BELSŐ ADATVÉDELEM

2015.

Szerzők:

dr. Ábrahám Dominika I. fejezet, VII, fejezet, X, XII. fejezet;

dr. Ujfaludi Zoltán VIII, fejezet IX . fejezet XI. fejezet;

dr. Kiss Attila II-VI fejezet;

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

MAGYARY PROGRAM

I. BEVEZETÉS

A Közigazgatás Korrupció-megelőzési Programja[1] a 2012-2014. cselekvési időszakra elsődlegesen a közigazgatási, és részben egyes közszolgálati korrupciós jelenségek visszaszorítását célozta meg. A koncepciót a Nemzeti Korrupcióellenes Program (2015-2018) (a továbbiakban: Program) tovább folytat oly módon, hogy az általános célkitűzésekhez igazodóan ezúttal már a kormányzaton kívüli szereplőket is orientálni kívánja.

A Program lefekteti a korrupció elleni kormányzati cselekvés főbb alapelveit, a cselekvési irányok meghatározásához szükséges elvi-módszertani alapokat, kitűzi az általános célokat és kitér a kapcsolódási, lehatárolási kérdésekre. A helyzetértékelés keretében összefoglalja a korrupció elleni fellépés magyarországi fejlődését, a korrupció megelőzésére és az integritás erősítésére tett kormányzati intézkedéseket, korrupciós elemzéseket, indexeket mutat be, foglalkozik a nemzetközi szervezetek megállapításaival, továbbá áttekinti a főbb nemzetközi antikorrupciós és integritás trendeket.

Figyelembe veszi a közigazgatás szereplőinek, továbbá a korrupció elleni küzdelemért különös felelősséget viselő független állami szervezeteknek a véleményét és javaslatait.

Általános célja az integritás kultúra erősítése, a közpénzekkel való gazdálkodás átláthatóbbá tétele, a hatósági eljárások fejlesztése, az üzleti élet tisztaságát elősegítő szabályozás kialakítása, a közérdekű bejelentések megtételének és a bejelentők védelmének optimalizálása, az oktatás és képzés kiterjesztése, a szemléletformálás, továbbá a hatékony korrupcióellenes küzdelemhez szükséges személyi és tárgyi feltételrendszer megteremtése; amely területekre vonatkozó intézkedésektől már középtávon a korrupcióval szembeni szervezeti és egyéni ellenálló képesség erősödését várja.

A tárgyi és személyi feltételrendszer legmarkánsabb eszköze az új integritás tanácsadók képzése és a már feladat és hatáskörben eljáró tanácsadók folyamatos képzése.

Annak érdekében, hogy a kormánytisztviselők megismerjék a megelőzéssel és az integritással kapcsolatos követelményeket, a Nemzeti Közszolgálati Egyetem ezeket beépítette alap- és mesterfokú képzéseibe, továbbá két féléves integritás tanácsadó szakirányú továbbképzést is indított. Ez a képzéssorozat az elmúlt évtizedek egyik legnagyobb közszolgálati továbbképzését valósította meg, és újszerűségüket, a bennük rejlő innovációt az Európai Bizottság is kiemelte a 2014-ben publikált EU Antikorrupciós Jelentésben. Az oktatás során

[1]

felhalmozódott ismeretek fenntarthatóságát és továbbfejlesztését a Nemzeti Közszolgálati Egyetemen belül 2013-ban létrejött Integritás Tudásközpont szolgálja A tanácsadói tananyagba elsőként kerül be a belső adatvédelem című tárgy. Elsődlegesen azért, mert az integritás tanácsadó feladatköre összekapcsolható a belső adatvédelmi felelős feladatkörével, és így komplex képzést kap erre is kiterjedően, másodsorban azért, mert a tanácsadói munka során számos olyan feladatot kell megoldania, amelyhez belső adatvédelmi ismeretekre van szükség. Mi is az a belső adatvédelem? Alapját az Információs önrendelkezésről és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv) képezi, tekintettel arra, hogy a belső adatvédelem nagy része gyakorlati feladatok megoldásából áll, ennek a megvalósításához szeretnénk az Infotv. és a saját gyakorlati tapasztalataink szintetizálásával hozzájárulni. Számos gyakorlati példát mutatunk meg annak érdekében,hogy a hallgató könnyedén navigáljon az olyan kérdések között, mint, hogy mi is a belső adatvédelmi nyilvántartás, hogyan kell az adatvédelmi nyilvántartásba bejelentkezni, vagy hogyan válaszoljunk meg egy közérdekű adatigényt és hogyan készítsünk el egy szervezetre szabott adatvédelmi és adatbiztonsági szabályzatot. Amennyiben felkeltettük az érdeklődését, kérem induljunk el velünk a személyes adatok rengetegében. Az erre vonatkozó feladatok megoldásához elengedhetetlen az elméleti áttekintés. A belső adatvédelem ezen részét, a talán kissé szárazabb és nehezebben érthető elméletet egy sokkal logikusabb és átláthatóbb láncolatra fűztük fel. Ennek alapját a fogalmak képezik, amelyek azonban nem a szokványos értelmező rendelkezés szerepét hivatottak betölteni, hanem egyszerű és tömör szintetizálását hozzák létre az elméleti és gyakorlati alkalmazásoknak.

Előre bocsátva csak annyit, hogy a belső adatvédelem feladata az adott szerv adatkezelésre terjed ki, tekintettel arra, hogy különböző adatcsoportokat különböztetünk meg egymástól a rájuk vonatkozó adatkezelési szabályok is különbözőek lesznek. Az egyes adatkezelési szabályokat tehát elkülönülnek egymástól, de mivel hatással vannak egymásra egy adott kérdés megoldása esetén, együtt érvényesülnek. A belső adatvédelem három részterületét szeretnénk bemutatni, amely egyenként és összességében is kapcsolatban van az integritási tanácsadói feladatokkal.

