyes adatainak gyűjtésére és felhasználására vonatkozó szabályok, eljárások fenntartása (8. és 12. cikk)
- különleges személyes adatok (ideértve a biometrikus adatokat) gyűjtésére és felhasználására vonatkozó szabályok vagy eljárások fenntartása (9. és 10. cikk)
- valamennyi adatfeldolgozóval kötött szerződés vagy megállapodás végrehajtására vonatkozó eljárás alkalmazása (28. és 29. cikk)
- kérelmeket megválaszoló eljárások biztosítása, mechanizmusok alkalmazása, melyek által az érintettek frissíthetik vagy javíthatják személyes adataikat (16. és 19. cikk)
- a személyes adatokhoz való hozzáférés korlátozására irányuló eljárások kidolgozása - pl. szerep alapú hozzáférés, feladatok szétválasztása (32. cikk)
- technikai biztonsági intézkedések alkalmazása - pl. behatolás észlelése, tűzfalak, megfigyelés (32. cikk)
- tájékoztató közzététele minden adatgyűjtésről és adatkezelésről
- az adatvédelmi hatásvizsgálat során azonosított problémák nyomon követése és kezelése (35. cikk)
- adatvédelmi hatásvizsgálat lefolytatása a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas adatvédelmi kockázattal járó adatkezelések esetében (13., 14. és 21. cikk)

De felmerülhet akár **közös adatkezelés** is sok esetben, például, ha egy intézmény fenntartója meghatározza az intézmény számára az adatkezelés valamely eszközét. Erre személyes tapasztalatból tudok egy példát felhozni, amely esetben az önkormányzat megállapodott arról az általa fenntartott óvodákkal, hogy az elektronikus úton benyújtott jelentkezéseket és kérelmeket az általa biztosított iratkezelő rendszerben tárolják és kezelik.

Közös adatkezelésnek minősül az az eset, **ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg**, A közös adatkezelők átlátható módon határozzák meg a GDPR szerinti kötelezettségek teljesítéséért fennálló felelősségük megoszlását. Részletes megállapodás szükséges, ami tisztázza a szerepüket. A megállapodásban az érintettek számára kapcsolattartót lehet kijelölni. Közös adatkezelés esetén az érintett mindegyik adatkezelővel szemben (külön-külön is) gyakorolhatja a GDPR szerinti jogait.

Adatvédelmi szempontból kockázatokat rejthet magában a **fenntartó és a költségvetési szerv között fennálló hatalmi egyensúly eltolódása**, amennyiben a fenntartó visszaél befolyásával. Az irányító szerv jogosult a költségvetési szerv kezelésében lévő közérdekű adatok és közérdekből nyilvános adatok, valamint az irányítási hatáskörök gyakorlásához szükséges, törvényben meghatározott személyes adatok kezelésére.[45] Tehát – ha csak a törvény másként nem rendelkezik – az intézmények vagy más költségvetési szervek tevékenységével összefüggésben kezelt személyes adatok (pl. óvodába járó gyermekek adatai, vagy a polgármesteri hivatal vagy közös önkormányzati hivatal adóügyi osztályán kezelt adatok) megismerésére az alapító nem jogosult, azonban a gyakorlatban könnyen előfordulhatna, hogy a polgármester hatalmi fölényével visszaélve mégis hozzájut ilyen adatokhoz, amivel bűncselekményt is megvalósítana.[46]

Végezetül érdemes áttekinteni a **NAIH eljárási gyakorlatát** abból a szempontból, a hatóság mely **önkormányzati szervvel szemben indított eljárást** az utóbbi években. Ezekből egyértelmű, hogy a legtöbb esetben maga az önkormányzat vagy a polgármesteri hivatal vagy közös önkormányzati hivatal az eljárás alá vont szerv, de találunk példát önkormányzati fenntartású intézménnyel, illetve önkormányzat által létrehozott gazdasági társasággal szembeni döntésre is.[47]

Az egyik esetben 2013-ban a bejelentő azt kifogásolta, hogy valaki **több száz diák személyes adatait** (név, oktatási azonosító, nem, születési hely és idő, anyja neve, apja neve, állampolgárság, lakhely, tanszak, tanár és iskola neve) hozta nyilvánosságra egy fájlmegosztó honlapon keresztül. A NAIH megállapította, hogy a Zeneiskola megsértette az Infotv. 5. § (1) bekezdését, mert nem rendelkezett megfelelő jogalappal az adatok nyilvánosságra hozatalához, valamint az Infotv. 7. § (2)-(3) bekezdéseiben előírt adatbiztonsági követelményeket nem tartotta be. A védendő személyes adatoknak egy olyan helyen történő tárolása, amelyhez

[45] Áht. 9. § j) pont, c)-i) pont

[46] https://nepszava.hu/1154103_vademeles-a-polgarmester-ellen-bukhat-az-ugyved-is (2020.04.23.) Egy szabolcsi polgármester, ügyvéd ismerőse kérésére, arra utasította az önkormányzat ügyintézőjét, hogy - jogosulatlanul - ingyen kérjen le tulajdoni lapokat a nyilvántartásból. A bűncselekmény révén kár is érte az önkormányzatot, mert a jogosulatlan lekérdezések miatt 302 ezer forint bírság megfizetésére kötelezte a polgármesteri hivatalt a Földmérési és Távérzékelési Intézet.

[47] NAIH-1881-5/2013/H és NAIH/2018/356/3/H számú határozatai

gyakorlatilag bárki bármikor hozzáférhet, nyilvánvalóan nem tesz eleget annak a jogalkotói elvárásnak, hogy az adatokat védeni kell az illetéktelen hozzáféréstől. [48]

Más esetben egy **önkormányzat kamerás megfigyelése** során személyes adatokat kezelt, ezzel megsértette az ügyfél információs önrendelkezési jogát. Az önkormányzat egy épületben és a környékén több kamerát helyezett el. Mindez érintette az alkalmazottakat, önkormányzati képviselőket, akik az épület néhány irodáját használták, továbbá az önkormányzati ügyintézésen részt vevő ügyfeleket. A kamerák hang nélkül készítettek videofelvételeket. A felvételek tartalmának megtekintése csak bizonyos esetekben, az arra jogosult személyek által történt. Az önkormányzat az eljárást megelőző időszakban nem rendelkezett kamerás megfigyelésre vonatkozó belső szabályzattal és adatkezelési tájékoztatóval, továbbá nem tájékoztatta előzetesen az érintetteket a kamerás adatkezelésről és annak körülményeiről. Az adatkezelés nem volt jogszerű és átlátható sem. Az eljárást megelőzően nem volt kijelölve az adatkezelésért felelős személy, illetve nem határozták meg, hogy mi az adatkezelés célja és jogalapja. Az önkormányzat nem vette figyelembe az adatkezelés szükségességét és arányosságát, illetve megsértette az adattakarékosság és a célhoz kötöttség elvét is.[49] A NAIH határozata szerint az önkormányzat megsértette a Kérelmező információs önrendelkezési jogát azzal, hogy a rendelet megsértésével kezelték a Kérelmező képmás személyes adatát, továbbá az adatkezelési gyakorlat nem felelt meg az általános adatvédelmi rendelet rendelkezéseinek. A kamerás adatkezelés tekintetében a jogszabályok nem határozzák meg a tájékoztatás formáját, azonban az elszámoltathatóság elvéből, valamint abból kifolyólag, hogy az adatkezelőnek igazolni kell az előzetes tájékoztatás megtörténtét, ennek módja jellemzően az írásbeli forma. A bírság mértéke 5 millió Ft volt.

Véleményem szerint az **adatkezelő személyének szerepe** az önkormányzati szférában elsősorban **az adatvédelemmel kapcsolatos feladatok teljesítésének kötelezettsége miatt igazán fontos,** hiszen egyértelműnek kell lennie, hogy kinek a feladata az adatkezelés jogszerűségének és az érintetti jogok gyakorlásának a biztosítása. Az anyagi felelősség szempontjából az adatkezelő szerepe másodlagos – mindaddig, amíg nem csúszik ki a költségvetési szervek kategóriájából –, hiszen végső soron az önkormányzat költségvetéséből lesz a bírság megfizetetve, amely szerv nem hagyhatja, hogy a közfeladat ellátását veszélyeztesse vagy ellehetetlenítse egy ilyen szankció. Az adott szerv vezetőjének felelősségre vonására ezt követően viszont nagy az esély.

Jelentős eltérés egy önkormányzati adatkezelő esetében, hogy az adatkezelőt megillető döntési jogosultságok a kötelező adatkezelések esetében valójában nem gyakorolhatóak, hiszen ezekben az esetekben az adatkezelés körülményeit magának a jogszabálynak kellene meghatároznia.

Szintén sajátosan alakul az adatkezelői minőség az elmúlt években bevezetett önkormányzati ASP rendszer tekintetében, amelynek lényege, hogy az önkormányzatok által végzett tevékenységekkel összefüggő adatok (amelyek között rengeteg a személyes adat) jelentős

[48] NAIH-1881-5/2013/H számú határozata. Ld. még a https://gdprbirsagok.hu/ honlapot.
[49] NAIH/2019/2076/11 számú határozata. Ld. még a https://gdprbirsagok.hu/ honlapot.

részét központi rendszerben tárolja az állam, ezzel korlátozva az adatkezelő önkormányzat döntési jogosultságát a személyes adatok felett.[50]

Az alábbiakban tekintsük át azokat a **fontosabb intézkedéseket,** amelyeket egy polgármesteri vagy közös önkormányzati hivatal vezetője hajt végre annak biztosítása céljából, hogy a **személyes adatok kezelése GDPR rendelettel összhangban történik:**

a) Adatvédelmi tisztviselő kijelölése,

b) Adatvédelmi hatásvizsgálat elvégzése,

c) Adatvagyon leltár elkészítése,

d) Belső szabályzatok elkészítése,

e) Adatkezelési nyilvántartás vezetése,

f) Érintettek jogai érvényesítéséhez szükséges tájékoztatók elkészítése.

Az információbiztonság és annak technikai feltételek ismertetésétől annak terjedelme miatt most eltekintek.

2.2 Adatvédelmi tisztviselő

A GDPR Preambulumának (97) bekezdése szerint az adatkezelőt vagy az adatfeldolgozót az e rendeletnek való belső megfelelés ellenőrzésében egy, **az adatvédelmi jogot és gyakorlatot szakértői szinten ismerő személy** segíti. A korábbi Infotv. „18. Belső adatvédelmi felelős és adatvédelmi szabályzat" pontjában már tartalmazott az adatvédelmi tisztviselőhöz nagyon hasonló szerepkört adatvédelmi felelős néven, azonban az adatvédelmi szabályzattal ellentétben ez akkor még nem volt kötelező az önkormányzatok számára. **Adatvédelmi tisztviselőt kell kijelölni, ha az adatkezelés közhatalmi vagy egyéb, közfeladatot ellátó szervek végzik**.[51] Ez a kötelezettség nem csak az önkormányzatra vagy a polgármesteri hivatalra, hanem a többi szervre és intézményre is vonatkozik.

A**datvédelmi tisztviselőt három esetben kötelező** kijelölni:[52]
- ha az adatkezelést **közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik**,

- ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé, vagy

- ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

[50] 257/2016. (VIII. 31.) Korm. rendelet az önkormányzati ASP rendszerről
[51] GDPR 37. cikk (1) bek. a) pontja alapján
[52] GDPR 37. cikk (1) bek.

A **29-es Munkacsoport** iránymutatása szerint – amelyet az Európai Adatvédelmi Testület továbbra is fenntart – **mentesülnek** viszont a tisztviselő kijelölésének kötelezettsége alól az olyan, a magánjog hatálya alá tartozó közfeladatot ellátó szervek, mint a **köztulajdonban álló gazdasági társaságok.** Bár esetükben a közfeladatot ellátó szervi minőséget számos jogszabály – köztük az Alaptörvény is – megerősíti, de mégsem kötelesek tisztviselőt alkalmazni, amennyiben a GDPR-ban foglalt egyéb feltételek nem állnak fenn esetükben.[53] A **29-es Munkacsoport** azonban jó gyakorlatként azt tanácsolja, hogy az ilyen szervezetek is jelöljenek ki adatvédelmi tisztviselőt, de esetükben saját maguk dönthetnek erről.[54]

Az **adatvédelmi tisztviselő lehet a szervezet alkalmazottja vagy megbízási (szolgáltatási) szerződés keretében is elláthatja feladatait,** ez a közfeladatot ellátó szervek esetén sincs másként.[55] Az adatvédelmi tisztviselői pozíció betöltésének nincsen olyan jogszabályban rögzített szigorú feltételei, mint például az információbiztonságért felelős személy esetében, a GDPR nem ír elő konkrét végzettséget.[56] Egy jól kiválasztott külső tanácsadó igénybevétele esetén biztosított az adatvédelmi jog és gyakorlat megfelelő ismerete, viszont ez magasabb költségekkel járhat, kevesebb rendelkezésre állás mellett. Egyre több hivatal külső szakértőt bíz meg az adatvédelmi feladatok ellátásával, azonban ez sem jelent mindig garanciát a megfelelőségre, hiszen az adatvédelmi jog ismerete mellett szükség van az önkormányzatok belső eljárásainak mélyreható ismeretére is.

Elvárás a szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, továbbá alkalmasnak kell lennie a szervezetnél meghatározott feladatok elvégzésére.

A **29-es Munkacsoport** és a szakirodalom is részletesen foglalkozott már ezeknek a követelményeknek az kibontásával. A közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv esetében az adatvédelmi tisztviselőnek alaposan kell ismernie a szervezet igazgatási szabályait és eljárásait.[57] Ez logikus elvárás a potenciális tisztviselővel szemben, hiszen a közigazgatási szervek működése nagyon eltérő a magánszférában tapasztalhatótól, nem véletlen, hogy az önkormányzati köztisztviselőknek törvény írja elő a közigazgatási szakvizsga abszolválását.[58] Ez nem azt jelenti, hogy az adatvédelmi tisztviselőnek is feltétlenül ilyen szakvizsgával kell rendelkeznie, de mindenképp szükséges, hogy az adatvédelmi jogi ismeretek mellett tisztában legyen az adott szerv feladatellátását meghatározó jogszabályi előírásokkal.

A NAIH által vezetett **adatvédelmi tisztviselők nyilvántartásában** elérhető adatok alapján az látható, hogy több önkormányzati szerv döntött külső adatvédelmi tisztviselő megbízása mellett.

A szervezet saját munkavállalójának kijelölése esetén kérdéses lehet a függetlenség biztosítása abban az esetben, ha a kijelölt személy korábbi munkaköre továbbra is fennmarad, hiszen a közigazgatási szervekben erősebb hierarchia jellemző, mint a versenyszférában. A GDPR viszont előírja, hogy az adatkezelő és az adatfeldolgozó biztosítsa, hogy az adatvédelmi

[53] Péterfalvi – Révész – Buzás*:* i.m. 247-248. oldal
[54] WP243 7. oldal
[55] GDPR 37. cikk (6) bek.
[56] 26/2013. (X. 21.) KIM rendelet
[57] WP243 14. oldal
[58] 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről (Kttv.)118. § (1) bek.

tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Továbbá az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja.[59] A saját dolgozó kijelölése mellett szólhat hosszú távon, miszerint jobban érvényesülhet a **29-es Munkacsoport** által megfogalmazott „**elérhetőség követelménye**", vagyis az adatvédelmi tisztviselő sokkal közvetlenebb módon tud kapcsolatot tartani és felvilágosítást adni mind az érintettek, mind a kollégák, mind a felügyeleti hatóság számára.[60]

Az **adatkezelő vagy az adatfeldolgozó kulcsfontosságú szerepe van** az adatvédelmi tisztviselő hatékony feladatellátásában. Az adatvédelmi tisztviselők részére **elegendő önállóságot és forrást kell biztosítani** a feladataik hatékony végrehajtásához. Az adatvédelmi tisztviselőket nem terheli személyes felelősség a GDPR be nem tartásáért. A GDPR egyértelművé teszi, hogy az adatkezelőnek vagy az adatfeldolgozónak kell biztosítani és bizonyítani, hogy az adatkezelés a GDPR rendelkezéseivel összhangban történik[61]. Az adatvédelmi rendelkezések betartásáért az adatkezelő vagy az adatfeldolgozó felelős.[62]

A GDPR[63] alapján ha az adatkezelő vagy az adatfeldolgozó közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv, **közös adatvédelmi tisztviselő** jelölhető ki több ilyen szerv számára, az adott szervek szervezeti felépítésének és méretének figyelembevételével. Tekintettel arra, hogy az adatvédelmi tisztviselő számos feladatot lát el, az adatkezelőnek vagy az adatfeldolgozónak ilyen esetben is gondoskodnia kell arról, hogy a közös adatvédelmi tisztviselő hatékonyan elvégezhesse ezeket a feladatokat, annak ellenére, hogy több közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv számára jelölték ki.[64] A NAIH kifejezetten támogatta a **közös tisztviselő kijelölésének lehetőségét a helyi önkormányzatok esetében**.[65]

A gyakorlatban kétféle módon valósulhat meg a **közös adatvédelmi tisztviselő kijelölése**. Általában egy vagy több önkormányzaton belül az összes hivatal és más szervek, intézmények esetén egy közös adatvédelmi tisztviselő megbízása vagy több, különálló adatvédelmi tisztviselő önkormányzatonként. Míg előbbi bevett megoldás idehaza, különösen a kisebb önkormányzatok esetében, addig az utóbbira hivatalos formában nem került sor, csak külső megbízottak útján, ami viszont a költségek megtöbbszörözését jelenti, hiszen minden önkormányzat külön szerződést köt és fizet díjat a külső tanácsadó számára.