Tekintsük át, hogy mely területek ezek a belső adatvédelemben.

1. Közérdekű adatok, közfeladatot ellátó szerv átláthatósága.

Minden közfeladatot ellátó szervnek[2], lehetővé kell tennie, hogy a kezelésében lévő közérdekű és közérdekből nyilvános adatok átláthatók, megismerhetők legyenek. A közérdekű adat megismerésére adatigényt nyújthat be bárki, amelyre az adott adatkezelő szervnek az Alaptörvényben és az infotv-ben foglalt kötelezettség alapján a megismerési korlátokat figyelembe véve, eleget kell tennie. Amikor egy közérdekű adatigényt teljesít a közfeladatot ellátó szerv tudnia kell, hogy a közérdekű adatok visszatartása, közérdekű adattal való visszaélés vétségét, míg amennyiben a közérdekű adatok kiadásával személyes adatokat is megismerhetővé tesz, személyes adattal való visszaélés vétségét valósítja meg. A megismerési eljárás, mindig egy vékony határvonalon zajlik, a mérleg két serpenyőjében az információszabadság és az információs önrendelkezés joga helyezkedik el. A két jog, azaz a közérdek és magánérdek összeütközésekor a szükségesség és arányosság elve lehet a mérce, amelyre láthatunk példát is) Az Infotv.-ben a fentiek az információszabadságban testesülnek meg.

2. A személyes adatok védelme.

Az Infotv. hatálya[3], minden Magyarországon kezelt személyes adatra vonatkozik, legyen az bárki adata. Ebből azonban következik, hogy a nem Magyarország területén kezelt személyes adatokra nem alkalmazható az Infotv. A Magyarországon kezelt adatok tekintetében nem mindegy, hogy ki az adatkezelő, mivel a természetes személy kizárólag saját személyes céljait szolgáló adatkezelése sem tartozik az Infotv. hatálya alá. A közfeladatot ellátó szerv adatkezeléseinek jogalapját törvényi szabályozás vagy az érintett fél hozzájárulása alapozza meg. Minkét jogalap alapján kezelt adatkezelésekre az Infotv. információs önrendelkezési joga vonatkozik. A közfeladatot ellátó szerv adatvédelme a természetes személyek személyiségi jogát és az adott intézmény jogbiztonságát alapozza meg. A személyes adatok védelme a legszorosabban az integritás bejelentési eljárásnál kapcsolódik a tanácsadó munkájához és a bejelentő védelem tekintetében nyilvánul meg, ezért erre a gyakorlatban is kitérünk.

[2] Infotv. 26. § (1) bekezdés alapján közfeladatot ellátó szerv: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv.

[3] Infotv. 2. § (1) E törvény hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik.

3. Közzétételi kötelezettség

Az Infotv. 1. számú mellékletében található általános közzétételi listában meghatározott és egyes esetekben más törvényekben megjelölt adatokat kell a költségvetési szerveknek a honlapjukon illetve a Közadattárban közzétenni. A kötelezően megjelenítendő adatok a közérdekű vagy közérdekből nyilvános adatok csoportjába tartoznak, amelyekre a továbbiakban részletesen kitérünk. A közzététel szintén hozzájárul a közfeladatot ellátó szerv átláthatóságához.

II. SZEMÉLYES ADATOK VÉDELME

BEVEZETÉS

A 2012. január 1-től hatályos új Alaptörvény közös bekezdésben említi az információs alapjogokat: a személyes adatok védelmét és a közérdekű adatok nyilvánosságát. Az Alaptörvény nevesíti azt is, hogy e két alapvető jog érvényesülését sarkalatos törvénnyel létrehozott független hatóság (a Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH) ellenőrzi.[4]

A közigazgatás napjaink egyik legkomplexebb rendszere, amelyet a működése során kialakuló számos jogviszony miatt jogszabályok széles köre szabályoz. Érdekesség, hogy a személyes adatok védelmére vonatkozó jogi szabályozás születése is közvetlenül a közigazgatás összetettsége miatti túlzott információéhségéhez kapcsolódott. 1970-ben a németországi Hessen tartományban új informatikai rendszerek kialakításával, összekapcsolásával egy funkcionálisan integrált igazgatási rendszert kívántak bevezetni, ami 70 különböző adatot kezelt volna egymással összekapcsolt adatbázisokban minden állampolgárról.[5] A mindent tudó Nagy Testvér, az orwelli világ rémképe miatt azonban társadalmi igény jelent meg az adatkezelés korlátok közé szorítására,[6] ugyanis, ha személyes adataink fölött nem rendelkezhetünk, nem tudhatjuk meg, hogy mely adatunkat ki, és milyen célból kezeli, akkor fennállhat a veszélye annak, hogy azokat – akár gazdasági, politikai előnyt remélve – rosszhiszeműen használják majd fel. Hessenben a tömeges tiltakozások

[4] Magyarország Alaptörvénye, VI. cikk (2)-(3)
[5] Spiros Simitis: The Hessian Data Protection Act (Wiesbaden: The Hessian Data Protection Commissioner, 1987), p. 5.
[6] Sólyom László: Egy új szabadságjog: az információszabadság (Világosság, 1988/1.) p. 25.

hatására ezért még ugyan ebben az évben elfogadták Európa első adatvédelmi törvényét, melyet szerte a világban számos hasonló tárgyú jogszabály követett.[7]

A közigazgatás szereplői kiterjedt feladat és hatásköri rendszerük következtében napjainkban is nagy mennyiségű, a személyek magánéletére vonatkozó információt ismernek meg, a közigazgatás információs társadalmi térben mozog.[8] A jogállami működéshez azonban alapvető elvárás, hogy az általuk kezelt valamennyi adat (így különösen a személyes adatok) bizalmasságát, sértetlenségét, és integritását garantálni tudják, és emellett az érintetteknek az adataikhoz kapcsolódó jogait is biztosítsák.[9] Az állampolgárok magánszférájának védelmét akkor lehet hatékonyan biztosítani mind a papír adatkezelések során, mind az elektronikus térben, ha megismerjük az adatvédelem jogi és intézményi rendszerét, és (adott esetben akár belső adatvédelmi felelősként) ennek megfelelően alakítjuk ki az egyes feladatok ellátására vonatkozó belső szabályozást is.