Amikor 2018 végén egy országos érdekképviseleti szervet, a Települési Önkormányzatok Országos Szövetségét (TÖOSZ) képviselve Prágában egy kifejezetten az önkormányzatoknak szóló nemzetközi GDPR konferencián jártam, akkor több előadó is arról számolt be, hogy egy állam (pl. Csehországban, Franciaországban) olyan rendszer kialakításán munkálkodott, amelynek keretében a kisebb önkormányzatok számára a közigazgatás valamely felsőbb szintjén segítséget nyújtottak volna a GDPR-ban foglalt kötelezettségek teljesítéséhez. Így például közös adatvédelmi tisztviselőt vagy tisztviselők csoportját bocsátották volna

[59] GDPR 38. cikk (3) bek.
[60] Péterfalvi – Révész – Buzás: i.m. 252. oldal
[61] GDPR 24. cikk (1) bek.
[62] WP 243 5. oldal
[63] GDPR 37. cikk (3) bek.
[64] WP 243 19. oldal
[65] NAIH/2017/5364/2/V állásfoglalás

rendelkezésre a települések számára, ezzel biztosítva a megfelelő szakmai tudás meglétét. A költségek fedezetét az állam biztosította volna azon települések számára, akiknek ez jobban megterhelte volna a költségvetését.

Közismert tény, hogy Magyarország településszerkezete elaprózódott, a települések több mint a felének a lakosságszáma nem éri el az ezer főt. Az 1990-ben elfogadott önkormányzati törvény valamennyi önálló település számára biztosította a helyi önkormányzás jogát, amely az adott politikai helyzetben óriási jelentőséggel bírt. Azzal azonban feltétlenül számolni kellett, hogy az alacsony lélekszámú települések önállóan nem képesek a közszolgáltatások széles körének biztosítására. A hasonló adottságú országokban ezért a hatékony, gazdaságos feladatellátás érdekében élnek a differenciált hatáskör telepítés lehetőségével, alapjellemző a szintek közötti munkamegosztás, valamint széles tere van a helyi önkormányzatok együttműködésének, a társulásoknak. [66]

A települési önkormányzatok száma jelenleg több mint háromezer, amelyek közül számosan önálló költségvetési szerveket, intézményeket tartanak fenn. Az adatvédelmi tisztviselő alkalmazása ugyanúgy kötelező a kisebb települési önkormányzatok számára, mint például egy megyei jogú városnak, az anyagi lehetőségek és a rendelkezésre álló humánerőforrás terén azonban óriási különbségek vannak, ráadásul bizonyosan nincs is ennyi adatvédelmi szakértő az országban, ezért megfontolásra javaslom a kisebb települések esetén az állami segítséget az adatvédelmi feladatok szakszerű és hatékony ellátásához. Valószínűsíthető, hogy több önkormányzatnál mind a mai napig nincs adatvédelmi tisztviselő.

A GDPR 4. szakasza szerint az adatvédelmi tisztviselőt **ténylegesen el kell tudni érni**. A **szükséges szakértelem** szintje nincs szigorúan meghatározva, arányosnak kell azonban lennie a szervezet által kezelt adatok érzékenységével, összetettségével és mennyiségével. Ha például az adatkezelési tevékenység különösen bonyolult, vagy nagy mennyiségű érzékeny adatot érint, az adatvédelmi tisztviselőnek adott esetben magasabb szintű szakértelemmel és támogatással kell rendelkezni. Az adatvédelmi tisztviselőknek **szakértelemmel kell rendelkezni a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén**, valamint alaposan ismernie kell a GDPR-t. Közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv esetében az adatvédelmi tisztviselőnek alaposan kell **ismerni a szervezet igazgatási szabályait és eljárásait.** A személyes tulajdonságai közé tartozik például az integritás és a magas szintű szakmai morál, az adatvédelmi tisztviselő elsődleges feladata a GDPR-nak való megfelelés lehetővé tétele. Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában.[67]

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban **titoktartási kötelezettség** vagy az **adatok bizalmas kezelésére vonatkozó kötelezettség** köti.[68] A titoktartási, illetve

[66] Szerk. dr. Bekényi József – dr. Barabás Zoltán: Önkormányzatokról önkormányzatoknak, Budapest, Belügyminisztérium kiadványa – többszerzős – (2019) 36. oldal. https://2015-2019.kormany.hu/download/b/4d/b1000/%C3%96nkorm%C3%A1nyzati%20k%C3%B6nyv%20-%20Online.pdf#!DocumentBrowse

[67] WP 243 14. oldal

[68] GDPR 38. cikk (5) bek.

bizalmas kezelésre vonatkozó kötelezettség azonban nem tiltja, hogy szükség esetén a felügyeleti hatósághoz forduljon és kikérje tanácsát.

A GDPR előírja, hogy az **adatkezelőnek közzé kell tennie az adatvédelmi tisztviselő nevét** és elérhetőségét, és azokat a felügyeleti hatósággal is közölnie kell.[69] E követelmények célja annak biztosítása, hogy az érintettek, a felügyeleti hatóságok közvetlenül tudjanak hozzá fordulni. Emellett az adatvédelmi tisztviselővel minél előbb konzultálni kell, ha adatvédelmi vagy más incidens következett be.

Az alábbi táblázat az adatvédelmi tisztviselő fontosabb feladatait, valamint a feladat ellátáshoz szükséges kompetenciákat, képességeket mutatja be:

ADATVÉDELMI TISZTVISELŐ	
Adatvédelmi tisztviselő feladatai	**Kompetenciái, szükséges képességek**
- működteti a Hivatalon belüli adatvédelmi folyamatokat	- ismeri az adatvédelmi tisztviselő feladatait, szerepét a Hivatalnál
- közreműködik a Hivatal adatvédelmi belső szabályzatai elkészítésében, az adatkezelési nyilvántartás kialakításában	- ismeri a GDPR előírásait, az Info tv. és az ágazati jogszabályok adatvédelemmel kapcsolatos előírásait és azokat a gyakorlatban is tudja alkalmazni
- tanácsot ad Adatkezelőnek a jogszerű adatkezelés biztosítása érdekében	- képes értelmezni a hatósági eljárásokat, döntéseket, állásfoglalásokat
- segíti a szervezet adatvédelmi, adatbiztonsági munkáját, ellenőrzi a GDPR-nek, az adatvédelmi jogszabályoknak és a Hivatal belső szabályainak való megfelelést	- ismeri az adatvédelemhez és az információszabadsághoz kapcsolódó eljárásokat, jogszabályokat, továbbá az intézmények feladatkörét, hatáskörét, illetékességét és a joghatóságukat;
- figyelemmel kíséri az adatkezelési és adatfeldolgozási tevékenységet	- képes azonosítani az adatkezelés kockázatait, ismeri a kockázatkezelés módját
- segíti a Hivatal munkáját az érintettektől érkező beadványok elbírálásakor, adatvédelmi incidens bekövetkezése esetén tanácsot ad a Hivatal számára a megfelelő intézkedések meghozatala érdekében	- ismeri az adatvédelem területén az érintett jogokat, az adatkezelői és az adatfeldolgozói kötelezettségeket, el tudja határolni egymástól az adatkezelőt és az adatfeldolgozót

[69] GDPR 37. cikk (7) bek.

Adatvédelmi tisztviselő feladatai	Kompetenciái, szükséges képességek
- beazonosítja az adatvédelmi incidenseket, közreműködik a jogszabályban meghatározott bejelentési eljárásban	- képes megállapítani az egyes adatkezelési műveleteket, adatvédelmi szempontból képes rendszerezni az egyes személyes adatokat, elkötelezett a személyes adatok védelme iránt
- ellátja a jogszabályban vagy belső szabályzatban előírt adatszolgáltatási feladatokat	- megfelelő adatvédelmi jogi ismeretekkel rendelkezik, illetve képes az adatvédelmi hatósággal vagy a bíróságokkal történő kapcsolattartásra
- titoktartási kötelezettsége van, továbbá az adatok bizalmas kezelésére vonatkozó kötelezettsége	- képes rangsorolni a tevékenységeket, és a magasabb adatvédelmi kockázatot jelentő ügyekre összpontosítani
- kapcsolatot tart a jegyzővel, a felügyeleti hatósággal	- nyitott olyan szakmai és módszertani újítások iránt, amelyek hatékonyabbá teszik a feladatellátást, magas szintű szakmai morállal bír
- szükség esetén adatvédelmi hatáselemzést végez vagy szakmai tanácsot ad	- jó problémamegoldó képességgel bír, együttműködő, bizalmasan kezeli a szervezettel kapcsolatban a tudomására jutott információkat
- szakmai tanácsot és tájékoztatást ad az adatvédelem témakörében az érintett munkavállalóknak, a felmerült kérdéseket megválaszolja, figyelemmel kíséri az adatkezeléssel kapcsolatos jogszabályi változásokat.	- képes közreműködni a munkavállalók adatvédelmi-tudatossági képzésében, kompetenciáik fejlesztésében, oktatást tart.

2. számú ábra: Az adatvédelmi tisztviselő, feladatai, kompetenciái[70]

A NAIH honlapján nyilvánosságra hozza a **bejelentett tisztviselők listáját** az adatkezelő feltüntetése mellett. Ez alkalmas lehet annak vizsgálatára, vajon milyen arányban tettek eleget az önkormányzatok a kötelezettségüknek, és alkalmazták-e a közös adatvédelmi tisztviselő kijelölésére lehetőséget adó szabályt az önkormányzati szervek és intézmények esetében.

[70] Az ábra saját szerkesztésű.

Összefoglalásként elmondható, hogy nem lehetett maradéktalanul eleget tenni a GDPR adatvédelmi tisztviselőre vonatkozó előírásának a közszférában 2018. május 25-ig, mert a közfeladatot ellátó szerveknél nem állt rendelkezésre elegendő számú adatvédelemben és közigazgatásban is megfelelően járatos személy, amely főleg a kisebb önkormányzatok számára okozhat problémát, ahol a kis létszámú hivatalokban nem jut kapacitás az adatvédelmi feladatok ellátását saját munkavállalóval megoldani. A legtöbb esetben a fő cél az lehetett, hogy az adatkezelők teljesítsék az adatvédelmi tisztviselő alkalmazására vonatkozó kötelezettséget és háttérbe szorult a megfelelő szaktudás követelménye. Megoldást jelenthet a külső szolgáltató igénybevétele, de a kapacitásuk nekik is véges.

Az adatvédelmi képzésekre hatalmas igény keletkezett a GDPR hatálybalépését követően.[71] Számos **adatvédelmi tisztviselői (DPO) képzést** indítanak erre szakosodott cégek, amelyeken a GDPR rendelet, az Info tv., továbbá ágazati jogszabályok bemutatásán túl olyan átfogó ismeret birtokába lehet jutni, amely szükséges az adatvédelmi tisztviselő feladatai ellátásához. Egyetemen, általában három féléves képzési idővel adatbiztonsági és adatvédelmi jogi szakokleveles szakember vagy európai uniós adatvédelmi szaktanácsadó szakképesítés vagy adatvédelmi szakjogász végzettség is szerezhető.

Végezetül röviden összehasonlítom az **információbiztonságért felelős személy** és az **adatvédelmi tisztviselői pozícióját**, abból a szempontból, vajon betöltheti-e ugyanaz a személy mindkettőt.

Az Ibtv. előírja a képviselő-testület hivatalának vezetője (jegyző) számára, hogy az **elektronikus információs rendszer biztonságáért felelős személyt** (továbbiakban: **IBF)** nevezzenek ki vagy bízzanak meg, tehát alkalmazásuk valamennyi polgármesteri hivatalban (közös önkormányzati hivatalban) szükséges. Az IBF feladata – nagyon leegyszerűsítve – a szervezet által kezelt adatok (közöttük személyes adatok) megvédése. Ez alapján magától értetődik, hogy miért gondolták sok helyen, hogy az IBF-et nevezik ki egyben adatvédelmi tisztviselőnek is, azonban alapvető különbségek fedezhetőek a két személy között.

Az első szempont, amit vizsgálni kell, az a feladatkör betöltésére való **alkalmassági követelmények.** Láthattuk, hogy az **adatvédelmi tisztviselő** számára konkrét végzettségre vonatkozó követelményt nem határoz meg a GDPR, hanem a szakmai rátermettséget, az adatvédelmi jog és gyakorlat szakértői szintű ismeretét, valamint a meghatározott feladatok ellátására való alkalmasságot írja elő számára. Ezzel szemben az **IBF-ek számára** a ***26/2013. (X. 21.) KIM rendelet*** [72] konkrét végzettség vagy bizonyos szakmai szervezetek által kiadott oklevél megszerzését írja elő, bár amolyan „joker megoldásként" a jogszabály lehetővé teszi, hogy öt év releváns szakmai tapasztalattal ki lehessen váltani ezt a követelményt. Maga a jogszabály rendelkezik az IBF képzés részleteiről, amelyet hivatalosan csak a Nemzeti Közszolgálati Egyetemen lehet elvégezni. A képzés két féléves, szakirányú továbbképzés,

[71] Kálmán Attila: A GDPR felértékeli az adatvédelmi szaktudást https://jogaszvilag.hu/a-gdpr-felertekeli-az-adatvedelmi-szaktudast/ (2020.04.28.)

[72] 26/2013. (X. 21.) KIM rendelet - az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

amelynek elvégzését követően elektronikus információbiztonsági vezető megnevezésű képesítés szerezhető. A képzésre az a személy vehető fel, aki felsőfokú végzettséggel és angol nyelvből legalább alapfokú komplex nyelvvizsgával vagy ezzel egyenértékű bizonyítvánnyal, oklevéllel rendelkezik, valamint a képzés megkezdéséhez szükséges feltételeket teljesítette.

Az IBF képzés tematikájában az adatvédelmi jog és gyakorlat nem szerepel, legfeljebb érintőlegesen, tehát önmagában a végzettség megszerzése nem elégíti ki a GDPR-ben foglalt elvárásokat, de természetesen ez nem jelenti azt, hogy egy IBF ne szerezhetné meg ezt a tudást más módon (pl. más képzés elvégzésével, korábbi szakmai tapasztalattal).[73]

Ha az adatvédelmi tisztviselő számára meghatározott feladatokat vesszük sorba, akkor az tűnik ki, hogy az a)-b) pontban foglalt feladatok (tanácsadás, jogszabályi kötelezettségeknek való megfelelés ellenőrzése) valóban indokolják az adatvédelmi jogban való jártasságot, ezért inkább egy jogi ismeretekkel rendelkező személy lehet ideális ebből a szempontból a feladat elvégzésére.

Az adatvédelmi hatásvizsgálattal kapcsolatban fontos megjegyezni, hogy bár annak gerincét egy kockázatelemzés képezi, amely feladat az IBF-ek számára is ismert, de nagyon nagy különbség, hogy míg egy információbiztonsági kockázatelemzés során magára a szervezetre vonatkozó kockázatokat kell mérlegelni, addig az adatvédelmi hatásvizsgálat során az érintettek jogaira és szabadságaira jelentett veszély van a középpontban és ezért teljesen más gondolkodásmódot igényel.

A többi feladat (kapcsolattartás a hatósággal, érintettekkel) véleményem szerint nem igényel olyan speciális képzettséget, amely kizáró okot jelentene bármely köztisztviselő számára, az Ibtv. pedig szintén előír hasonló feladatot az IBF számára. Mindezek fényében úgy gondolom, hogy egy információbiztonságért felelős személyt végzettsége és ezen a területen szerezett szakmai tapasztalata önmagában nem tesz alkalmassá az adatvédelmi tisztviselői pozíció betöltésére, de nincs akadálya annak, hogy az elvárt ismereteket más módon megszerezze.