III. A MAGYAR ADATVÉDELMI SZABÁLYOZÁS ALAPJAI

E fejezet célja, hogy az olvasó megismerkedjen a személyes adat és az információs önrendelkezési jog fogalmával, az adatok kezelésére, védelmére vonatkozó legfontosabb alapelvekkel, valamint annak Európai Uniós és hazai jogszabályi környezetével.

1. A személyes adatok kezelésére vonatkozó jogszabályi környezet

A személyes adatok védelmének törvényi szintű szabályozására először 1992-ben került sor Magyarországon, az Alkotmánybíróság nagy hatású döntésének – a népesség-nyilvántartás és a személyi szám általános azonosítóként történő alkalmazását alkotmányellenesnek minősítő határozata[10] – közvetlen eredményeként. A jogalkotó az Alkotmánybíróság által azonosított információs önrendelkezési jogot (és annak korlátait) valamint az információszabadságot

[7] Az adatvédelmi jogi szabályozás nemzetközi fejlődéséről, az egyes generációk legfontosabb jellemzőiről lásd bővebben Szőke Gergely László: Az adatvédelem szabályozásának történeti áttekintése, in: Infokommunikáció és Jog 10:3, 2013.

[8] Budai Balázs Benjámin: E- Közigazgatás axiomatikus megközelítésben. (Pécs 2008.) p. 324.

[9] Magyarország Alaptörvénye védelemben részesíti a magán- és családi életet, a kapcsolattartást és jó hírnevet, valamint a személyes adatok védelmét. Ezekre vonatkozó információ jogosulatlan harmadik személyhez kerülése, vagy jogosulatlan felhasználása a fentieken túl sérti még az emberi méltósághoz fűződő alapjogot is.

[10] A 15/1991. (IV. 13.) AB határozat kimondja, hogy az Alkotmánybíróság „*a személyes adatok védelméhez való jogot nem hagyományos védelmi jogként értelmezi, hanem annak aktív oldalát is figyelembe véve, információs önrendelkezési jogként. … a személyes adatok védelméhez való jognak eszerint az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról. Személyes adatot felvenni és felhasználni tehát általában csakis az érintett beleegyezésével szabad; mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját, vagyis mindenkinek joga van tudni, ki, hol, mikor, milyen célra használja fel az ő személyes adatát.”*

ugyanabban a törvényben, a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvényben (a továbbiakban Avtv.) szabályozta. Fontos kiemelnünk, hogy a személyes adatok védelméhez való jogot nem hagyományos védelmi jellegű (passzív) jogként kell értelmeznünk, azaz nem csak az adatokat kell megvédenünk, hanem az információs önrendelkezési jog aktív oldalát is figyelembe kell vennünk, azaz az érintettnek az adatai feletti rendelkezéshez, és a zavartalan magánélethez való jogát kell biztosítanunk. A szabályozás alapvető célja, hogy személyes adatai felett mindenki szabadon rendelkezhessen, ugyanakkor az állam működésének átláthatóvá tételéhez szükséges információt mindenki megismerhesse.[11]

Az Avtv.-t természetesen számos alkalommal módosították, ezek közül ki kell emelnünk az Európai Unióhoz való csatlakozásunkhoz kötődő változásokat, amikor a hazai szabályozás mellett megjelent az Európai Unió joganyaga is. Az adatvédelem közösségi szintű, harmonizált szabályozási kereteinek kialakítása az Európai Unió információs társadalommal kapcsolatos politikájának is lényeges területe. Az uniós jog számos rendelkezése foglalkozik a személyes adatok kezelésének és védelmének kérdéseivel, a joganyagban általános hatályú, a területet átfogó elvek szerint szabályozó dokumentumokat, és szektorális szabályokat egyaránt találunk. A jelenleg hatályos uniós jogforrások közül a legfontosabb az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (adatvédelmi irányelv), de emellett 2004 májusától figyelembe kell már vennünk az irányelvet értelmező, azt eseti döntésekkel továbbfejlesztő Európai Unió Bíróságának határozatait is. Ezek az adatkezelésekre vonatkozó már-már precedens értékű döntések általános iránymutatást adnak.

2012. január 1-től az 1992-es szabályozást felváltotta az információs önrendelkezési jogról és az információszabadságról szóló, jelenleg is hatályos 2011. évi CXII. törvény (Infotv. vagy adatvédelmi törvény). E jogszabály – bár nagymértékben támaszkodik a korábbi szabályozásra, és számtalan rendelkezést szó szerint átvesz az Avtv.-ből – számos ponton módosítja is a korábbi szabályozást, új adatkezelési jogalapokat határoz meg, és teljesen átalakítja az adatvédelem felügyeleti rendszerét. Az Infotv. címében külön megjelenik az adataink feletti információs önrendelkezés joga, azonban e jognak nem szolgáltat egyértelmű

[11] A főszabály alól kivétel, hogy ha azt törvény, vagy törvényi felhatalmazás alapján született önkormányzati rendelet előírja, akkor személyes adat hozzájárulás hiányában is kezelhető, bizonyos közérdekű adatokat pedig a vonatkozó törvényben meghatározott esetekben titkosan lehessen kezelni.

definíciót a törvény az értelmező rendelkezései között, hanem az Alkotmánybíróság korábbi meghatározására hagyatkozik, így a fent leírt alapelvek továbbra is alkalmazandóak.[12]