A második szempont az **összeférhetetlenség kérdése**. A tisztviselő más feladatokat is elláthat, azonban biztosítani kell, hogy ezekből ne fakadjon összeférhetetlenség.[74] Ez a 29-es Munkacsoport iránymutatásai szerint különösen azt jelenti, hogy az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit. Bár az adatvédelmi tisztviselőknek lehetnek más feladataik, csak olyan egyéb feladatokkal bízhatók meg, amelyek nem okoznak összeférhetetlenséget. Összeférhetetlenséget okozó szervezeten belüli pozíciók lehetnek a felsővezetői pozíciók (jegyző, pénzügyi, humán erőforrás vagy informatikai osztályvezető), de más, a szervezeti struktúrában alacsonyabb szinten lévő pozíciók is, ha ezek a pozíciók az adatkezelés céljainak és eszközeinek meghatározásával járnak.[75]

[73] https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok (2020.04.30.)
[74] GDPR 38. cikk (6) bek.
[75] WP 243 19. oldal

A szervezet tevékenységeitől, méretétől és szerkezetétől függően jó gyakorlat lehet az adatkezelők vagy az adatfeldolgozók számára:
- azon pozíciók meghatározása, amelyek összeegyeztethetetlenek az adatvédelmi tisztviselő tevékenységével,
- belső szabályok megállapítása az összeférhetetlenség elkerülése érdekében,
- általánosabb magyarázat nyújtása az összeférhetetlenségről,
- e követelmény tudatosításának módjaként nyilatkozat arról, hogy az adatvédelmi tisztviselő nem összeférhetetlen az adatvédelmi tisztviselőként végzett feladatai tekintetében,
- a szervezet belső szabályaiban biztosítékok szerepeltetése, és annak biztosítása, hogy az adatvédelmi tisztviselői pozíció betöltésére vagy szolgáltatási szerződés megkötésére vonatkozó felhívás kellően pontos és részletes az összeférhetetlenség elkerülése érdekében.[76]

Az **információbiztonság** szükségképpen magába foglalja a személyes adatok védelmét (jogosulatlan hozzáférés megakadályozása, adatok tárolásának módja és eszközei stb.), de gyakran maguk a védelmi intézkedések is személyes adatok kezelésével járnak együtt (pl. beléptető rendszer vagy kamerás megfigyelés alkalmazása, esetleg a munkavállalók online tevékenységének nyomon követése) és **ezek tervezéséért, koordinálásáért az IBF felel**.[77]

Az IBF nyomon követi a jogszabályi követelményeket, kockázatelemzéseket végez és ezek alapján ajánlásokat fogalmaz meg a szervezet vezetője számára. Ezek a javaslatok adott esetben meghatározhatják adatkezelések céljait és eszközeit, de fontos hangsúlyozni, hogy a jogszabály szerint az IBF csak tanácsot ad, véleményez, tervez, de a konkrét döntést egy eljárás bevezetéséről, egy új eszköz alkalmazásáról a szervezet vezetője (pl. jegyző, intézményvezető) hozza meg.

Tehát az IBF maga nem határozza meg a szó jogi értelmében egy adatkezelés célját és eszközeit, hanem közreműködik a döntés előkészítésében. De véleményem szerint nincs akadálya annak, hogy bizonyos döntési jogköröket akár önálló hatáskörébe utaljon a jegyző vagy az adott intézmény vezetője, ami viszont egyértelmű összeférhetetlenséget eredményezne.

Ha egyértelműen nem is jelenthető ki az összeférhetetlenség a két feladatkör között, én magam több érvet is látok **a két pozíció külön személyek általi betöltése mellett**. Bár az információbiztonság és az adatvédelem megvalósítása egy jelentős területen, az adatbiztonság esetében metszi egymást, azonban nem szabad elfeledkezni, hogy amíg az információbiztonság elsődleges célja a szervezet érdekeinek, javainak megóvása, addig az adatvédelemnek az érintettek jogainak és szabadságainak a védelme.

A két terület pedig bizonyos esetekben egymással szemben is állhat olyan esetekben, amikor az információbiztonság megvalósítása miatt az érintettek számára nagyobb kockázatot jelentő adatkezelésekre kerül sor (pl. munkavállalók, látogatók ellenőrzése). Ilyen esetekben, ha ugyanaz a személy tölti be az IBF és az adatvédelmi tisztviselő pozícióját kérdés, hogy melyik irányba fog eltolódni nála a mérleg nyelve. Bár a megfelelő ismeretek birtokában lehetséges a

[76] WP 243 19. oldal
[77] Ibtv. 13. §

jogszerű, de mégis hatékony intézkedések megtalálása, de két külön személy közötti konstruktív szakmai vita erre nagyobb garanciát jelenthet.

Ráadásul, ha két személy tölti be a két munkakört, az azt jelenti, **hogy kétszeresen érvényesül a kontroll az adatbiztonság területén**, amely mind az adatkezelő szervezet, mind az érintettek számára kedvező.

Időközben a NAIH is foglalkozott a kérdéssel egyik állásfoglalásában, és egyértelműen kimondta, hogy a két pozíció között összeférhetetlenség áll fenn.[78]

2.3 Adatvédelmi hatásvizsgálat elkészítése

Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelyet **az adatkezelő folytat le** egy új, még meg nem kezdett – tulajdonképpen még tervezési szakaszban lévő – **adatkezelés megkezdése előtt.** Célja, hogy az adatkezelő még az új adatkezelés megkezdése előtt felmérje azt, hogy az meg fog-e felelni az adatvédelmi jog előírásainak.[79]

Az adatkezelőnek, amennyiben az adatkezelése **valószínűsíthetően magas kockázattal jár,** a természetes személyek jogaira és szabadságaira nézve, az adatkezelést megelőzően szükséges **elvégeznie adatvédelmi hatásvizsgálatot**.

A NAIH a honlapján közzétette a GDPR szerinti azon adatkezelési műveletek típusainak a jegyzékét, amelyekre nézve az adatkezelőnek kötelező hatásvizsgálatot lefolytatnia. A közzétett listában szereplő adatkezelési műveleteken túl az adatkezelőknek általános kötelezettsége az általa folytatott adatkezelések vonatkozásában az adatvédelmi kockázatok felmérése és a megfelelő kockázatkezelés. A listán szereplő adatkezelések nem jelentik azt, hogy csak ezekben az esetekben kell az adatkezelőnek hatásvizsgálatot lefolytatnia. Ha az adatkezelés a GDPR 35. cikkének (1), illetve (3) bekezdésében található feltételeknek megfelel, úgy köteles az adatkezelő hatásvizsgálatot lefolytatni. [80]

A GDPR 35. cikk (1) bekezdése alapján **az adatvédelmi hatásvizsgálatot akkor kell elvégezni**, amikor az **adatkezelés „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve”**. Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával. Az adatvédelmi hatásvizsgálat eredményéről előzetesen konzultálni kell a felügyeleti hatósággal, ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő

[78] NAIH 2020/7539/2. számú állásfoglalása

[79] Eszteri Dániel: Az adatvédelmi hatásvizsgálat és az előzetes konzultáció (Nemzeti Közszolgálati Egyetem) 2019.
A kiadvány letölthető: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/14671/Az%20adatvedelmi%20hatasvizsgalat%20es%20az%20elozetes%20konzultacio.pdf?sequence=3&isAllowed=y

[80] Ld.a https://www.naih.hu/hatasvizsgalati-lista honlapot.

intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére, azaz a fennmaradó kockázatok továbbra is jelentősek.[81]

Az **elfogadhatatlanul magas fennmaradó kockázatra** példa, ha az érintettek olyan jelentős vagy akár visszafordíthatatlan következményekkel szembesülnek, amelyeket nem tudnak leküzdeni (például adatokhoz való jogosulatlan hozzáférés, amely az érintettek életét fenyegető veszélyt, elbocsátást vagy pénzügyi nehézséget eredményez). A NAIH – mint az Alaptörvény VI. cikk (4) bekezdése és az Infotv. 38. § (2a) bekezdése szerint az általános adatvédelmi rendelet szerinti felügyeleti hatóság – ebből következően az adatvédelmi hatásvizsgálatra vonatkozó előzetes konzultációt elvégzi[82]

A NAIH az előzetes konzultáció keretében a szervezet által már lefolytatott hatásvizsgálat dokumentációjából azt állapítja meg, hogy az adatvédelmi hatásvizsgálat lefolytatása a GDPR vonatkozó rendelkezései, illetve a hatásvizsgálati iránymutatás előírásai szerint történt-e. Továbbá azt vizsgálja, hogy a fennmaradó kockázatok mérséklésében tud-e segítséget nyújtani.[83]

Az adatvédelmi **hatásvizsgálat alapvetően két nagy részből áll.** Egyrészről az adatkezelő értékeli **az adatvédelmi alapelveknek történő megfelelést**, kvázi egy jogi megfelelőségi elemzést végez. Másrészről azonban az adatkezelőnek értékelnie kell az adatbiztonsági intézkedéseket, azaz egy **kockázatelemzést is el kell végeznie**. Az adatvédelmi hatásvizsgálatban kiemelten az adatbiztonsági intézkedések nyújtanak a legnagyobb mozgásteret a kockázatok csökkentésére. Ennek megfelelően a NAIH a magasabb szintű megfelelőség érdekében olyan módszertan kiválasztását javasolja, amelyet az adott adatvédelmi hatóság már összhangba hozott a GDPR rendelkezéseivel.

Ilyen például a francia adatvédelmi hatóság (CNIL) által a saját honlapján is közzétett módszertan, amely alkalmazását tovább erősíti az a tény, hogy a CNIL közzétett egy **nyílt forráskódú szoftvert is,** amellyel az adatkezelők könnyen elkészíthetik a módszertannak megfelelő adatvédelmi hatásvizsgálatot. A CNIL szoftvert főleg olyan adatkezelőknek fejlesztették ki, amelyek némileg jártasak a hatásvizsgálat elvégzésében. Az adatkezelők könnyen le tudják tölteni és elindítani a számítógépre az önálló verziót. A szoftvert egy szervezet a szerverére is telepítheti, hogy más eszközökkel és rendszerekkel integrálva együtt tudja használni a cégen belül. A fenti szoftver magyar nyelvű verzióval is rendelkezik és elérhető a NAIH honlapjáról.[84]

Ezt az eszközt az adatkezelőknek, főképpen azon adatkezelőknek címezték, akik az adatvédelmi hatásvizsgálat folyamatát illetően alapszintű ismeretekkel rendelkeznek. A szoftver önállóan futtatható verziója letölthető és könnyen elindítható a felhasználó számítógépén. Emellett a szoftver használata oly módon is lehetséges, hogy azt a szervezet saját szerverére telepítik annak érdekében, hogy a már meglévő egyéb eszközök és rendszerek közé integrálják.[85]

[81] Ld. https://www.naih.hu/az-adatvedelmi-hatasvizsgalat-es-elozetes-konzultacioja honlapot.
[82] Ld. https://www.naih.hu/az-adatvedelmi-hatasvizsgalat-es-elozetes-konzultacioja honlapot.
[83] Ld. https://www.naih.hu/az-adatvedelmi-hatasvizsgalat-es-elozetes-konzultacioja honlapot.
[84] Ld. a https://www.naih.hu/az-adatvedelmi-hatasvizsgalat-es-elozetes-konzultacioja honlapot.
[85] Ld. a https://www.naih.hu/hatasvizsgalati-szoftver honlapot.

Amennyiben az előzetes konzultáció során a NAIH véleménye szerint a tervezett adatkezelés megsértené a GDPR-t, különösen, ha az adatkezelő a kockázatot nem elégséges módon azonosította vagy csökkentette, úgy gyakorolhatja a GDPR 58. cikkében említett hatásköreit, így többek között az adatkezelést megtilthatja.[86]

A GDPR 35. cikk (1), illetve (3) bekezdésében írt kötelező eseteken túl – figyelembe véve a GDPR 35. cikk (10) bekezdésében írt kivételeket – **az adatkezelő az alábbi adatkezelési műveletek esetében köteles,** többek között **adatvédelmi hatásvizsgálatot lefolytatni**. [87] A felsorolás nem teljes körű.

a) Ha egy természetes személy **biometrikus adatainak** kezelése módszeres megfigyelésre irányul. A GDPR alapján biometrikus adatnak minősül egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat (4. cikk, 14. pont). A biometrikus adatok kapcsán fontos kiemelni, hogy ezek az adatok különleges kategóriájába (különleges adat) tartoznak, így kezelésük kapcsán a különleges adatok kezelésére vonatkozó szabályoknak is eleget kell tenni. [88]

b) Ha **kiszolgáltatott helyzetben lévő érintettekkel** – különös tekintettel a gyermekekre, munkavállalókra, idős, mentális betegségben szenvedőkre – kapcsolatos biometrikus adat kezelése történik (pl. szociális vagy egészségügyi intézményben).

c) Ha az adatkezelés egy természetes személy genetikai adatainak egyéb különleges adatokhoz vagy fokozottan személyes jellegű adatokhoz történő **hozzákapcsolásával** jár.

d) Ha egy természetes személy genetikai adatai kezelésének célja a természetes személy **értékelése vagy pontozása** abból a célból, hogy az érintett bizonyos tulajdonságait felmérje, és annak eredménye kihatással van az érintett részére nyújtott, illetve nyújtandó szolgáltatás létrejöttére vagy minőségére.

e) **Fizetőképesség értékelése** a személyes adatok nagy számú, illetve módszeres értékelése útján.

f) **Harmadik személytől gyűjtött adatok további felhasználása** az érintettre vonatkozó szolgáltatás visszautasítására vagy megszüntetésére vonatkozó döntés meghozatalánál.

g) **Diákok, hallgatók személyes adatainak értékelésre való felhasználása.** Az adatkezelés célja a diákok, hallgatók felkészültségének, teljesítményének, alkalmasságának, illetve mentális állapotának rögzítése, valamint vizsgálata és az adatkezelés nem jogszabályon alapul, függetlenül attól, hogy az oktatás alap-, közép- vagy felsőfokú.

h) **Profilozás.** Az adatkezelés célja személyes adatok nagy számú, illetve módszeres értékelése révén végzett profilozás, különösen, ha az az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körére,

[86] GDPR 36. cikk (2) bekezdés.

[87] Ld. a https://www.naih.hu/hatasvizsgalati-lista honlapot.

[88] Ld. https://gdpr.blog.hu/2020/07/10/biometrikus_azonositassal_kapcsolatos_felreertesek honlapon. Biometrikus azonosítással kapcsolatos félreértések című cikke.

megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján történik.

i) Az adatkezelés célja közműszolgáltatók által telepített **„okosmérők”** alkalmazása (fogyasztási szokások nyomon követése).

j) Joghatással vagy hasonló jelentős hatással járó **automatizált döntéshozatal**. Az adatkezelés célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala, amely adatkezelés adott esetben egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti.

k) **Érintettek nagyszámú és módszeres megfigyelése** jellemzően közterületeken vagy nyilvános helyeken történő kamerarendszerek, drónok felhasználásával, illetve bármely más új technológia használatával (Wi-Fi tracking, Bluetooth tracking, testkamera).

l) **Helymeghatározási adatok kezelése**, ha az módszeres megfigyelésre vagy profilalkotásra utal.

m) **Munkavállaló munkájának megfigyelése** során a munkavállaló személyes adatainak nagy számú és módszeres feldolgozása, illetve értékelése (pld. GPS megfigyelő autóban történő elhelyezése, kamerás megfigyelés lopás vagy csalás elleni fellépés céljából).

n) **Különleges adatok nagy számban való kezelése**. A GDPR (91) preambulumbekezdése alapján a személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik.

o) Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, **nagy számban kezelt adatok eredeti céltól eltérő kezelése:** pl. gyermekek, idősek, mentális betegségben szenvedők esetében.

p) **Gyermekek személyes adatainak kezelése** profilozás, automatikus döntéshozatal, vagy marketing céljából, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása vonatkozásában.

r) **Új technológiai megoldások használata az adatkezelés során,** ideértve az érzékelővel ellátott eszközök által előállított adatok interneten vagy más csatornán keresztül történő nagyszámú kezelését (pl. okos eszközök) és amelyek adatokat szolgáltatnak a természetes személy fizetőképességére, egészségére, személyes érdeklődési körére, megbízhatóságára vagy viselkedésére, tartózkodási helyére és amelyek alapján profilalkotás történik.

s) **Egészségügyi adatokra vonatkozó adatkezelések**. Nagy számban kezelt adatok tekintetében a kórházak, egészségügyi ellátó intézmények, magán-egészségügyi szolgáltatók által kezelt különleges adatok vonatkozásában, ideértve a nagyobb sportlétesítmények, edzőtermek által a tagoktól felvett egészségügyi adatok kezelését is.

t) Amikor **több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni,** amelyben különleges adatokat is kezelnek.

u) Az adatkezelés célja a **különböző forrásokból származó adatok összevonása**, egymással való megfeleltetése vagy összehasonlítása.

Az adatvédelmi **hatásvizsgálat eredményéről előzetesen konzultálni kell a felügyeleti hatósággal,** ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére, azaz a fennmaradó kockázatok továbbra is jelentősek.

Az adatkezelőknek **folyamatosan értékelniük kell az adatkezelési tevékenységeiből eredő kockázatokat,** hogy felismerjék, ha az adatkezelés valamely fajtája „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve". Az adatvédelmi hatásvizsgálat egy folyamat, különösen akkor, ha az adatkezelési művelet dinamikus és állandóan változik. Az **adatvédelmi hatásvizsgálatot** nem egyetlen alkalommal, hanem **folyamatosan kell végezni**.[89]

2.4 Adatvagyon leltár

A polgármesteri hivatalok (közös önkormányzati hivatalok) számos feladatot látnak el és többféle olyan közszolgáltatást nyújtanak a településen élő lakosok számára, amelyek ellátása során információkat gyűjtenek és állítanak elő. Az adattömeg jelentős része ma már elektronikusan is rendelkezésre áll.

Az **adatvagyon hasznosításának** előfeltétele az **adatvagyon felmérése**. A felmérés során célszerű előnyben részesíteni azokat, amelyek a helyi vállalkozások és lakosok számára közvetlenül hasznosíthatók és máshonnan nem elérhetők, mint például az egyes intézmények, szolgáltatók (pl. szociális, köznevelési, egészségügyi intézmények, helyi vállalkozások, vállalkozók, önkormányzati közszolgáltatók, vendéglátóipari egységek) címei, elérhetőségei telephelyei, általuk nyújtott szolgáltatások jegyzékei, az igénybevétel feltételei.

Az adatvagyon leltár egy olyan tételes jegyzék, amely tartalmazza, hogy **a hivatal milyen folyamatokban, hol, kinek, hogyan, milyen személyes adatait gyűjti, azokat hol tárolja, milyen célra kezeli, milyen jogalapon, mennyi ideig őrzi meg és mikor törli azokat.**

A GDPR nem mondja ki, hogy adatvagyon leltár készítése kötelező lenne. Viszont azon hivataloknak, önkormányzati tulajdonú cégeknek – amely szervezeteknél meglehetősen sok személyes adatot kezelnek - ajánlott adatvagyon leltárt készíteni azért is, mert enélkül nehéz a GDPR-nak való megfelelés. Az adatvagyon leltár az alapul szolgálhat az elkészítendő adatvédelmi nyilvántartásnak és az adatkezelési tájékoztatónak is. Segítségével könnyebben meg lehet felelni a GDPR szerinti adatkezelési alapelveknek is.

Egy jól elkészített adatvagyon leltár arra is fényt derít, hogy az önkormányzatnál és a polgármesteri hivatalnál (közös önkormányzati hivatalnál) ki, milyen személyes adatokhoz fér hozzá, illetőleg milyen külső szervezetnek történik adattovábbítás, illetve rávilágíthat a GDPR követelményei be nem tartására is.

Az alábbiakban egy **kérdéslistát** mutatok be, amely mintául szolgálhat egy hivatal adatvagyon leltárának az elkészítéséhez, amely szabadon bővíthető.

[89] Ld. a https://www.naih.hu/hatasvizsgalati-lista honlapot.

Kérdések az adatvagyon leltárhoz polgármesteri hivatal vagy közös önkormányzati hivatal esetén

Adatkezelő megnevezése:

Székhelye:

Szervezeti egység megnevezése:

Kitöltő személy neve, elérhetősége:

Adatvagyon megnevezése	
Kezelt adatok (név, sorszám, cím, azonosító, stb.)	
Adatok típusa (személyes, különleges személyes, gazdálkodásra vonatkozó, stb.)	
Adatkezelés célja	
Adatkezelés jogalapja	
Adatkezelés időtartama	
Érintettek köre	
Végleges törlés időpontja	
Adat megismerésére jogosultak	
Tárolás helye	
Tárolás módja	
Adattovábbítás címzettjei	

2.5 Belső szabályzatok

2.5.1 Adatkezelési szabályzat

A GDPR-ra való felkészülés során többféle kérdés érkezett a szabályzatkészítési kötelezettséggel kapcsolatban a NAIH-hoz különféle szervezettől, így az önkormányzatoktól, polgármesteri hivataloktól (közös önkormányzati hivataloktól) is.[90] Tény, hogy az adatvédelmi szabályzat elkészítése prioritást kapott az önkormányzatok részéről a GDPR köztudatba

[90] NAIH/2018/1212/2/K és NAIH/2017/5364/2/V állásfoglalások.

kerülését követően. Az önkormányzati pályázati kiírások az adatvédelmi szabályzat elkészítése iránti igénnyel kezdődtek, ami azért volt kissé meglepő, mert az Infotv. korábbi változatának egy bekezdése[91] már a GDPR előtt is előírta az adatkezelők számára az elkészítését.

Bár a GDPR kifejezetten nem írja elő a szabályzat készítésének kötelezettségét az adatkezelő számára, a NAIH pedig úgy nyilatkozott, hogy ennek hiánya miatt önmagában nem fog büntetést kiszabni az adatkezelőkre.[92] Az adatkezelő feladatait meghatározó 24. cikk (2) bekezdése azonban úgy fogalmaz, hogy ha az az adatkezelési tevékenység vonatkozásában arányos, a megfelelő technikai és szervezési intézkedések részeként **az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.** A NAIH vonatkozó állásfoglalása szerint „ez alapján azt kell tehát az adatkezelőnek mérlegelnie, hogy a kezelt adatok mennyisége és köre alapján „arányosnak" mutatkozik-e adatvédelmi szabályzat vagy más szabályrendszer (pl. utasítás, folyamatleírás, biztonsági szabályzat) elkészítése."

Az önkormányzatok és szerveik, intézményeik nagy mennyiségű személyes adatot kezelnek, amelyek között lehetnek az érintettek számára nagyon érzékeny adatok (pl. adózással, vagyoni helyzettel, szociális helyzettel kapcsolatosak), illetve különleges adatok is (pl. szociális ellátás során az érintett egészségi állapotára vonatkozó adatok, óvodában, bölcsődében a gyermekek bizonyos egészségügyi adatai), illetve az adatkezelési tevékenységek nagy számára és a bonyolult belső szervezetrendszerre miatt is szükséges az adatvédelmi szabályzat megalkotása.

A GDPR nem ír elő konkrétumokat a belső adatvédelmi szabályokkal kapcsolatban, se formai se tartalmi követelmények nem jelennek meg. Az adatkezelő felelősséggel tartozik azért, hogy a szabályzat alapján kialakított adatkezelési gyakorlat összhangban legyen a GDPR-ral.[93]

Hazánkban a **szabályzat elkészítésének kötelezettségét az Info tv. előírja**.[94] Adatkezelőként a polgármesteri hivatal (közös önkormányzati hivatal) adatvédelmi és adatbiztonsági szabályzatot ad ki, ha az adatkezelő adatvédelmi tisztviselő kijelölésére köteles.

A szabályzatalkotás nem újdonság a közfeladatot ellátó hivatalok, intézmények számára, a legfontosabb tevékenységeiket általában valamilyen jogszabály által kötelezően előírt szabályzat alapján végzik. Több olyan szabályzattal is kötelezően rendelkezniük kell, amelyek közvetlenül érintik az adatvédelmet (pl. iratkezelési szabályzattal és irattári tervvel, információátadási szabályzattal, közérdekű adatok egyedi igénylésének és teljesítésének szabályzatával).

Az **informatikai biztonsági szabályzatot az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény** (továbbiakban: **Ibtv.**) teszi kötelezővé valamennyi önkormányzat képviselő-testületének hivatala számára (fontos, hogy csak a hivatalnak), és az ebben foglaltak nagymértékben segíthetik az adatkezelő szervet a GDPR 32. cikkében foglalt adatbiztonsági követelmények teljesítésében.[95]

[91] Info tv. 24. § (3) bek.
[92] NAIH/2018/1212/2/K állásfoglalás
[93] NAIH/2018/1212/2/K állásfoglalás
[94] Info tv. 25/A. (1) és (3) bek.
[95] 2013. évi L. tv. 11. § (1) bek. f)

Az interneten nyilvánosan elérhető adatkezelési szabályzatokat áttekintve leginkább az a tendencia figyelhető meg, hogy a legtöbb önkormányzat gyakorlatilag a rendelet előírásait ismétli meg ezekben a dokumentumokban és ritkább a konkrét eljárásokat részletező, gyakorlati útmutatást tartalmazó szabályzat. Szerencsére ma már sok jó példát találhatunk valóban jól hasznosítható, érdemi tartalommal rendelkező adatkezelési szabályzatra.

Az adatvédelmi és adatbiztonsági szabályzat a hivatal szervezetén belül érvényesülő olyan belső előírás, amely az érintettek jogainak érvényesülését garantálja, részletes eljárási szabályokkal, és a felelősség meghatározásával.

A **szabályzat célja**, hogy meghatározza a hivatalnál vagy az intézménynél folytatott személyes adatok kezelésének jogszerű rendjét, valamint az adatvédelem elveinek érvényesülését.

A **szabályzat hatálya** kiterjed a hivatalnál vagy az intézménynél foglalkoztatott valamennyi munkavállalóra, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatott személyekre (pl. megbízási szerződés).

A személyes adatok védelméért és az adatkezelés jogszerűségéért a hivatal vagy az intézmény vezetője (jegyző, intézményvezető) felelős.

Minden adatkezelőnek külön-külön szabályzattal kell rendelkeznie, illetve **közös adatkezelés** esetén együttesen is meghatározhatók a szabályokat, ilyenkor a szabályzat hatálya valamennyi érintett szervre kiterjed.[96] Az önkormányzati intézmények esetében a speciális tevékenységeik miatt szükség lehet önálló adatkezelési szabályzatokra, amelyek tartalmazzák ezekre az egyedi folyamatokra vagy jogszabályi követelményekre vonatkozó rendelkezéseket. Az egységességből itt alacsonyabb szinten is hasznot lehetne húzni, hiszen egy településen belül akár több ugyanolyan feladat ellátására létrehozott intézmény is lehet (pl. több önálló óvoda vagy bölcsőde), amelyek vezetői közös szabályzatot is készíthetnek.

Vannak olyan egyedi, komplex vagy nagy jelentőséggel bíró adatkezelési tevékenységek, amelyekre vonatkozóan **külön szabályok megállapítása** lehet szükséges, ilyen lehet például a kamerás megfigyelés vagy beléptető rendszer alkalmazása.

Elengedhetetlen, hogy **a többi szabályzattal is összhangban legyen az adatkezelési szabályzat**, hiszen a személyes adatok kezelése szinte valamennyi folyamat részét képezi.

A **legfontosabb témakörök,** amelyekről egy szabályzatban legalább rendelkezni kell: az érintettek tájékoztatásának a módja, érintetti jogok gyakorlására vonatkozó eljárásrend, ideértve az érintett által benyújtott kérelmek elintézésének módját és felelőseit, a GDPR által előírt nyilvántartások vezetésére vonatkozó eljárásrend, az adatvédelmi tisztviselő jogállása és feladatai, az informatikai biztonsági szabályzat hatálya alá nem tartozó adatkezelésekre vonatkozó adatbiztonsági követelmények és eljárások, a dolgozók adatvédelmi oktatása, valamint az incidensek kezelésére vonatkozó eljárásrend.

[96] NAIH/2017/5364/2/V állásfoglalás

Egy polgármesteri hivatal (közös önkormányzati hivatal) Adatvédelmi és Adatbiztonsági Szabályzatának tartalma (minta)

Szabályzatot kiadó jegyzői utasítás száma
Szabályzat hatályba lépésének kezdő ideje (év, hó, nap)
Általános rendelkezések
- Szabályzat célja, hatálya
- Adatkezelésre vonatkozó szabályok, fontosabb alapelvek, fogalmak
- Adatfeldolgozás a hivatalban
Adatvédelmi nyilvántartás készítése és vezetése, ennek keretében:
- Az adatkezelés célja, jogalapja, a kezelt adatfajták meghatározása
- Az adatok forrása
- Adatfelvétel, az adatok tárolásának módja, helye és időtartama
- Adattovábbítás belső szervezeti egységeknek
- Adatok továbbítása külső szervezetek számára, hatósági adatszolgáltatás, statisztikai célú adatszolgáltatás
- Adatok másolásának szabályai
- Adatok nyilvánosságra hozatala, önkormányzati honlapok kezelése
- Adatok törlése, módosítása
Az érintett jogai (tájékoztatáshoz, hozzáféréshez való jog, helyesbítés, adatkezelés korlátozásához, törléshez, adathordozhatósághoz, tiltakozáshoz való jog)
Az érintetti jogok érvényesítése, a kérelmek elintézésének módja és felelősei, külső szervezetek (NAIH, bíróság)
Adatkezelési tevékenységet folytató személyek feladatai
Adatvédelmi tisztviselő jogállása, feladatai
A munkavállalókra vonatkozó adatok felvétele, kezelése, személyi anyagok tárolása, közszolgálati, munkaügyi, személyzeti adatok nyilvántartása
- A munkáltató által biztosított eszközök ellenőrzésére vonatkozó szabályok
- Személyi anyagokba betekintés szabályai, adattovábbítás
- Titoktartási nyilatkozat
Az informatikai biztonsági szabályzat hatálya alá nem tartozó adatkezelésekre vonatkozó adatbiztonsági követelmények és eljárások
Adatvédelmi incidens kezelésére vonatkozó eljárásrend
Szabályzat módosítása, megismertetése a munkavállalókkal
Mellékletek (pl. nyomtatványok)

2.5.2 Kérdőív szabályzatok felméréséhez

A kérdőív megkönnyíti a szervezet vezetőjének és adatvédelmi tisztviselőjének a munkáját. A szabályzatok felülvizsgálatakor, aktualizálásakor azt is ellenőrizni szükséges, hogy a szabályzatok összhangban állnak-e a jogszabályi előírásokkal, igazodnak-e a hivatali sajátosságokhoz és teljeskörűek-e, illetve nem történt-e a hivatalon belül olyan személyi vagy szervezeti változás, ami a módosítást indokolja. A szabályzatok felméréséhez az alábbi kérdőív nyújt segítséget.

Kérdőív szabályzatok felméréséhez

Kérdés	Válasz
Rendelkezik a költségvetési szerv adatkezelési szabályzattal?	igen/nem
Mikor volt utoljára módosítva?	év, hónap, nap
Rendelkezik a költségvetési szerv adatkezelési tájékoztatóval?	igen/nem
Rendelkezett a költségvetési szerv 2018. május 25. előtt adatkezelési szabályzattal?	igen/nem
Rendelkezett a költségvetési szerv 2018. május 25. előtt adatkezelési tájékoztatóval?	igen/nem
Rendelkezik a költségvetési szerv információbiztonsági szabályzattal?	igen/nem
Mikor volt utoljára módosítva?	év, hónap, nap
Rendelkezik a költségvetési szerv adatvagyonleltárral?	igen/nem
A leltárt milyen időszakonként vizsgálják felül?	évente/félévente
Rendelkezik a költségvetési szerv nyilvántartással a hozzáférésekről?	igen/nem
Tárolják a hozzáférés igényléseket?	igen/nem
Rendelkezik a költségvetési szerv adatvédelmi hatásvizsgálattal?	igen/nem
Mikor volt utoljára felülvizsgálva a hatásvizsgálat?	év, hónap, nap
Bevezetett irányítási rendszerrel rendelkezik a cég?	igen/nem
Rendelkezik a költségvetési szerv adatkezelés megszüntetési nyilvántartással?	igen/nem
Rendelkezik a költségvetési szerv adatvédelmi incidens nyilvántartással?	igen/nem
Rendelkezik a költségvetési szerv érdekmérlegelési teszttel?	igen/nem
Rendelkezik a költségvetési szerv titoktartási nyilatkozattal?	igen/nem
Rendelkezik a munkaügyi folyamatokhoz kapcsolódó adatkezelési nyilvántartással?	igen/nem
Szabályozva van-e a személyi anyagokba a betekintési jog?	igen/nem

2.6 Adatkezelési nyilvántartás

A GDPR egyik – véleményem szerint – méltatlanul elfeledett újítása az adatkezelő és az adatfeldolgozó számára előírt **adatkezelési tevékenységek nyilvántartásának kötelezettsége**.[97] A korábbi Infotv. a felügyeleti hatóság számára írta elő az ún. adatvédelmi nyilvántartás vezetését, amelybe az adatkezelők feladata volt bejelenteni a különböző személyes adatok kezelésével járó tevékenységeiket. Ez vonatkozott a kötelező és a hozzájárulás alapján végzett adatkezelésekre is. Az adatvédelmi nyilvántartás nyilvános volt, abba bárki betekinthetett, valamint a kötelező adatkezelések kivételével a nyilvántartásba vételért szolgáltatási díjat is kellett fizetni a törvény alapján. Ennek fényében nem meglepő, hogy az adatkezelők többsége nem vette komolyan a bejelentési kötelezettséget, leginkább a közműszolgáltatók esetében találkozhattunk nyilvántartási számmal rendelkező adatkezelésekkel. A belső adatvédelmi felelős számára azonban már korábban is előírta a törvény a belső adatvédelmi nyilvántartás vezetését, de ez csak bizonyos szervezeteknél volt kötelező.[98]

A GDPR már általános jelleggel írja elő a **nyilvántartás vezetésének kötelezettségét**, amelyről az **adatkezelő vagy adatfeldolgozó gondoskodik**, írásban vagy elektronikus formában. Az adatkezelő vagy az adatfeldolgozó megkeresés alapján a felügyeleti hatóság részére rendelkezésére bocsátja a nyilvántartást, **a nyilvántartási kötelezettség nem teljesítése pedig bírságot vonhat maga után.**

Álláspontom szerint a nyilvántartás az egyik leghasznosabb eszköz lehet az adatkezelő számára a GDPR-ban foglalt egyéb kötelezettségei teljesítésére. A szabályokból látható, hogy az egyik célja a nyilvántartásnak, hogy a felügyeleti hatóság megfelelő információkhoz jusson az adatkezelő által folytatott tevékenységekről egy esetleges eljárás során, de ezeknek az információknak az adatkezelő saját maga is hasznát tudja venni, hiszen ez által átláthatja saját folyamatait, és a nyilvántartás adatait felhasználhatja például a tájékoztatási kötelezettség teljesítése során vagy összekapcsolhatja az incidens nyilvántartással is.