Ki kell emelnünk, hogy a személyes adatok védelmének szabályozása nem oldható meg egyetlen átfogó jellegű törvényben. Az Infotv. csupán a hatálya alá tartozó valamennyi adatkezelés során figyelembe veendő általános követelményeket és garanciákat határozza meg (keretet ad a szabályozásnak), amit azonban az adott adatkezelés sajátosságaira koncentráló nagyszámú, az általános szabályokat konkretizáló ágazati adatvédelmi jogszabály (EU rendelet, törvény, vagy törvényi felhatalmazás alapján született önkormányzati rendelet) egészíthet ki. Ennek megfelelően például az egészségügyi ellátáshoz kapcsolódó adatkezelésre vonatkozó általános szabályokat is az Infotv. tartalmazza, de ezeket sok esetben kiegészíti, pontosítja egy külön jogszabály, az egészségügyi adatok kezeléséről szóló törvény (Eüak.).[13] Szintén gyakori, hogy az Infotv. általános szabályai szerint az adatok egy meghatározott köre személyes adatnak minősülne (pl. az érintett neve, fizetése, vagy beosztása),[14] de egy külön jogszabály, például a közszolgálati tisztviselőkről szóló törvény (Kttv.) bizonyos érintettek esetében ezeket közérdekből nyilvános adatnak minősíti (pl. kormánytisztviselők vagy köztisztviselők meghatározott adatai).[15]

[12] Az Alkotmánybíróság az Alaptörvény megszületését követően sem változtatott a korábbi, fent idézett álláspontján, azt változatlan formában megerősíti a 2/2014. (I. 21.) AB határozatában.
[13] Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény
[14] Infotv. 3. § 2. pont
[15] 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről 179.§, valamint 226.§ (2) bekezdése

1. ábra Az egyes adatkezelési műveletekre irányadó jogszabályok áttekintése

2. Alapfogalmak

2.1. Személyes adat, különleges adat

Az Infotv. a *személyes adat* fogalmát igen szélesen határozza meg, személyes adat az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat fogalma egy másik fogalommal, az *érintett* fogalmával lesz teljes. Az Infotv. alapján az érintett bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.[16] A törvény szerint személyes adata csak természetes személyeknek van; a jogi személyekre és más szervezetekre az adatvédelmi garanciák nem terjednek ki. Az adatvédelmi törvény csak élő személyek személyes adatait védi, az elhunyt személy adataival kapcsolatban elsősorban a kegyeleti jog rendelkezéseit kell figyelembe vennünk, melyet a Polgári törvénykönyv és a Büntető törvénykönyv szabályoz, illetve részben az egészségügyi adatok kezeléséről szóló törvény is tartalmaz rendelkezéseket az elhunyt betegre vonatkozó adatok sorsáról.

[16] Infotv. 3. § 1. pont

A törvény szigorúbb adatkezelési feltételeket határoz meg a személyes adatoknak arra a körére, amelyekkel való visszaélés súlyosabb következményekkel járhat (szenzitív vagy érzékeny adat). Az Infotv. ezeket az adatokat *különleges adatnak* nevezi. Ezek közé tartozik – a törvény zárt felsorolása szerint – egyrészt a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, másrészt az egészségi állapotra, a kóros szenvedélyre, a szexuális életre vonatkozó adat, valamint a bűnügyi személyes adat.[17]

2.2. Adatkezelés, adatfeldolgozás, adatkezelő, adatfeldolgozó

Az *adatkezelés* az adatokon végzett bármely művelet vagy a műveletek összessége, függetlenül az alkalmazott eljárástól, azaz a törvényt mind az automatizált, mind a manuális módon végzett adatkezelésekre alkalmazni kell. Adatkezelés – a törvény példálózó felsorolásában – az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, a fénykép-, hang- vagy képfelvétel készítése.[18]

Az a természetes személy vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza, és e döntéseket – maga vagy egy adatfeldolgozó megbízásával – végrehajtja, az *adatkezelő*.[19]

Az Infotv. hatálya alá eső adatkezelések csak akkor minősülnek jogszerűnek, ha a törvényben foglalt valamennyi adatvédelmi elvnek és feltételnek megfelelnek, például kellően pontosan meghatározott és jogszerű célból történnek, megfelelő jogalappal rendelkeznek, az adatkezelés időtartamát előre meghatározzák, az adatok minősége megfelelő, az érintetteket megfelelően tájékoztatják, és biztosítják számukra az adatok módosításához, adott esetben azok törlésének kéréséhez való jogukat. E feltételeket a továbbiakban részletesen is kifejtjük.

Az adatkezelési műveletekhez kapcsolódó technikai feladatok – az alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől független – elvégzése az adatvédelmi törvény szerint *adatfeldolgozás*nak minősül. Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából személyes adatok feldolgozását végzi, az adatfeldolgozó. Az adatkezelő és az adatfeldolgozó

[17] Infotv. 3. § 3. pont
[18] Infotv. 3. § 10. pont
[19] Infotv. 3. § 9. pont

közötti megbízási jogviszonyból következően az adatfeldolgozó az adatkezelő utasításainak megfelelően végzi a tevékenységét, ő maga az adatkezelést érintő érdemi döntést nem hozhat. Felelőssége a saját tevékenységi körén belül a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért áll fenn. Az általa az érintettnek okozott kárért az érintettel szemben az adatkezelő felel.[20]

Adatfeldolgozói jogviszony a gyakorlatban jellemzően olyankor jön létre, amikor az adatkezelő valamely olyan tevékenységét szervezi ki, amelynek keretében a neki szolgáltatást nyújtó szervezetnek személyes adatokhoz kell hozzáférnie és azon valamilyen műveletet végeznie, például egy ivóvíz szolgáltatást nyújtó cég a befizetendő díjról szóló számlákat egy nyomdával készítteti el, amelyhez át kell adnia a kezelésében lévő személyes adatokat, az ügyfél nevét, címét, a számla végösszegét. Ebben az esetben tehát az ügyfél adatait a nyomda csak az adatkezelő által az adatfeldolgozói szerződésben meghatározott célból és keretek között kezelheti, és csak azért felelős, ha ennek kereteit átlépi, de azért nem tartozik felelősséggel, ha az adatkezelő nem jogszerűen szerezte meg az adatokat, vagy hibás adatokat adott át neki.