A GDPR ugyan lehetőséget ad a 250 főnél kevesebb személyt foglalkoztató vállalkozásoknak vagy szervezeteknek, hogy mentesüljenek a nyilvántartás vezetési kötelezettség alól, de ennek olyan szigorú feltételei vannak, amelyek egy önkormányzat vagy polgármesteri hivatal (közös önkormányzati hivatal), de szinte bármely más adatkezelő szervezet esetében aligha teljesülnek, hiszen az érintettek jogaira és szabadságaira kockázatot jelentő, nem alkalmi adatkezeléseket végeznek, amelyek magukban foglalják sok esetben a különleges adatok kezelését is.

A GDPR felsorolja, hogy **mit kell tartalmaznia a nyilvántartásnak** az egyes adatkezelési tevékenységekre vonatkozóan (pl. érintettek kategóriái, kezelt személyes adatok kategóriái stb.), azonban magát az **adatkezelési tevékenység fogalmát** nem határozza meg. Elsőre talán egyértelműnek tűnik, hogy mit is értünk adatkezelési tevékenység alatt, de a mai világban, ahol

[97] GDPR 30. cikk

[98] Infotv. 24. § (1) bek. e) pont (2016.07.01 - 2017.12.31 között hatályos állapot szerint)

gyakorlatilag nincs olyan folyamata egy szervezetnek, amely során ne kerülne sor személyes adatok kezelésére, ez rögtön bonyodalmat okozhat a nyilvántartás elkészítése során. Egy szűkebb tevékenységi körrel rendelkező vállalkozás esetében a főtevékenységekhez kapcsolódó adatkezelések számbavétele nem annyira bonyolult (például egy kisebb webshop esetében), de a munkavégzéssel kapcsolatos adatkezelési tevékenységekből már jóval több lehet (pl. munkaidő nyilvántartás, munkaszerződések, bérszámfejtés, cafeteria juttatások).

Kérdés, mennyire kell ezeket különválasztani, hiszen ezzel kapcsolatban nem ad útmutatást a GDPR. Mint az már sokszor említésre került, az önkormányzatok és szerveik nagyon eltérnek a más típusú adatkezelő szervezetektől, különösen a polgármesteri hivatal (közös önkormányzati hivatal), amely az önkormányzati adatkezelések jelentős részét bonyolítja le. Az adatkezelések nagy száma és azon belül a kötelező adatkezelések aránya, nem igazán teszi lehetővé, hogy azokat egyesével belefoglalják az adatkezelési szabályzatba, egyrészt terjedelmi okokból, másrészt pedig az egyes tevékenységeket meghatározó jogszabályok változása esetén a szabályzat módosítása válna szükségessé.

A részletesség kérdése ebben az esetben még inkább előtérbe kerül, hiszen nagyon nagy számú adatkezelési tevékenységről van szó, amelyek összegyűjtése, rendszerezése komoly erőforrásokat vehet igénybe a szervezet részéről. A szakjogász képzés során az önkormányzati adatkezelésekkel foglalkozó óra keretében a Budapesti Főpolgármesteri Hivatal adatvédelemmel foglalkozó munkatársának elmondása szerint a kb. 900 fős hivatalban csaknem egy évig tartott mire áttekintették és nyilvántartásba vették az összes adatkezelési tevékenységet.

Egy polgármesteri hivatalban (közös önkormányzati hivatalban) többféle foglalkoztatási jogviszony keretében - ezáltal különböző jogszabályi előírások szerint - kezelnek személyes adatokat a munkavállalókról, tucatnyi ügycsoport keretében számos eljárást folytatnak le, többféle nyilvántartást kezelnek, különböző szerződéseket kötnek. Lehet egy adott ügycsoport keretében végzett feladatokat egy adatkezelési tevékenységnek tekinteni? Vagy akár a hatósági ügyeket egy kalap alá venni az adatkezelési nyilvántartásban? Vagy pont fordítva, minden egyes ügyet, nyilvántartást, eljárást külön-külön elemként kell feltüntetni a nyilvántartásban? Sajnos ezzel kapcsolatban szintén nincs hivatalos álláspont, de véleményem szerint gyakorlati értelme az utóbbi megoldásnak van, hiszen még azonos csoportba tartozó ügyek esetében is lehetnek eltérések az adatkezelésben (pl. egyes adóügyek esetében teljesen eltérő adatokat kezelhet a hivatal).

Saját kutatás keretében megpróbáltam összeszedni a polgármesteri hivatalokban jogszabály alapján végzett és személyes adatok kezelésével járó folyamatokat, amely során több mint húsz féle ügycsoport (mint például az adóügyi igazgatás, gyermekvédelmi igazgatás, építésügy, anyakönyvi igazgatás stb.) keretében csaknem 140 különböző ügyet és nyilvántartást (pl. anyakönyvi nyilvántartás, adózói törzsadat-nyilvántartás, szociális támogatásban részesülők, támogatási kérelmek, köztisztviselők személyi anyaga stb.) azonosítottam, és biztos vagyok benne, hogy a lista nem teljes. Ezek csak a jogszabály alapján végzett tevékenységek, és csak a polgármesteri hivatal (közös önkormányzati hivatal), mint adatkezelő hatáskörében.

Az önkormányzatok számos egyéb adatkezelési tevékenységet végeznek, elég csak a képviselő-testület ülései során hozott döntésekre (határozatok, rendeletek) gondolni, ahol gyakorlatilag bárkinek bármilyen ügyhöz kapcsolódó személyes adata kezelésre kerülhet. Az önkormányzatok különféle rendezvényeket tarthatnak, amelyeken fotók és videofelvételek készülhetnek a résztvevőkről. Ezek a fotók bekerülhetnek az önkormányzat helyi lapjába vagy a videofelvételek felkerülhetnek az önkormányzat honlapjára. Az önkormányzati intézmények, (pl. az óvodák, bölcsődék, könyvtárak és művelődési házak, szintén tucatnyi adatkezelési tevékenységet folytatnak).

Az összes adatkezelési tevékenység azonosítása és nyilvántartásba vétele hatalmas munkát igényel egy önkormányzat részéről. Mivel az ellátandó közfeladatok típusa nagyrészt független az önkormányzat méretétől, ez azt jelenti, hogy a kisebb önkormányzatok is meghatározott esetekben hasonló adatkezelési tevékenységeket végeznek, mint a nagyobbak, csak az ügyek számában van különbség. Ennek fényében valószínű – ezzel kapcsolatos statisztika nem áll rendelkezésre, csak saját személyes tapasztalatok –, hogy az önkormányzati adatkezelők többségénél nem találkozhatunk részletes adatkezelési nyilvántartással, mert nem áll rendelkezésre megfelelő szakértelem és személyzet ennek létrehozására minden egyes önkormányzat esetében.

Az adatkezelési nyilvántartás ezért tipikusan egy olyan terület, ahol sokkal hatékonyabb lenne, ha központilag készítené el azt valamely szerv vagy egy olyan önkormányzati hivatal (közös önkormányzati hivatal), ahol erre megfelelő kapacitás áll rendelkezésre és azt a többi hivatal rendelkezésére bocsátanák ahelyett, hogy minden szervezet külön-külön kezdi nyilvántartásba venni az azonos jogszabályon alapuló, ugyanolyan módon és eszközökkel végzett adatkezelések tucatjait, ha egyáltalán foglalkoznak ezzel a kérdéssel.

2.7 Érintettek jogai érvényesítéséhez szükséges tájékoztatók

Az átláthatóság elve alapján minden adatkezelő kötelezettsége, hogy az előírtak szerint megfelelően tájékoztassa az érintetteket személyes adataik kezeléséről.[99] Minél kevesebb és minél egyszerűbb adatkezelési tevékenységgel rendelkezik egy adatkezelő, annál könnyebben tud eleget tenni ennek a kötelezettségnek. Az önkormányzatok esetében nagyszámú adatkezelés zajlik, ezért a tömör, átlátható, érthető és könnyen hozzáférhető tájékoztatás biztosítása nagyobb kihívást jelent számukra.

A GDPR 13. és a 14. cikk szerinti eljárás alkalmazására is szükség lehet, hiszen a kérelemre induló eljárások mellett hivatalból induló eljárásokra is sor kerülhet, ahol nem közvetlenül az Érintettől származnak az ügy tárgyát képező vagy annak lefolytatásához szükséges személyes adatok. Van olyan eljárás is, amikor az adatkezelő nem az érintettektől szerzi meg a személyes adatokat (például korábban a jegyző által az óvodaköteles korú gyerekekről vezetett nyilvántartás esetében).[100] Valamennyi önkormányzatnál indítható ügy szükségképpen együtt

[99] GDPR 13-14.cikk
[100] 22/2015. (IV. 21.) EMMI rendelet

jár személyes adatok kezelésével. Ezek az ügyek még adott szakterület esetében is eltérő jogszabályon alapulhatnak, amelyek eltérő adatok kezelését írhatják elő, más lehet az adatok megőrzésének ideje, a címzettek köre, az adatkezelés célja, de akár az adatkezelés módja is változhat (pl. elektronikus formában az önkormányzati ASP portálon keresztül vagy papír alapon). A hivatalnál eltérő tartalmú és formájú tájékoztatókra lehet szükség.

Nagy számú adatkezelési tevékenységnél kiemelt szempont, hogy valamilyen módon szortírozva legyenek a tájékoztatás szempontjából az egyes adatkezelések, egy egységes adatkezelési tájékoztatóban az érintettek bizonyosan elvesznének és nem teljesülne az átlátható, egyértelmű tájékoztatás követelménye.

A 29-es Munkacsoport hasonló esetekre azt ajánlja, akár több lépcsőben valósítsa meg az adatkezelő a tájékoztatást, ahelyett, hogy mindent egyetlen dokumentumba sűrítene.[101] A kérelemre induló ügyek esetében legtöbbször formalizált űrlapokat használnak a hivatalok, amelyek papír alapú változatára az adott adatkezeléssel kapcsolatos legfontosabb információk rávezethetőek, míg az egyéb adatkezelésekről szóló tájékoztatókat ügycsoportonként össze lehet foglalni egy rövidebb, átlátható dokumentumban.

Elektronikus ügyintézés során az iForm vagy ÁNYK űrlap tartalmazhat egy linket az adatkezelési tájékoztatók online eléréséhez. Mindezeket kiegészítheti az adott a hivatal általános adatkezelési tájékoztatója, amely tartalmazza az adatkezelő és az adatvédelmi tisztviselő nevét, elérhetőségeit, tájékoztatást az érintetti jogokról és a jogorvoslati lehetőségeket, így ezeket nem kellene minden egyes külön tájékoztatóban feltüntetni. Egy egységes jellegű módszer alkalmazására szintén lehetőség nyílna a teljes önkormányzati szférában, különösen, ha egy egységes adatkezelési nyilvántartáson alapul.

Az adatkezelési tájékoztatók tartalmában és színvonalában tapasztalható eltérés árulkodik talán a legjobban az önkormányzati szféra GDPR-nak való megfelelőségének ad hoc jellegéről, amely bizonyos érintett állampolgárok jogainak sérelmével járhat, valamint ez a heterogenitás rossz fényt vethet a teljes önkormányzati szektorra.

Az alábbiakban egy **érintettek jogai érvényesítéséhez szükséges tájékoztatót** mutatok be mintaként.

ADATKEZELÉSI ÉS ADATVÉDELMI TÁJÉKOZTATÓ

HATÓSÁGI FELADATOK ELLÁTÁSÁHOZ

(LEHETSÉGES MINTA)

Az Európai Parlamentnek és a Tanácsnak a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679/EU rendelete **(a továbbiakban: GDPR)**, valamint az információs önrendelkezési jogról és az információszabadságról szóló

[101] A 29. cikk szerinti adatvédelmi munkacsoport WP 260 rev.01 számú iránymutatása az (EU) 2016/679 rendelet szerinti átláthatóságról 21. oldal

2011. évi CXII. törvény alapján a …… Közös Önkormányzati Hivatal/….Polgármesteri Hivatal (a továbbiakban: **Hivatal**) az alábbi adatkezelési tájékoztatást adja.

Az Adatkezelési és Adatvédelmi Tájékoztató …. év …hó … naptól történő személyes adatkezelésekre vonatkozóan hatályos, módosítására a Hivatal jogosult. A közzététel helye: …. (honlap, hirdetőtábla stb.)

A szervezet honlapján a vonatkozó jogszabályok értelmében sütik (cookie) akkor helyezhetők el a felhasználó hozzájárulása nélkül, ha azok a webhely működéséhez elengedhetetlenek (adatkezelő jogos érdeke). Minden más célú (nem szükségszerű) cookie kizárólag a felhasználó hozzájárulására esetén helyezhető el. A szükséges sütik a weboldal minél jobb használhatóságát segítik elő. Olyan alapvető funkciókat is lehetővé tesznek, mint pl. a honlapon beállítások eltárolása, a honlapon történő navigálás. A Honlap ezen cookie-k használata nélkül nem működik megfelelően.

Az adatok tárolása elektronikusan, a ……. Hivatal által a ….szerveren történik.

A Hivatal, mint adatkezelő megteszi mindazokat a technikai és szervezési intézkedéseket, továbbá kialakítja azokat a belső eljárási szabályokat, amelyek a titoktartásra, az adatkezelés biztonságára vonatkozó szabályainak érvényre juttatásához szükségesek.

A Hivatal a kezelt adatokat megfelelő intézkedésekkel védi. Megőrzi az adatok sértetlenségét, biztosítja szükség esetén a titkosságot, védi az adatokat a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, sérülés ellen. A Hivatal megfelelően védi az informatikai rendszereit és hálózatait egyaránt a számítógépes csalások, számítógépes vírusok ellen.

Az üzemeltető a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik.

Jogszabályi háttér:

1) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, röviden: GDPR)
2) A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (a továbbiakban: Ltv.)
3) Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.)
4) A közigazgatási perrendtartásról szóló 2017. évi I. törvény (a továbbiakban: Kp.)
5) Az adózás rendjéről szóló 2017. évi CL. törvény (a továbbiakban: Art.)
6) Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (a továbbiakban: Mötv.).

Az adatkezelés átláthatóságának elvéből következik, hogy az érintettek részére nyújtott minden tájékoztatásnak az érintett számára könnyen érthetőnek, tömörnek kell lennie.

Tájékoztató elemei	Adatok (Szöveges rész)	Megjegyzés, jogszabályi háttér
Adatkezelő megnevezése	**Szervezet neve, székhelye, postacím, e-mail, telefonszám, képviselőjének neve.**	Hivatalnál a szerv vezetője a jegyző, önkormányzatnál a polgármester.
Adatvédelmi tisztviselő neve, elérhetősége	**Név, e-mail, telefonszám** **Az érintett jogosult a Hivatal adatvédelmi tisztviselőjéhez fordulni személyes adatai kezelésével kapcsolatban.**	Az adatkezelő és az adatfeldolgozó a személyes adatok kezelésére vonatkozó jogi előírások teljesítésének és az érintettek jogai érvényesülésének elősegítése érdekében adatvédelmi tisztviselőt alkalmaz, többek között ha állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot lát el. Adatvédelmi tisztviselőnek az jelölhető ki, aki a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik és alkalmas az Info. tv. 25/M. § (1) bek. szerinti feladatok ellátására.
Adatkezelés célja	**A Hivatal által a jogszabályokban előírt, a személyes adatok védelmével összefüggő követelmények érvényesítésével a hatósági feladatok ellátása.** **Az ügyek lezárását követően az adatok kezelésére az Ltv. szabályai szerint közérdekű archiválás, statisztikai, illetve tudományos, történelmi kutatási célból kerül sor.** **Az adatkezelés megkezdése előtt az érintett személy tájékozódhat arról, hogy a Hivatal a személyes adatait miért, milyen célból használja, az érintettet milyen jogok illetik meg, azokat hogyan gyakorolhatja.**	
Adatkezelés jogalapja	**Az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (GDPR 6. cikk (1) bek. e) pont).**	- Info. tv. 71. § (1) bek. szerint a Hivatal eljárása során - az annak lefolytatásához szükséges mértékben és ideig - kezelheti mindazon személyes adatokat, valamint törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatokat, amelyek az eljárással összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges. - Ákr. 27. § (2) bek. - a Hivatal gondoskodik arról, hogy a törvény által védett titok és egyéb adat ne kerüljön nyilvánosságra, ne juthasson illetéktelen személy tudomására,

		és ezen adatok törvényben meghatározott védelme a hatóság eljárásában is biztosított legyen. - Ákr. 33. § (1) bek. - az ügyfél az eljárás bármely szakaszában és annak befejezését követően is betekinthet az eljárás során keletkezett iratba.
Tájékoztató elemei	**Adatok (Szöveges rész)**	**Megjegyzés, jogszabályi háttér**
A kezelt adatok köre, ha azokat nem az érintett személy bocsátotta rendelkezésre	**Az ügyfél és a hatósági eljárás egyéb résztvevői természetes személyazonosító adatai, illetve az adott ügy tárgyától függően a tényállás tisztázásához, az eljárás eredményes lefolytatásához szükséges más személyes adat.**	Az adat forrása lehet: a) a panaszos vagy a hatósági eljárást kezdeményező személy azonosításához szükséges személyes adatok mellett az önként megadott adatok; b) személyi adat- és lakcím-nyilvántartásból adatszolgáltatás; c) adatkezelők által vezetett nyilvántartások; d) a hatósági eljárás egyéb résztvevői adatai (pl. tanú, szemletárgy birtokosa).
A személyes adatok címzettjei	**a) Az iratkezeléssel, az ügyfelekkel történő kapcsolattartás keretében történő adatátadás.** **b) A Hivatal a hatósági eljárásaival összefüggésben, egyedi ügyekben, a saját vagy más szerv közhatalmi eljárása lefolytatása céljából más szervekkel.**	a) pl. az illetékes Levéltárnak a Hivatal irattári terv szerint átadott nem selejtezhető iratai, az ügyfelekkel való kapcsolattartás keretében átadott adatok a Magyar Posta Zrt-nek; b) - Kp. 40. § (1) bek. - A Hivatal döntéseivel szembeni közigazgatási perben a Hatóság a keresetlevéllel együtt az ügy iratait felterjeszti a bírósághoz. A keresetlevelet a benyújtástól számított 30 napon belül kell az ügy irataival együtt a hatáskörrel és illetékességgel rendelkező bírósághoz továbbítani. - Kp. 40. § (2a) bek. - Jogszabály kötelezővé teheti, hogy valamely ügyben a keresetlevél benyújtásáról a felügyeleti szervet értesíteni kell. - Ákr. 134. § (1) bek. - A végrehajtást - ha törvény, kormányrendelet vagy önkormányzati hatósági ügyben helyi önkormányzat rendelete másként nem rendelkezik - az állami adóhatóság foganatosítja. - Art. 97. § - Ha az adóhatóság az elhunyt természetes személy adóügyével összefüggésben adóigazgatási eljárást folytat vagy azt kezdeményez, és ennek során az örökösök személyének ismerete szükséges, az adóhatóság megkeresésére a hagyatéki leltározásra illetékes önkormányzati jegyző adatot szolgáltat a hagyatéki leltár készítésének tényéről, a hagyatéki eljárást lefolytató közjegyző

		nevéről és székhelyéről, valamint a rendelkezésére álló hozzátartozói adatokról (név, cím). - Nyomozó hatóságok – a Hivatal a nyomozás lefolytatása érdekében átadja a szükséges iratokat az abban található személyes adatokkal együtt. - Mötv. 81. § k) - rögzíti a talált dolgok nyilvántartásába a talált idegen dologgal kapcsolatos, jogszabályban meghatározott adatokat, valamint a talált idegen dolog tulajdonosnak történő átadást követően törli azokat.
Tájékoztató elemei	**Adatok (Szöveges rész)**	**Megjegyzés, jogszabályi háttér**
Az érintett adatkezeléssel kapcsolatos jogai	**Az érintett személy a rá vonatkozó személyes adatokkal kapcsolatban bármikor, korlátozás nélkül kérhet tájékoztatást, az adataihoz való hozzáférést, helyesbítést, törlést, az adatkezelés korlátozását, az adatok hordozhatóságát, a hozzájárulásának visszavonását, továbbá tiltakozhat a személyes adatai kezelése ellen.**	
Tájékoztatáshoz való jog	**A Hivatal intézkedéseket hoz annak érdekében, hogy az érintettek részére, a személyes adatok kezelésére vonatkozó információt és minden egyes tájékoztatást átlátható, közérthető és könnyen hozzáférhető formában nyújtsa.** **A tájékozódáshoz való jog a Hivatal elérhetőségein keresztül gyakorolható. Az érintett részére kérésére tájékoztatás – személyazonosságának igazolását követően – szóban is adható.**	
Hozzáféréshez való jog	**Az érintett jogosult arra, hogy a Hivataltól tájékoztatást kérjen arra vonatkozóan, hogy a Hivatalnál folyamatban van-e személyes adatai kezelése, illetve a Hivatal mely jogalapon, milyen forrásból, mely személyes adatát, mennyi ideig és milyen adatkezelési céllal kezeli, illetve a Hivatal kinek, milyen célból, mely jogszabály alapján, mikor biztosított személyes**	

	adataihoz hozzáférést vagy kinek továbbította azokat, valamint azt, hogy a Hivatal alkalmaz-e valamilyen automatizált döntéshozatalt. **Az érintett kérelmére az információkat a Hivatal elektronikus formában is szolgáltathatja (e-mail útján vagy nagy mennyiségű adat esetén CD-re kiírva)**	
Tájékoztató elemei	**Adatok (Szöveges rész)**	**Megjegyzés, jogszabályi háttér**
Helyesbítéshez való jog	**Az érintett kérheti a Hivatal által kezelt, rá vonatkozó adat módosítását, a pontatlan személyes adatok helyesbítését és a hiányos adatok kiegészítését.**	
Az adatkezelés korlátozásához való jog	**Az érintett kérésére a Hivatal korlátozza az adatkezelést, ha:** **- az érintett vitatja a személyes adatok pontosságát (a Hivatal arra az időtartamra korlátozza az adatkezelést, amíg ellenőrzi a személyes adatot);** **- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;** **- a Hivatalnak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy** **- az érintett tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Hivatal jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.**	Ákr. 28. § (1) A hatóság kérelemre vagy hivatalból elrendeli az ügyfél illetve az eljárás egyéb résztvevője természetes személyazonosító adatainak és lakcímének zárt kezelését, ha a) őt az eljárásban való közreműködése miatt súlyosan hátrányos következmény érheti, vagy b) ugyanazon tényállás alapján a jogerősen vagy véglegesen lezárt, vagy párhuzamosan zajló és a hatóság előtt ismert más bírósági vagy hatósági eljárásban az ügyfél vagy az eljárás egyéb résztvevője adatainak zárt kezelését rendelték el. Ákr. 30. § A hatóság a kiskorú, a cselekvőképtelen és a cselekvőképességében részlegesen korlátozott nagykorú ügyfél, tanú, szemletárgy birtokos vagy megfigyelt személy védelme érdekében erre irányuló kérelem nélkül is dönthet az érintett személy adatainak zárt kezeléséről és az iratbetekintési jog korlátozásáról.

	Ha az adatkezelés korlátozás alá esik, a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni. **A Hivatal az érintettet az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.**	
Tájékoztató elemei	**Adatok (Szöveges rész)**	**Megjegyzés, jogszabályi háttér**
Tiltakozáshoz való jog	**Az érintett a saját helyzetével kapcsolatos okokból bármikor tiltakozhat személyes adatainak közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelés, vagy az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges kezelése ellen. Tiltakozás esetén a Hivatal a személyes adatokat nem kezelheti tovább, kivéve, ha azt olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.** **A személyes adatok közvetlen üzletszerzés érdekében történő kezelése elleni tiltakozás esetén az adatok e célból nem kezelhetők.**	
Törléshez való jog	**Az érintett az alábbi indokok valamelyikének fennállása esetén jogosult arra, hogy kérésére a Hivatal indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, ha:** **- a személyes adatokat jogellenesen kezelték,**	A levéltárba adandó iratok esetén az adatok törlésének kérelme nem teljesíthető, mert sérülne az irat integritása.

	- személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték, **- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja,** **- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,** **- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell,** **- a személyes adatok gyűjtésére információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.** **Az adatok törlése nem kezdeményezhető, ha az adatkezelés a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából, a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából, a népegészségügy területét érintő, vagy archiválási, tudományos és történelmi kutatási célból vagy statisztikai célból, közérdek alapján; vagy jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.**	
Tájékoztató elemei	**Adatok (Szöveges rész)**	**Megjegyzés, jogszabályi háttér**
Jogorvoslathoz való jog	**Ha az érintett megítélése szerint a Hivatal a személyes adatai kezelése során megsértette a hatályos adatvédelmi követelményeket, akkor panaszt nyújthat be a Hivatal honlapján feltüntetett módon.** **A felügyeleti Hatóság neve: Nemzeti Adatvédelmi és**	

	Információ-szabadság Hatóság (honlap: http://www.naih.hu; 1055 Budapest, Falk Miksa utca 9-11., e-mail: ugyfelszolgalat@naih.hu.) **Személyes adataival kapcsolatos jogsértés észlelése esetén a lakóhelye, tartózkodási helye szerinti illetékes bírósághoz is fordulhat.**	
Tájékoztató elemei	**Adatok (Szöveges rész)**	**Megjegyzés, jogszabályi háttér**
Személyes adatok másolata	**A Hivatal az érintett írásbeli kérésére az adatkezelés tárgyát képező személyes adatok másolatát díjmentesen bocsátja rendelkezésre. Többszöri kérelem esetén a Hivatal szabályzatában meghatározott díj felszámítására jogosult. Az érintett jogainak védelme érdekében a Hivatal meggyőződik arról, hogy az érintett és a hozzáférési jogával élni kívánó személy személyazonossága megegyezik-e, továbbá a betekintési jog gyakorlása is az érintett személy azonosításához kötött.**	
Személyes adatok tárolása	**A Hivatal a hatósági ügyekhez kapcsolódó iratokat az Ltv. szerinti követelményeknek megfelelőem az iratkezelési szabályzatában foglaltak szerint iktatja és adatokat az irattári tervben meghatározott selejtezésig, illetve levéltárba történő adásáig kezeli. A selejtezéssel (törléssel), illetve a levéltárnak történő átadással a személyes adatok kezelése megszűnik.**	
Eljárási szabályok	**A Hivatal indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 1 hónapon belül tájékoztatja az érintettet a fentiekkel kapcsolatosan az érintett által benyújtott kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további 2 hónappal meghosszabbítható.**	

	Ha nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 1 hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával. **A Hivatal a kért információkat és tájékoztatást díjmentesen biztosítja. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre észszerű díjat számolhat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.**	

2.8 Adatvédelmi bírság

Jelen pontban az Infotv. konkrét szabályai és a NAIH bírságolási gyakorlata kerül fókuszba.

A GDPR 83. cikk (7) bekezdése szerint az adott tagállam dönthet arról, hogy az ott székhellyel rendelkező közhatalmi vagy egyéb közfeladatot ellátó szervekkel szemben lehet-e bírságot kiszabni, és ha igen, annak mennyi a maximális mértéke.

A hatályos **Infotv.** ettől eltérően úgy fogalmaz, hogy a költségvetési szervek esetében nem lehet magasabb a kiszabott bírság összege 20 millió forintnál. A költségvetési szervek kategóriája szűkebb, mint a közfeladatot ellátó szervek köre és a sokszor hangoztatott indoka ennek az, hogy az állam ne mozgasson feleslegesen nagyobb összegeket a költségvetésen belül. Viszont ez a szűken meghatározott adatkezelői kör így azt eredményezi, bár vannak olyan szervek, akik bár jogszabályon alapuló közfeladatot látnak el, mivel nem költségvetési szervek, ezért nem érvényes rájuk a bírságkorlát.

A helyi önkormányzatok esetében maga az önkormányzat, a képviselő-testület hivatala és a képviselő-testület által alapított intézmények is mentesülnek a nagyobb összegű bírság alól, de az önkormányzat által létrehozott gazdasági társaságok ezen értelmezés szerint nem, márpedig sok esetben ezek azok a szervek, amelyek nagymértékű adatkezelést folytatnak, például a helyi közlekedési vállalatok, az ingatlankezelők vagy akár egy gyógyfürdő üzemeltetője. Továbbá vannak olyan esetek, amikor egy önkormányzati közfeladatot szerződés vagy más jogi aktus alapján nem egy önkormányzati intézmény, hanem például egy egyházi fenntartású nonprofit szervezet lát el, tipikusan az óvodai ellátás, a közétkeztetés vagy más szociális jellegű ellátások

kapcsán. Ilyen esetben az a helyzet áll elő, hogy az önkormányzati óvodát, mint költségvetési szervet maximum 20 millió forintra büntetheti a hatóság, míg egy egyházi fenntartású óvodát, amely átvállalta a közfeladat ellátását, a GDPR-ban foglalt általános szabályok szerint szankcionálhatnak.

Köztudott a NAIH álláspontja a **személyazonosító okmányok fénymásolásával** kapcsolatban, azt a cél eléréséhez alkalmatlan eszköznek tartja, ezért ilyen tevékenység folytatása **jogellenes adatkezelésnek minősül** idehaza. A bemutatott érvényes hatósági igazolványokban szereplőadatokat a dokumentumok közhiteles voltára tekintettel másolatkészítés nélkül is el kell fogadni.[102] A személyes gondoskodást nyújtó szociális ellátásokról a Magyar Államkincstár nyilvántartást vezet, amelybe a szolgáltatást nyújtó szervezetek rögzítik az ellátottak személyes adatait az ún. KENYSZI rendszeren keresztül.[103] Amennyiben a rendszer nem tudja azonosítani az újonnan regisztrálásra kerülő ellátást igénybe vevő személyt (pl. megváltoztak a nyilvántartásban szereplő adatai vagy elírás történt), akkor a személyazonosító okmány fénymásolatának csatolását kéri, amelynek jogszabályi alapja nincs, és a NAIH szerint nem is alkalmas az adatkezelési cél elérésére.[104] Akár egy önkormányzati intézmény, akár egy külsős szolgáltató biztosítja az ellátást, mindkettőnek ugyanezt a rendszert kell használni az ellátást igénybe vevők adminisztrálására.

Ez egyrészt rávilágít arra a problémára, hogy a központi rendszerek kötelező használatának esetében mennyire nem érvényesülnek az adatkezelő klasszikus jogosultságai, másrészt, ha a szolgáltató eleget tesz a Kincstár kérésének, akkor a NAIH akár el is marasztalhatná a hatóság álláspontja szerint jogsértő adatkezelés miatt. Mivel egy ilyen szolgáltató akár több ezer ellátott adatát is kezelheti – bár a hibás adatok kijavítására csak az esetek kis százalékában van szükség – ez akár egy súlyos adatvédelmi bírságot is vonhatna maga után. Ezzel szemben az önkormányzati intézmény, amely ugyanazt a szolgáltatást nyújtja, ugyanazt a rendszert használja és ugyanolyan jogellenesnek minősülhető adatkezelést folytat ilyen esetben is csak az Infotv-ben meghatározott bírságmaximumig marasztalható el.

A NAIH több esetben megállapított jogalap nélküli adatkezelést, az érintettek előzetes tájékoztatásának hiányát vagy a tájékoztatási kötelezettség megszegését, a személyes adat nyilvánosságra hozatalát. Nagyobb összegű bírságot általában olyan esetben szab ki a NAIH, ha az adott ügy kapcsán többféle jogsértés is megvalósult. Kisebb mértékű bírsággal enyhébb jogsértés esetén sújt a hatóság. Enyhítő körülménynek minősül, ha már az eljárás alatt a szervezet megszünteti a jogsértést, enyhíti a kárt.

A NAIH által 2012 és 2020 között nyilvánosan közzétett határozatok alapján megállapítható, hogy a Hatóság mintegy 20 olyan döntést hozott, amelyek önkormányzati kötődésű adatkezelőkre vonatkoznak, és ezek közül 4 született a GDPR alkalmazása óta. Összesen 14 esetben szabott ki a Hatóság **adatvédelmi bírságot** az adatkezelőkkel szemben, a leggyakoribb jogsértések a helyi adókötelezettségüket nem teljesítő adósok listájának közzétételével, valamint a zárt ülések jegyzőkönyveiben szereplő személyes adatok nyilvánosságra kerülésével

[102] NAIH/2018/3654/2/V állásfoglalás 1. pont
[103] 1993. évi III. törvény a szociális igazgatásról és szociális ellátásokról 20/C. §
[104] KENYSZI Felhasználói leírás: https://tevadmin.nrszh.hu/docs/Felhasznaloi_leiras_KENYSZI_OEP-TAJ_ellenorzes.pdf (2020.05.03.), 20. oldal

kapcsolatosak, de nem megfelelően alkalmazott kamerás megfigyelőrendszer miatt is sor került pénzbeli szankció alkalmazására.[105]

Általánosságban elmondható, hogy a GDPR-t megelőzően a bírságok mértéke 100 ezer és 500 ezer forint között mozgott, de a híres BKK-ügyben igencsak nagy összegbe, 10 millió forintba került a jogsértés az adatkezelőnek.[106] A NAIH 5 millió forint bírságot szabott ki jogalap nélküli adatkezelésért a vagyonvédelmi célú kamerarendszer kapcsán Kerepes Város Önkormányzatával szemben, amely döntés során figyelembe vette, hogy az adatkezelő semmilyen belső szabályzattal nem rendelkezett a kamerás megfigyelésre vonatkozóan.[107]

3. A GDPR-on kívülről fakadó eltérések az önkormányzati adatkezelésekben

3.1 Az adatkezelés jogalapja, a kötelező adatkezelés problémái

Két olyan terület nem került még említésre, amelyek kiemelkedő jelentőséggel bírnak az adatvédelem és a jogszerű adatkezelés megvalósítása során: az **adatkezelés jogalapja** és az **adatbiztonság**. Az önkormányzati adatkezelés jellegzetességei úgy gondolom inkább az adatkezelő szerv sajátosságaiból és a GDPR adott esetben eltérést engedő szabályaiból eredtek, az adatbiztonság és a jogalapok esetében viszont az igazi eltérések oka ezektől szinte független, azok más jogszabályokból és a NAIH sajátos álláspontjából fakadnak.