2.3. Az Infotv. hatálya

Az Infotv. rendelkezéseinek hatálya a Magyarország területén folytatott minden olyan adatkezelésre és adatfeldolgozásra kiterjed, amely természetes személy adataira, valamint közérdekű adatra vagy közérdekből nyilvános adatra vonatkozik. A törvény területi hatálya tehát Magyarországra terjed ki.

A törvényt az adatkezelés módjától függetlenül a teljesen vagy részben automatizált eszközzel, valamint a manuális módon végzett adatkezelésre és adatfeldolgozásra is alkalmazni kell.

Végül fontos kivétel, hogy nem kell alkalmazni az adatvédelmi szabályokat a természetes személynek a kizárólag saját személyes céljait szolgáló adatkezeléseire.[21] E kivétel nélkül előállhatna az a nyilvánvalóan értelmetlen helyzet, hogy egy magánszemély mobiltelefonos telefonkönyve (amelyben a személy mások személyes adatait tárolja, ami tehát adatkezelésnek minősül) is az adatvédelmi szabályozás hatálya alá esne. Megjegyzendő ugyanakkor, hogy amennyiben azonban e telefonszámokat a személy a saját személyes célján

[20] Infotv. 3. § 17-18. pont, 10. §
[21] Infotv. 2. §

kívüli célból, például az újonnan indított vállalkozásának népszerűsítésére használja, úgy ezen adatkezelés már az Infotv. hatálya alá kerül.

3. Az adatkezelés jogalapja

A 80-as évektől kezdődően az európai adatvédelmi szabályozás egyik legfontosabb jellemzőjévé vált, hogy a személyes adatok kezelésére csak meghatározott, jogszabályban tételesen felsorolt jogalapok megléte esetén kerülhet sor. Az adatkezelőnek tehát minden esetben igazolni kell tudnia az adatkezelés jogalapját.

3.1. Az érintett hozzájárulása

Az információs önrendelkezési jogból következően az adatvédelem rendszerében az első és az egyik legfontosabb jogalap az érintett adatkezeléshez történő hozzájárulása.

A törvény meghatározása alapján a hozzájárulás az érintettnek az a nyilatkozata, amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. A NAIH álláspontja szerint az adatvédelmi törvény akkor tekinti megadottnak az érintett hozzájárulását, ha az önkéntes, határozott, kifejezett, félreérthetetlen és a megfelelő tájékoztatáson alapul.[22] A „kifejezett hozzájárulás" körébe tartozik valamennyi olyan helyzet, amikor felteszik az egyének számára a kérdést, hogy egyetértenek-e vagy sem személyes adataiknak egy adott felhasználásával, vagy közzétételével, és ők nem pusztán tudomásul véve, hanem aktív magatartással, szóban vagy írásban válaszolnak a kérdésre.[23] Az érintettet ezért már az adat felvétele előtt tájékoztatni kell az adatkezelés legfontosabb körülményeiről, hogy e tájékozott és kifejezett hozzájárulását megadhassa. A tájékoztatásnak ki kell terjednie az adatkezelés önkéntes vagy kötelező jellegére, az adatkezelés céljára és jogalapjára, az adatkezelésre és az adatfeldolgozásra jogosult személyére, az adatkezelés időtartamára, az adatokat megismerők személyére, illetve az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire.[24]

Az érintettek önrendelkezési joga nem korlátozható akkor sem, ha az adatkezelés elektronikus úton történik, ezért amennyiben nincs más jogalapja az adatkezelésnek, akkor az adatok

[22] http://naih.hu/files/2223-2-2013-v.pdf [2015.03.20.] p. 3.
[23] A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport által elfogadott, a hozzájárulás fogalmáról szóló 15/2011. számú vélemény (WP187) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_hu.pdf [2015.03.20.]
[24] Infotv. 3. § 7. pont, 20. §

interneten való közzétételéhez, továbbításához, rögzítéséhez is az érintett kifejezett hozzájárulása szükséges.[25]

A hozzájárulás általában nincs alakiságokhoz kötve, azaz szóban, sőt ráutaló magatartással is megadható (az adatkezelés „eltűrése" azonban nem minősül hozzájárulásnak, mert annak kifejezettnek kell lennie). A törvény szigorúbb alakiságot követel meg azonban a különleges adatok, így például az egészségügyi adatok kezelése esetén is, ahol csak az írásbeli hozzájárulás tekinthető jogszerűnek. A 29. cikk alapján létrehozott Adatvédelmi Munkacsoport ezzel kapcsolatban megállapította, hogy az egészségügyi adatok kezeléséhez „on-line környezetben elektronikus vagy digitális aláírások alkalmazásával is adható kifejezett hozzájárulás. A helyzettől függően azonban még gombokra történő kattintással, megerősítő e-mailek küldésével, ikonokra való kattintással, stb. is adható."26 A hozzájárulásnak az érvényességhez nem kell rögzíthetőnek lenni a Munkacsoport álláspontja szerint, de a bizonyíték megőrzése az adatkezelő érdekében áll, mivel a hozzájárulás érvényességét, illetve az adatkezelés jogszerűségét az adatkezelőnek kell biztosítani, illetve vitatott esetben később bizonyítani. Az egészségügyi adatok kezeléséhez való internetes hozzájárulás ezért az adatvédelmi biztos és a NAIH értelmezése alapján csak akkor tekinthető megadottnak, ha egyértelműen bizonyítható, hogy az érintettől származik, engedélyező tartalmú, illetve, hogy az adott szolgáltató adott szolgáltatására vonatkozik.[27]

A törvény megállapít további hozzájárulási vélelmeket is:

1) Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni (például kiskorú, vagy eszméletlen állapotban van), akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatai kezelhetőek.[28] Az „életfontosságú érdek" alapján például az eszméletlen sérülthez kiérkező mentős megismerheti a beteg adatait azért, hogy azonosítani tudja kiveheti a beteg zsebéből az iratait.