Legyen szó bármilyen típusú adatkezelőről az általa folytatott adatkezelési tevékenységek csak annyiban jogszerűek, amennyiben a GDPR 6. cikkének (1) bekezdésében felsoroltak egyike legalább teljesül, ezek jelentik az **adatkezelés jogalapját**. A GDPR-t megelőzően idehaza a korábbi Infotv. alapján – 95/46/EK irányelv nem megfelelő módon történő átültetésének köszönhetően – az esetek döntő többségében kétféle jogalap került alkalmazásra: **az érintett hozzájárulása**, vagy ha azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendelte.[108] Utóbbit nevezte a törvény **kötelező adatkezelésnek**. A GDPR hatálybalépését követően immár 6 féle jogalap közül választhat az adatkezelő, de valójában ezek már mind benne voltak az irányelvben is.[109] Láthattuk, hogy a közfeladatot ellátó és közhatalmi szervek esetében milyen speciális előírásokat tartalmaz a GDPR, azonban ezeknél sokkal meghatározóbb „körülmények" is hatással vannak a közfeladatot ellátó szervek – így az önkormányzatok – adatkezelésének jogszerűségére.

A GDPR az unió olyan másodlagos jogforrása, amely közvetlenül alkalmazandó és teljes egészében kötelező, tehát csak azon az alapon lehet személyes adatokat kezelni, amelyeket a rendelet taxatíve felsorol.[110] A 6. cikk (2) bekezdése azonban némi mozgásteret enged a

[105] NAIH-1303-9/2013/H és NAIH/2016/5877/5/H határozatai
[106] NAIH/2018/356/3/H határozat
[107] NAIH/2019/2076/11 határozat
[108] Infotv. 5. § (1) bek. (2016.07.01 - 2017.12.31 között hatályos állapot szerint)
[109] Az Európai Parlament és a Tanács 95/46/EK irányelve 7. cikk
[110] Várnay Ernő – Papp Mónika: Az Európai Unió joga, Budapest, Wolters Kluwer (2016) 313. oldal

tagállamok számára azzal, hogy az (1) bekezdés c) és e) pontja esetén konkrétabb követelmények meghatározását teszi lehetővé.

A magyar jogalkotó élt is ezzel a felhatalmazással és a hatályos Infotv. 5. § (3) bekezdésében úgy rendelkezik, hogy a c) és e) ponton alapuló adatkezelések esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát **az adatkezelést elrendelő törvénynek, illetve önkormányzati rendeletnek kell meghatároznia.** Ez egyfajta korlátozásként fogható fel, hiszen a GDPR maga csak azt írja elő, hogy ezekben az esetekben az adatkezelés jogalapját az uniós jognak vagy a tagállami jognak kell megállapítania.

A kötelező adatkezelés fogalma tehát tovább él az új törvényben is, azonban lényeges különbség, hogy immár nem csak törvény felhatalmazása alapján születhet az adatkezelés körülményeit meghatározó önkormányzati rendelet. A rendelkezés hátterében a magyar alkotmányos fejlődés keretében kialakított jogelvek állnak, melynek lényege, hogy alapjogot csak törvényben ill. önkormányzati rendeletben lehessen korlátozni, az adatkezelés pedig szükségképpen valamilyen szintű korlátozásként tekinthető az érintett jogaira és szabadságaira nézve.[111]

Csakhogy időközben a társadalmi és gazdasági folyamatok jóval bonyolultabbá, összetettebbé váltak, az adatkezelés pedig nagyon sok folyamat szükséges velejárója lett. Nincs ez másként az önkormányzati ügyek esetében sem, amelyek jelentős számát korábban már említettem. Az általam azonosított hivatali ügyek jelentős részében nem teljesül az Infotv-ben foglalt követelmény, mivel az adatkezelés részleteit nem törvény vagy önkormányzati rendelet, hanem kormányrendelet vagy miniszteri rendelet szabályozza, amelyek ugyan a GDPR alapján erre alkalmasak lennének – hiszen jogszabályok –, de a magyar jogalkotó által alkotott kiegészítő szabály alapján nem.

Ez gyakorlatilag azt jelentette volna, hogy a polgármesteri hivatalokban vagy az önkormányzati intézményeknél zajló adatkezelések többsége jogellenes, de az ezekkel összefüggő közfeladatok ellátása nyilvánvaló okokból nem szüntethetőek be. Az adatvédelem szempontjából olyan kiemelt fontosságú előírások is, mint az önkormányzati hivatalok egységes irattári terve – amely gyakorlatilag az adatok megőrzési idejét rögzíti a polgármesteri hivatalok számára – is miniszteri rendeletben került kiadásra.[112] Valószínűleg az adatvédelmi hatóság, a NAIH is érzékelte a problémát, ezért az egyik korai GDPR szerinti eljárásában a következő – rendkívül nagy jelentőségű – megállapításokat tette:

„Annak ellenére, hogy az Infotv. 5. § (3) bekezdése szerint kötelező adatkezelést csak törvény vagy törvény felhatalmazása alapján kiadott önkormányzati rendelet írhat elő, a pénzügyi intézmények informatikai rendszerének védelméről szóló kormányrendelet alapján a biztonsági mentésekben történő adatkezelés is kötelező adatkezelésnek minősül, mivel az Infotv. fenti rendelkezésének a jogalkotó a címzettje, nem pedig a jogalkalmazók.

[111] Bártfai – Hári – Jóri – Soós: i.m. 151. oldal
[112] 78/2012. (XII. 28.) BM rendelet - az önkormányzati hivatalok egységes irattári tervének kiadásáról

A Kérelmezett mint jogalkalmazó, nincs abban a jogi helyzetben, hogy a jogalkotónak címzett kötelezettség teljesítését értékelje, a megítélése szerint nem megfelelő jogforrási szinten számára előírt és hatályos jogi kötelezettségének teljesítését erre tekintettel mellőzze, ezért a személyes adatok kezelését kormányrendelet rendelkezéseire mint kötelező adatkezelést előíró normára is alapozhatja. A Hatóság jogalkalmazó szervként az ilyen – a GDPR rendelkezéseibe közvetlenül nem ütköző – norma előírásait szintén nem hagyhatja figyelmen kívül mindaddig, amíg az az adott állam arra jogosult szerve, jelen esetben az Alkotmánybíróság a megfelelő eljárásban az arra jogosult szervek vagy személyek indítványára eltérően nem rendelkezik."[113]

A NAIH kijelentette, hogy az Infotv. 5. § (3) bekezdésének nem az adatkezelő, hanem a jogalkotó a címzettje és jogszerűen jár el az adatkezelő, ha egyéb jogszabályban foglalt kötelezettségeit teljesíti. Mindezek fényében kérdéses, hogy a jogalkotó valaha is eleget fog-e tudni tenni az Infotv. rendelkezéseinek, hiszen **a jogrendszer tele van rendeleti szinten szabályozott adatkezelésekkel** és az elmúlt két év során nem igazán történtek lépések ennek orvoslására.

Véleményem szerint a kötelező adatkezelésre vonatkozó követelmények az idő múlásával meghaladottá váltak, és manapság nem várható el a jogalkotótól, hogy minden egyes adatkezeléssel járó folyamatot törvényben szabályozzon, és ennek legfőbb oka, hogy a legtöbb folyamat esetében a személyes adatok kezelése nem cél, hanem járulékos eszköz a megvalósítás érdekében.

Megjegyezni kívánom, hogy a GDPR alkalmazására maga a jogalkotó sem készült fel időben, ezért több olyan jogszabály maradt a jogrendszerben, amelyek nem voltak összhangban a GDPR előírásaival. A legjobb példa erre a hatósági eljárások általános szabályait meghatározó általános közigazgatási rendtartás (Ákr.) volt, amelynek az adatkezelésre vonatkozó 27. §-a korábban úgy szabályozott, hogy *„A kérelemre induló eljárásban vélelmezni kell, hogy a kérelmező ügyfél a tényállás tisztázásához szükséges személyes adatok – ideértve a különleges adatokat is – kezeléséhez hozzájárulást adott."* Végül a NAIH véleménye alapján módosították a törvényt, de jól látható ebből, hogy még egy ilyen kiemelt jelentőségű, és viszonylag frissen alkotott jogszabály esetében sem került sor időben a kiigazításra.

A **jogalapokkal** kapcsolatban korábban egy másik kérdés is felmerült az önkormányzatok számára, hogy **egyes adatkezelések esetében mégis melyiket válassza az adatkezelő** a GDPR 6. cikk (1) bekezdésében felsoroltak közül. Azóta a NAIH megállapította, hogy *„az adatkezelő közfeladatait meghatározó jogszabályi rendelkezéseken alapuló adatkezelések jogalapja tehát a GDPR 6. cikk (1) bekezdés e) pontja. Fontos kiemelnünk azt is, hogy egy közhatalmi tevékenységet vagy egyéb közfeladatot ellátó szerv – mint költségvetési szerv – minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya, ettől eltérő minősége fogalmilag kizárt. Ebből fakadóan e jogalap, mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat."*[114]

[113] NAIH/2019/1841 határozat
[114] NAIH 2018-as beszámolója, 36. oldal

A NAIH ezen jogértelmezésével kapcsolatban számos kritikát fogalmaztak meg a szakemberek, amelyekkel magam is egyetértek. Véleményem szerint a NAIH nem lenne jogosult ilyen tartalmú jogértelmezésre, mivel ez ebben a formában sokkal inkább alkotmányjogi kérdés, nem pedig adatvédelmi jogi.

A GDPR egyértelműen meghatározza a felügyeleti hatóságok feladat- és hatásköreit[115] az 57. cikkben. A NAIH jogértelmezése pedig a költségvetési szervek jogállására vonatkozik, amelynek értelmezése álláspontom szerint nem az adatvédelmi hatóság feladata. Az idézett szövegben a NAIH összemossa a közfeladatot ellátó szervek fogalmát a költségvetési szervekkel, holott a kettő nem azonos, nem minden közfeladatot ellátó szerv költségvetési szerv is egyben. Ez felveti azt a kérdést is, minden közfeladatot ellátó szerv esetében irányadó-e ez az értelmezés, vagy csak a költségvetési szervekre igaz.

Az Áht.[116] szerint a **költségvetési szerv** jogszabályban vagy alapító okiratban meghatározott közfeladat ellátására létrejött jogi személy.

A költségvetési szerv tevékenysége lehet

a) **alaptevékenység**, amely a létrehozásáról rendelkező jogszabályban, alapító okiratában a szakmai alapfeladataként meghatározott, valamint a szakmai alapfeladatai ellátását elősegítő más, nem haszonszerzés céljából végzett tevékenység,

b) **vállalkozási tevékenység**, amely haszonszerzés céljából, államháztartáson kívüli forrásból, nem kötelezően végzett termelő-, szolgáltató-, értékesítő tevékenység.

A költségvetési szerveknek alap- és vállalkozási tevékenysége egyaránt lehet, amelyek nem kapcsolódnak egymáshoz. Ezt erősíti meg a Pénzügyminisztérium álláspontja is, vagyis az alap- és a vállalkozási tevékenység között alapvetően aszerint tehető különbség, hogy míg az alaptevékenység minden esetben kapcsolódik a költségvetési szerv alapfeladatához, és annak ellátása nem irányul haszonszerzésre, a vállalkozási tevékenység végzése nem kötelező és annak célja nyereség elérése.*”*[117]

A fentiekre tekintettel vitatható a NAIH azon állítása, miszerint a költségvetési szerv minden közjogi és magánjogi jogviszonyának kizárólag közfeladatai ellátásával összefüggésben lehet alanya. A vállalkozási tevékenység keretében a költségvetési szervek úgy járnak el, mint bármely más nem közfeladatot ellátó jogi személy, az ilyen tevékenységeket nem jogszabály előírása alapján végzik. Ez problémát okoz a személyes adatok kezelés szempontjából.

A NAIH motivációja vélelmezhetően az lehetett, hogy megkönnyítse a közfeladatot ellátó szervek számára az adatkezelés jogalapjának meghatározását, de ezzel gyakorlatilag megfosztotta őket a választás lehetőségétől. Az e) pont szerinti jogalap megköveteli, hogy az adatkezelés uniós vagy tagállami jogon alapuljon, azonban ez csak az alaptevékenységek esetében teljesülhet. Mint említettem, a vállalkozási tevékenységre vonatkozóan ilyen

[115] GDPR 57. cikk
[116] Áht. 7. § (1) és (2) bek.
[117] https://allamhaztartas.kormany.hu/koltsegvetesi-szervek (2020.05.03.)

jogszabályok nem léteznek, ebben az esetben a költségvetési szerv eljárása nem különbözik a magánszférába tartozó más szervezetekétől.

Amíg a magánszférába tartozó adatkezelők alkalmazhatják a hozzájárulást, a szerződéses jogalapot, esetleg a jogos érdeket, addig a közfeladatot ellátó szerveknek akkor is az e) pontot kell megjelölniük az adatkezelés jogalapjaként, ha nincs olyan jogszabály, amely rendelkezne az adatkezelés részleteiről. Ezt a problémát a NAIH is észlelhette, ezért a következő kiegészítő szabályt fogalmazta meg: „Ha pedig a jogalkotó ezen adatkezelésekre vonatkozó részletes szabályokat az Infotv. 5. § (3) bekezdésének előírásait figyelmen kívül hagyva nem rögzítette, az **adatkezelő** az általános adatvédelmi szabályok – így különösen **az alapelvek és a jogalap szükségességi mércéje – szerint köteles adatkezelési tevékenységét végezni**, és annak **jogszerűségét az elszámoltathatóság elvének megfelelően igazolni**."[118] A NAIH ezáltal a jogszabályban rögzített garanciák helyett az adatkezelőre bízza a Hatóság a jogszerűség és az arányosság biztosítását, amely adott esetben azt is eredményezheti, hogy az adatkezelés jobban korlátozza az érintettek jogait és szabadságait vagy nagyobb kockázatot jelent ezekre nézve.

A NAIH álláspontja azért is elgondolkodtató, mert maga a GDPR szabályaiból is az következne, hogy a közfeladatot ellátó szervek kezelhetnek adatokat más jogalappal is, illetve más felügyeleti hatóság szerint is van erre lehetőség, sőt a NAIH elnöke által szerkesztett „Magyarázat a GDPR-ról" című könyvben még a jogos érdek alkalmazására is találhatunk példát a közhatalmi szervek esetében.[119]

A GDPR 55. cikke egyértelművé teszi, hogy nem csak az e) pont alapján kezelhet adatot egy közfeladatot ellátó szerv, amikor a felügyeleti hatóság illetékességével kapcsolatban úgy fogalmaz, hogy ha az adatkezelést a 6. cikk (1) bekezdésének c) vagy e) pontja alapján eljáró közhatalmi szervek vagy magánfél szervezetek végzik, az érintett tagállam felügyeleti hatósága az illetékes.[120]

Az Egyesült Királyság felügyeleti hatósága, az ICO úgy fogalmaz, hogy a közhatalmi szervek alkalmazhatják a jogos érdek jogalapot, amennyiben az adatkezelés nem az általuk ellátott közfeladat végrehajtásához kapcsolódik.[121] Ugyanezen a véleményen van A GDPR magyarázatának szerzője is.[122] Úgy gondolom amennyiben az uniós jogalkotó ki szerette volna zárni a közfeladatot ellátó szervek esetében a többi jogalap alkalmazását, akkor ezt explicite ki is mondta volna a GDPR szövegében, de ott csak az f) pont szerinti jogalap alkalmazásával kapcsolatban találkozhatunk megszorító szabállyal, amelyből logikai értelmezés alapján szintén az következik, hogy más esetekben lehetséges ennek a jogalapnak is a használata a közhatalmi szervek számára, tehát hivatkozhatnak az e) ponton kívül más jogalapra.

[118] NAIH 2018-as beszámolója, 36. oldal
[119] Péterfalvi – Révész – Buzás: i.m. 131. oldal
[120] GDPR 55. cikk (2) bekezdés
[121] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ (2020.05.03.)
[122] Bártfai – Hári – Jóri – Soós: i.m.172. oldal

Hogy mennyire **bonyolult lehet a megfelelő jogalap kiválasztása** az közhatalmi szervek számára, azt jól mutatja az önkormányzati hivatal épületében alkalmazott **vagyonvédelmi célú kamerás megfigyelőrendszer problémája**.