[25] Az adatvédelmi biztos 679/P/2007 számú ügyben hozott állásfoglalása
[26] WP187 p. 28.
[27] Nemzeti Adatvédelmi és Információszabadság Hatóság beszámolója 2012.03.30 http://naih.hu/files/NAIH-2012-Beszamoloja-vegleges-web.pdf [2015.03.20.] pp. 25-26; és az adatvédelmi biztos 679/P/2007 számú ügyben hozott állásfoglalása.
[28] Infotv. 6.§ (2)

2) Már az érintett 16. életévének betöltését elegendőnek tekinti a törvény ahhoz, hogy érvényes hozzájárulást adhasson adatai kezeléséhez.

3) Megadottnak tekinti az adatkezeléshez való hozzájárulást az érintett közszereplése során az általa közölt vagy a nyilvánosságra hozatal céljából általa átadott adatok tekintetében.

4) Végül vélelmezni kell a hozzájárulást az érintett kérelmére, kezdeményezésére indult bírósági vagy hatósági eljárásban az eljárás lefolytatásához szükséges személyes adatok tekintetében, az érintett kérelmére indult más ügyben az általa megadott személyes adatok tekintetében. E vélelmek kiterjednek a különleges adatok esetére is.

3.2. Jogszabályon alapuló (kötelező) adatkezelés

Az érintett hozzájárulásán kívül személyes adat kezelését közérdekből törvény, valamint törvény felhatalmazása alapján kiadott helyi önkormányzati rendelet is előírhatja (kötelező adatkezelés). A kötelező adatkezelés célját és egyéb feltételeit az adatkezelést elrendelő jogszabály határozza meg. A korábban említett ágazati adatkezelési szabályok sok esetben éppen ilyen, adatkezelést elrendelő jogszabályoknak tekinthetők, amelyek gyakran nem önálló törvényként, hanem az adott szektort szabályozó törvény részeként jelennek meg. Az ilyen, jogszabályon alapuló adatkezelés tehát az érintett akarata ellenére is jogszerű lehet, például egy büntetőeljárás során, de az egészségügyi adatok kezeléséről szóló törvény is kötelezően előírja a kezelőorvos számára, hogy haladéktalanul továbbítsa az egészségügyi államigazgatási szervnek az adatfelvétel során tudomására jutott egészségügyi és személyazonosító adatot, ha meghatározott fertőző betegséget észlel a betegnél.[29]

Fel kell hívni ugyanakkor a figyelmet arra is, hogy a törvényen alapuló adatkezelés csak az ott meghatározott célra, adatkörre, időtartamra terjedhet ki. Az ezeken kívül eső adatkezelések esetén más jogalapot kell találnia az adatkezelőnek, ami lehet az érintett kifejezett vagy a fenti szabályok alapján vélelmezett hozzájárulása vagy valamely más jogszabály is.

[29] A jogalkotó a személyes adatok, illetve a szigorúbban védett különleges adatok kezelését akkor rendelheti el, „ha az adatkezelés lehetővé tételével egyidejűleg meghatározza az adatkezelés pontos feltételeit, azaz az Alkotmány 59. § (1) bekezdésben garantált személyes adatok hoz való alapjog korlátozásának konkrét részletszabályait.” (ABH 2002, 357, 363.)

3.3. Érdekmérlegelésen és jogi kötelezettség teljesítésén alapuló adatkezelés

Az új Infotv. talán legjelentősebb újdonsága az adatkezelési jogalapok bővítése. A korábbi adatvédelmi törvény kizárólag két esetben tette lehetővé a személyes adatok kezelését: ha ehhez az érintett hozzájárult, vagy ha ezt törvény, illetve törvény felhatalmazása alapján, az abban meghatározott körben helyi önkormányzat rendelete előírta. A 2012 januárjától hatályos szabályozásban az érdekmérlegelés jelentősen kitágítja a jogszerű adatkezelések körét, és egyúttal szükségszerűen bizonytalanabbá is teszi azok határait.[30]

Az Infotv. alapján személyes adat kezelhető akkor is, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna,[31] és a személyes adat kezelése az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.[32]

Az érdekmérlegelésen alapuló jogalap megjelenése indokolt mértékű rugalmasságot hoz a szabályozásba, és világos helyzetet teremt számos, jelenleg jogsértő, de jogkövetkezmény nélkül maradó adatkezelés számára. Ilyen jogsértések állhattak elő többek között a munkáltató adatkezelési gyakorlatában, amikor pontosan meghatározott jogalap nélkül ellenőrizte a munkavállalók tevékenységét, vagy a munkáltatók (akár a közigazgatási szervek, intézmények, akár magánvállalkozások) a szervezetnél dolgozók részére nyújtottak hírközlési szolgáltatásokhoz kapcsolódó szolgáltatásokat, vagy épp az oknyomozó újságíró tevékenységéhez kapcsolódóan.[33]

A Nemzeti Adatvédelmi és Információszabadság Hatóság vizsgálatai során az adatkezelés összes körülményét figyelembe véve, az egyedi jellemzők alapján állapítja meg annak jogszerűségét, illetve az esetleges jogosulatlan adatkezelés tényét. Mivel egy újonnan a törvénybe iktatott jogalapról beszélünk, ezért nincs egyelőre erre vonatkozó kikristályosodott gyakorlat hazánkban. Kérdéses, hogy milyen mértékben tekinthető elegendő felhatalmazásnak az e szakaszra való hivatkozás, erre vonatkozóan a hazai bíróságok eltérő álláspontra helyezkedhetnek majd az általuk vizsgált ügyekben, ahogyan egy, az adatkezelést vizsgáló

[30] Polyák Gábor – Szőke Gergely László: Elszalasztott lehetőség? Az új adatvédelmi törvény főbb rendelkezései, In.: Drinóczi Tímea (szerk.): Magyarország új alkotmányossága, Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, 2011, p. 160.
[31] Megjegyezzük, hogy az Infotv. ezen kitétele az érdekmérlegelés jogalapját feltételekhez köti, ami ellentétes az EU adatvédelmi irányelvével. (Lásd. bővebben Polyák – Szőke im.)
[32] Infotv. 6. § (1)
[33] Polyák – Szőke im. p. 160.

NAIH eljárás döntése is bizonytalannak tűnik egy erre alapuló adatkezeléssel kapcsolatban, ezért erre hivatkozva az adatkezelő a NAIH által kiszabható akár a 10 millió forintig terjedő bírságot is kockáztat.

Meg kell ugyanakkor jegyezni, hogy a NAIH joggyakorlata alapján nincs helye az érdekmérlegelésen alapuló adatkezeléseknek azokon a területeken, ahol az adatkezelés részleteit törvény szabályozza, mivel itt a jogalkotó már mérlegelte a különböző érdekek egyensúlyát. Tekintettel arra, hogy az egészségügyi ellátások során többnyire különleges adatokat kezelnek, és az ehhez kötődő adatkezelések egy része törvényi előíráson alapul, az érdekmérlegelési jogalap alkalmazása valószínűleg nem merülhet fel.

4. A célhoz kötöttség követelménye és az adatok minősége

A személyes adatok kezelésének legfontosabb garanciája, hogy arra minden esetben pontosan meghatározott, jogszerű cél teljesítése érdekében kerüljön sor (célhoz kötöttség). „*A célhozkötöttségből következik, hogy a meghatározott cél nélküli, „készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és -tárolás alkotmányellenes*."[34]

A célhoz kötöttség garanciáját az adatvédelmi törvény összetett követelményként fogalmazza meg:

- személyes adatot kezelni csak meghatározott célból,[35] jog gyakorlása és kötelezettség teljesítése érdekében lehet;
- a célhoz kötöttségnek az adatkezelés minden szakaszában teljesülnie kell, azaz az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelési célnak;
- csak az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas személyes adat kezelésére kerülhet sor;
- az adatkezelés nem haladhatja meg a cél megvalósulásához szükséges mértéket és időtartamot;
- ha az adatkezelés célja megszűnt, akkor a személyes adatot törölni kell;

[34] 15/1991. (IV. 13.) AB hat.

[35] A törvény példálózó felsorolást tartalmaz a lehetséges adatkezelési célokra vonatkozóan. A személyes adatot – akár az érintett hozzájárulásával, akár jogszabály alapján – különösen akkor lehet kezelni, ha ez közérdekű feladat vagy az adatkezelő törvényi kötelezettségének teljesítéséhez, az adatkezelő vagy az adatátvevő harmadik személy hivatalos feladatának gyakorlásához, az érintett létfontosságú érdekeinek védelméhez, az érintett és az adatkezelő között létrejött szerződés teljesítéséhez, az adatkezelő vagy harmadik személy jogos érdekének érvényesítéséhez, társadalmi szervezetek jogszerű működéséhez szükséges.

- a célhoz kötöttség technikai garanciájaként az adattárolás módjának alkalmasnak kell lennie arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.[36]

Fontos hangsúlyozni, hogy az adatvédelmi biztos és a Nemzeti Adatvédelmi és Információszabadság Hatóság következetes joggyakorlata alapján a célhoz kötöttség követelményét a már nyilvánosságra hozott személyes adatok tekintetében is alkalmazni kell, azaz a nyilvánosságra hozatal céljától eltérő más célból azok újrafelhasználása új adatkezelésnek minősül, amely csak megfelelő jogalappal lehetséges. Az adatkezelés során elérni kívánt cél kellően pontos meghatározása ezért problémás lehet egy összetett egészségügyi adatokat kezelő rendszer esetében.

Az adatvédelmi törvény a kezelt adatok minőségére vonatkozó követelményeket is meghatároz. Eszerint az adatok felvétele és kezelése tisztességes és törvényes kell, hogy legyen. A tisztességes adatkezelés követelménye a törvényesség mércéjénél szigorúbb, pontos tartalma azonban általános érvénnyel nem határozható meg. Az adatminőség követelményeként a törvény előírja továbbá, hogy a kezelt személyes adatok legyenek pontosak, teljesek és, ha szükséges, időszerűek.[37] Ez úgy biztosítható egészségügyi adatok tekintetében, ha az érintettnek lehetősége van megismerni a róla kezelt adatokat, és ha szükséges, akkor jelezheti a változásokat az adatkezelő felé.

5. Az érintett jogai az adatkezeléssel kapcsolatban

Az Infotv. személyes adataik kezelésével kapcsolatban sajátos jogokat biztosít az érintettek részére, amelyek az adatkezelés egész folyamatában biztosítják az információs önrendelkezési jog érvényesítésének lehetőségét. Az érintett jogait kizárólag törvény korlátozhatja, az adatvédelmi törvényben meghatározott közérdekű célokból.[38]

- Az érintettet nem csak az adatfelvételkor kell tájékoztatni az adatkezelés lényeges körülményeiről, hanem azokról az adatkezelés során is tájékoztatást kérhet. Az adatkezelő köteles a kérelem benyújtásától számított a lehető legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a kért tájékoztatást.