Az élet- és vagyonvédelem céljából alkalmazott kamerás megfigyelés jogalapja a korábbi gyakorlat szerinti hozzájárulás helyett a GDPR-t követően az adatkezelő jogos érdeke lehet a legtöbb esetben, ahogy ezt az **Európai Adatvédelmi Testület 3/2019. számú iránymutatása** is megerősíti.[123] Azonban tudjuk, hogy a GDPR kizárja a jogos érdekre hivatkozást a közhatalmi szervek által feladataik ellátása során végzett adatkezelések esetében, de a szakirodalomban többen is azt az álláspontot képviselték, hogy a megfigyelőrendszer alkalmazása nem tartozik ebbe a körbe, azt a szerv nem az alaptevékenysége keretében végzi, így alkalmazható az 6. cikk (1) bekezdés f) pontja.[124]

Ezt az álláspontot képviselte a Jegyző és Közigazgatás szaklapban az egyik adatvédelemmel foglalkozó szerző is 2019 decemberében, amikor már ismert volt a NAIH álláspontja a közfeladatot ellátó szervek által használható jogalapról, illetve a cikkben hivatkozott 3/2019-es iránymutatás is megismétli a jogos érdek alkalmazásának tilalmát közhatalmi szervek esetében.[125]

Időközben a **NAIH** Kerepes Város Önkormányzatát 5 millió forintra büntette a kamerás megfigyelő rendszer jogalap nélküli alkalmazása miatt. A határozatban a NAIH egyértelművé tette, hogy **nem fogadja el a jogos érdekre hivatkozást**, mint az adatkezelés jogalapját az önkormányzat által a hivatal épületében vagyonvédelmi célból üzemeltetett megfigyelőrendszer esetében.[126]

3.2 Egységesség

Több alkalommal utaltam már arra, hogy az önkormányzatok esetében nagyon hasonló adatkezelő szervekről beszélhetünk és ez lehetőséget biztosítana arra, hogy az adatvédelemmel kapcsolatos kötelezettségek teljesítésében közös elvek mentén járjanak el.

Természetesen a helyi önkormányzatok méretükben, erőforrásaikban, az önként vállalt feladatok mennyiségében és fajtáiban nagyon is eltérnek egymástól, de szervezetrendszerüket és alapfeladataikat jogszabályok határozzák meg, így az általuk végzett adatkezelések túlnyomó többségét is jogszabályban rögzített előírások alapján végzik. Ez **az egységesség az egész közszféra jellemzője is egyben**, még az információbiztonsággal kapcsolatban is közös a követelményrendszer. Ezen túlmenően is olyan – az adatvédelem szempontjából kiemelt jelentőségű – további eszközök kerültek bevezetésre az egységesítés jegyében az elmúlt években, mint az önkormányzati ASP rendszer, amelyhez a törvényi alapot **az Mötv.**

[123] Az Európai Adatvédelmi Testület 3/2019. számú iránymutatása, 9. oldal
[124] Bártfai – Hári – Jóri – Soós: i.m.173. oldal
[125] Rádi Vilmos: Önkormányzati kamerarendszerek üzemeltetése a GDPR hatálybalépése után, Jegyző és Közigazgatás XXI. évfolyam, 5. lapszám 32. oldal
[126] NAIH/2019/2076/11 határozat

módosításáról szóló 2016. évi LIV. törvény teremtette meg az Mötv. 114. §-ának módosításával.

A jogszabály rögzíti, hogy a helyi önkormányzatoknak országosan és egységesen olyan informatikai rendszert kell működtetniük, amely biztosítja a pénzügyi, ügyviteli, ügyintézési és egyéb alapvető feladatok egységes szabályok szerinti elvégzését és átláthatóságát, továbbá összekapcsolható az állami informatikai rendszerrel. A módosítás előírja az önkormányzatok számára egy adott, az állam által biztosított, konkrét informatikai rendszerhez, az önkormányzati ASP rendszerhez való kötelező csatlakozást. A törvény tehát kimondja, hogy az ASP rendszert országosan egységesen és kötelezően alkalmazni kell annak érdekében, hogy a helyi önkormányzatok egyes kötelező feladatai megfelelő informatikai támogatással valósulhassanak meg.[127]

A versenyszféra heterogén felépítésű és működésű, ezért az adatkezelésekben is egyedi megoldásokkal rendelkező szereplőivel összehasonlítva megállapítható, hogy az önkormányzatok - bizonyos eltéréseket engedve - de lényegében egységes szervezetrendszerrel rendelkeznek, egységes szabályok alapján járnak el feladataik végrehajtása során, azonos információbiztonsági követelményeknek kell megfelelniük. és az önkormányzati ASP, valamint az egyéb kötelező módon használt központi rendszer (pl. bérszámfejtés esetében a KIRA rendszer) használata miatt nagyrészt egységes eszközökkel végzik adatkezelési tevékenységeiket.

[127] Rupp Zoltán – Schindler Gábor: ÖNKORMÁNYZATI ASP Az önkormányzati ASP szakrendszerekre való felkészítés, Budapest, Dialóg Campus Kiadó (2018) 22-23. oldal

4. Utószó

Ma már az önkormányzatok számára a digitalizáció területén számos lehetőség áll rendelkezésre. A helyi közszolgáltatások elektronikus úton történő igénybevétele területén igen nagy fejlődésnek lehetünk tanúi.

Az Állami Számvevőszék jelentésében[128] leírja, hogy a digitalizáció térnyerése és egyre gyorsuló fejlődése a közszolgáltatásokat és azok infrastruktúráját is érintette, elengedhetetlenné téve az elektronikus-közigazgatás fejlesztését. Magyarországon egymást követő, egymásra épülő stratégiák mellett jogszabályváltozások nyitották meg az utat az új technológiai lehetőségek alkalmazása előtt. Számos területen átfogó fejlesztés történt: átalakult a lakossági és az intézményi infrastruktúra, új jogszabályi környezet született, **új szolgáltatási csomagok** jelentek meg, illetve az egyes intézmények szervezési folyamatait felülvizsgálták. Az ügyfeleknek 2018-tól nem csak lehetőségük van ügyeiket elektronikus úton intézni, hanem a közfeladatot ellátó szervek széles köre 2018. január 1-jétől köteles is biztosítani az ügyek elektronikus intézésének lehetőségét. Az automatizáció és digitalizáció által fémjelzett fejlesztések javították a belső folyamatok hatékonyságát, növekedett az intézmények kapacitása, valamint javult a szervezeti integráció. A digitális közigazgatás ezzel együtt kiemelkedően fontos szerepet játszott a koronavírus-járvány kezelésében és a tájékoztatásban, jelentősen mérsékelve a korlátozások negatív hatásait, az ügymenet veszélyhelyzetben is folytonos maradhatott.

Az Állami Számvevőszék rámutatott, hogy jelentősebb a lemaradásunk az uniós átlagtól az összetettebb digitális szolgáltatások területén, mind az űrlapok automatikus kitöltése, a teljes körű online ügyintézés és annak igénybevétele területén is. Miközben az elektronikus ügyintézést igénybe vevők száma folyamatosan növekedett, a **felnőtt lakosság csaknem fele tartózkodik ezek használatától.** A szolgáltatások igénybevételének szintje így továbbra is szuboptimális.

A digitális állam megteremtése csak akkor lehetséges, ha minden állampolgár számára elérhető és kezelhető alkalmazások képezik az alapját. A mesterséges intelligencia alapú automatizáció, az elektronikus térben elvégzett, videotechnológia alkalmazásával történő személyazonosítás, a hangazonosításra épülő hangvezérlés, az intelligens dokumentum kezelő rendszerek, hitelesítési folyamatok csak ebben az esetben lehetnek hatékonyak. A személyes ügyintézést preferálók ugyanis gyakran **nem rendelkeznek megfelelő ismeretekkel, vagy nem tudják használni az összetettebb alkalmazásokat.** Az elemzés arra hívja fel a figyelmet, hogy az e-közigazgatási szolgáltatások használatának növelése érdekében szükség van az alkalmazások felhasználóbarát jellegének további erősítésére, alakossági digitális kompetenciák fejlesztésére, az ügyintézési lehetőségek megismertetésére és az e-közigazgatással szembeni bizalom növelésére.[129]

[128] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 5. oldal.

[129] Ld. Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. 2022. https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 5. oldal.

Az akadályok forrása az alkotmányos szabályozás sajátosságaiban és a magyar önkormányzati identitás erejében rejlik. A digitális írástudás fejlődésének egyik sarokköve a háztartások számítógépes ellátottsága és az internet-elérés.[130]

Az adatvédelem nem képzelhető el az adatok biztonságos kezelése nélkül. Bár a GDPR szövegében nem tűnik annyira hangsúlyosnak az adatbiztonság kérdése a rengeteg adminisztratív szabály mellett, a gyakorlatban azonban ez az a terület, amely a legnagyobb kockázatot hordozza mind az érintettek (pl. sérül az adatok bizalmassága vagy azok elvesznek), mind az adatkezelő (bírságot kap, a jó hírnevén csorba esik) számára és ez igényli az önkormányzatok részéről a legnagyobb anyagi ráfordítást is.

A GDPR-ra való felkészülés során az önkormányzatok egyik legfontosabb feladata volt, hogy eleget tegyenek ennek az előírásnak és biztosítsák az adatok megfelelő fizikai és informatika védelmét.

5. Felhasznált szakirodalom

Könyvek, cikkek, tanulmányok

Dr. Béres László: Aktualitások az adatvédelem területéről (Jegyző és Közigazgatás, 2021/4., 26-27. o.)

Dr. Balázs István CSc.: A „JÓ KÖZIGAZGATÁS" ILLÚZIÓJÁRÓL című cikke, 8. oldal. http://real.mtak.hu/73066/1/a_jo_kozigazgatas_illuziojarol.pdf .

Dr. Bekényi József – dr. Barabás Zoltán (szerk.): Önkormányzatokról önkormányzatoknak, Budapest, Belügyminisztérium kiadványa – többszerzős – (2019) https://2015-2019.kormany.hu/download/b/4d/b1000/%C3%96nkorm%C3%A1nyzati%20k%C3%B6nyv%20-%20Online.pdf#!DocumentBrowse

Csáki Gyula Balázs: Az elektronikus közigazgatás tartalma és gyakorlatának egyes kérdései. Doktori értekezés. https://ajk.pte.hu/sites/ajk.pte.hu/files/file/doktori-iskola/csaki-gyula/csaki-gyula-vedes-ertekezes.pdf

Eszteri Dániel: Az adatvédelmi hatásvizsgálat és az előzetes konzultáció (Nemzeti Közszolgálati Egyetem) 2019.
A kiadvány letölthető: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/14671/Az%20adatvedelmi%20hatasvizsgalat%20es%20az%20elozetes%20konzultacio.pdf?sequence=3&isAllowed=y

Horváth E. Írisz – Kalas Tibor – Kárpáti Magdolna – Kurucz Krisztina – Marosi Ildikó – Márton Gizella – Mudráné Láng Erzsébet – Petrik Ferenc – Rothermel Erika – Tóth Kincső: A közigazgatási perrendtartás magyarázata, Budapest, HVG-ORAC (2017)

Jóri András, Soós Andrea Klára, Bártfai Zsolt, Hári Anita: A GDPR magyarázata – HVGORAC (2018.)

Kálmán Attila: A GDPR felértékeli az adatvédelmi szaktudást https://jogaszvilag.hu/a-gdpr-felertekeli-az-adatvedelmi-szaktudast/

Muha Lajos – Krasznay Csaba : Az elektronikus információs rendszerek biztonságának menedzselése (Nemzeti Közszolgálati Egyetem kiadványa, 2018) Letölthető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y

Péterfalvi Attila, Révész Balázs, Buzás Péter: Magyarázat a GDPR-ról (Wolters Kluwer Hungary Kft)

Rádi Vilmos: Önkormányzati kamerarendszerek üzemeltetése a GDPR hatálybalépése után, Jegyző és Közigazgatás XXI. évfolyam, 5. lapszám 32. oldal

Rupp Zoltán – Schindler Gábor: ÖNKORMÁNYZATI ASP Az önkormányzati ASP szakrendszerekre való felkészítés, Budapest, Dialóg Campus Kiadó (2018)

Révész Balázs, Szabó Endre Győző, Dudás Gábor, Tóth András, Deli Gergely, Eszteri Dániel, Nikolicza Péter, Pataki Gábor, Bojnár Katinka, Báldy Péter, Árvay Viktor György, Domokos Márton, Buzás Péter, Sulyok Tamás, Trócsányi Sára, Villám Krisztián – AZ INFOTÖRVÉNYTŐL A GDPR-IG, Ludovika Egyetemi Kiadó (2021)

Várnay Ernő – Papp Mónika: Az Európai Unió joga, Budapest, Wolters Kluwer (2016)

Az adatkezelők és az adatfeldolgozók felelőssége című NAIH által készített ppt. (STAR projekt). These training materials are based on standard training materials developed in the context of the project "Supporting Training Activities on the Data Protection Reform" – STAR (http://www.project-star.eu/)

Handbook on Security of Personal Data Processing, European Union Agency for Network and Information Security (2018)

KENYSZI Felhasználói leírás:
https://tevadmin.nrszh.hu/docs/Felhasznaloi_leiras_KENYSZI_OEP-TAJ_ellenorzes.pdf

https://allamhaztartas.kormany.hu/koltsegvetesi-szervek honlap

http://unipub.lib.uni-corvinus.hu/4141/1/VT_2019n0708p88.pdf honlap

https://ikir.bm.gov.hu/ honlapot a helyi közszolgáltatás információs rendszerről (IKIR)

https://ohp-20.asp.lgov.hu/nyitolap honlap

https://www.magyarhirlap.hu/belfold/20191223-adatvedelmi-vizsgalat-jozsefvarosban

https://nepszava.hu/1154103_vademeles-a-polgarmester-ellen-bukhat-az-ugyved-is

https://gdpr.blog.hu/2020/07/10/biometrikus_azonositassal_kapcsolatos_felreertesek
Biometrikus azonosítással kapcsolatos félreértések

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

https://kti.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto/altalanos-informaciok

Fontosabb jogszabályok, uniós jog

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről **(GDPR)**

Az Európai Parlament és a Tanács 95/46/EK irányelve

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info tv.)

A köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Ltv.)

Az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (Ákr.)

A közigazgatási perrendtartásról szóló 2017. évi I. törvény (Kp.)

Az adózás rendjéről szóló 2017. évi CL. törvény (Art.)

Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (Mötv.).

A szociális igazgatásról és szociális ellátásokról szóló 1993. évi III. törvény (Sztv.)

A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény (Kttv.)

Az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény

Az önkormányzati ASP rendszerről szóló 257/2016. (VIII. 31.) Korm. rendelet

Az önkormányzati hivatalok egységes irattári tervének kiadásáról szóló 78/2012. (XII. 28.) BM rendelet

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet

A belügyminiszter 11/2018. (VI.12.) BM utasítása a Belügyminisztérium Szervezeti és Működési Szabályzatáról

Jogértelmezés, NAIH állásfoglalások, határozatok, iránymutatások, beszámolók, elemzések

A 29. cikk szerinti adatvédelmi Munkacsoport WP 243 rev.01 számú iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban (16/HU WP 243 rev.01)

https://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf

Az Európai Adatvédelmi Testület 3/2019. számú iránymutatása

Az Európai Bíróság C-210/16. sz. ügyben hozott ítélete

NAIH beszámoló a 2018. évi tevékenységről (www.naih.hu)

NAIH/2019/2076/11 számú határozata (https://gdprbirsagok.hu/ honlap)
NAIH/2019/1841 határozat
NAIH/2018/3654/2/V állásfoglalás
NAIH/2018/1212/2/K állásfoglalás
NAIH/2018/356/3/H határozata
NAIH/2016/5877/5/H határozata
NAIH-1303-9/2013/H határozata
NAIH/2019/2076/11 határozat
NAIH/2017/5364/2/V állásfoglalás
NAIH-1881-5/2013/H számú határozata (https://gdprbirsagok.hu/ honlap)

https://www.naih.hu/hatasvizsgalati-lista honlap

https://www.naih.hu/az-adatvedelmi-hatasvizsgalat-es-elozetes-konzultacioja honlap

https://www.naih.hu/hatasvizsgalati-szoftver honlap

https://www.naih.hu/hatasvizsgalati-lista honlap

Állami Számvevőszék: Elemezés – Az e-közigazgatás helye a digitális állam stratégiai pillérben. (2022.)
https://www.asz.hu/storage/files/files/elemzesek/2022/Elemzes_E_kozig_helye_a_digitalis_allam_strat_pillerben.pdf?download=true 13. oldal.

Az OECD értékelése a magyar Közigazgatás- és Közszolgáltatás-fejlesztési Stratégiáról (2014-2020), I. rész https://hirlevel.egov.hu/2018/01/01/az-oecd-ertekelese-a-magyar-kozigazgatas-es-kozszolgaltatas-fejlesztesi-strategiarol-2014-2020-i-resz/.

Nemzeti Digitalizációs Stratégia Ld. https://2015-2019.kormany.hu/download/f/58/d1000/NDS.pdf honlapot.
Készítette: Innovációs és Technológiai Minisztérium, Belügyminisztérium.