[36] Gálik, Mihály – Polyák Gábor: Médiaszabályozás, KJK-Kerszöv, 2005, p. 220.
[37] Infotv. 4. §
[38] Gálik – Polyák im. p. 223.

- Az érintett kérheti a valóságnak meg nem felelő személyes adatai helyesbítését. Ha a hiányos vagy téves adat jogszerűen nem korrigálható, akkor azt – törvény eltérő rendelkezése hiányában – törölni kell.
- A kötelező (törvényen alapuló) adatkezelések kivételével az érintett bármikor kérheti személyes adataink törlését, és ezzel az adatkezelés megszüntetését. Az adattörlés az adatok felismerhetetlenné tételét jelenti oly módon, hogy a helyreállításuk többé nem lehetséges. A törlésre irányuló kérelemnek nem feltétele, hogy az adatkezelés jogellenes legyen.[39]
- Az adatvédelmi törvény az érintett részére biztosítja továbbá a tiltakozás jogát, amelynek elsősorban az érdekmérlegelés alapján történő adatkezeléseknél van jelentősége. A tiltakozás az érintett olyan nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri. E jogával az érintett különösen akkor élhet, ha – a kötelező adatkezelés kivételével – a személyes adatok kezelése kizárólag az adatkezelő jogának vagy jogos érdekének érvényesítéséhez szükséges, valamint ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik. Az adatkezelő – az adatkezelés egyidejű felfüggesztésével – a tiltakozást köteles a kérelmet legfeljebb 15 nap alatt megvizsgálni, és annak eredményéről a kérelmezőt írásban tájékoztatni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést megszüntetni és az adatokat zárolni.[40]

6. További szabályok az adatkezeléssel kapcsolatban

6.1. Adatvédelmi nyilvántartás

Az adatkezelési tevékenység az Infotv. alapján hatósági nyilvántartásba vételhez, mint adminisztratív feltételhez kötött tevékenység. A személyes adatok kezelésének nyilvántartásba vételét az adatkezelő – a kötelező adatkezelés kivételével az adatkezelés megkezdése előtt – kérelmezi a Hatóságnál, és az eltérő célból történő adatkezelések önálló adatkezelésnek minősülnek, ezért külön be kell jelenteni még abban az esetben is, ha a kezelt adatok köre azonos.[41] A kötelező adatkezelés, valamint a NAIH hallgatása kivételével az adatkezelés a nyilvántartásba vételt megelőzően nem kezdhető meg, jelenleg a bejelentés nem

[39] Infotv. 14-17. §§
[40] Infotv. 21. §
[41] Infotv. 66.§(1) és (3)

kötött díjfizetéshez, mivel az annak mértékét meghatározó miniszteri rendelet még nem készült el.

6.2. Az adatbiztonság követelménye

Az adatkezelés akkor lehet törvényes és tisztességes, illetve az adatvédelmi követelmények csak akkor teljesíthetők, ha az adatkezelés technikai és szervezeti háttere azt lehetővé teszi. A törvény ezért előírja az adatbiztonság feltételeinek megteremtését, mely szabályoknak külön fejezetet szentelünk.

7. Az adatvédelem felügyeleti és szankciórendszere

Az adatvédelmi előírások megsértésére összetett szankciórendszert biztosít a jogrendszer. Az adatvédelmi követelmények megsértése esetére a jogalkotó mind reparatív, mind represszív jellegű szankciókat kilátásba helyez.

Amennyiben az adatkezelő az érintettet korlátozza jogainak gyakorlásában, akkor az érintett a jogait bírósági úton is érvényesítheti. A bírósági eljárásra vonatkozó rendelkezések az érintett részére kedvező helyzetet teremtenek, többek között a bizonyítási kötelezettség megállapításával. A bizonyítási eljárás általános szabályaival szemben nem az érintett, hanem az adatkezelő köteles bizonyítani azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel. Ha a bíróság a kérelemnek helyt ad, az adatkezelőt a tájékoztatás megadására, az adat helyesbítésére, törlésére, az érintett tiltakozási jogának figyelembevételére kötelezi. A bíróság elrendelheti ítéletének nyilvánosságra hozatalát, ha azt az adatvédelem érdekei és nagyobb számú érintett jogai megkövetelik.[42]

Mivel az adatvédelmet a Ptk. a személyhez fűződő jogok közé sorolja, ezért azzal kapcsolatban az általános polgári jogi szankciók is igénybe vehetők. Az adatvédelmi törvény ugyanakkor az általánostól eltérő kárfelelősségi mércét tartalmaz.

Az adatvédelem büntetőjogi következményeit olyan ún. keretténállás szabályozza, amelyek a magatartás jogellenes jellegét az általános és az adott adatkezelésre vonatkozó ágazati adatvédelmi rendelkezések alapján rendelik meghatározni.[43]

Az adatvédelem területét emellett széles jogkörökkel rendelkező felügyelő hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) is felügyeli.

[42] Infotv. 22. §
[43] Gálik – Polyák im. p. 224.

7.1. Kártérítési felelősség és sérelemdíj

Az Infotv. az adatvédelmi követelmények megszegésével okozott károkért viselt felelősséget az általános polgári jogi felelősségnél szigorúbban szabályozza. A törvény szerint az adatkezelő az érintett adatainak jogellenes kezelésével vagy a technikai adatvédelem követelményeinek megszegésével másnak okozott kárt köteles megtéríteni. Ha pedig az adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett az adatkezelőtől sérelemdíjat követelhet. A kártérítési felelősség és a sérelemdíj megfizetésének kötelezettsége alól kizárólag akkor mentesül, ha bizonyítja, hogy a kárt az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.[44] Nem kell megtéríteni a kárt annyiban, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.[45]

7.2. Büntetőjogi felelősség

A Btk. Személyes adattal visszaélés című tényállása (Btk. 219. §) egyes adatvédelmi követelmények súlyosabb megszegésével szemben büntetőjogi szankciók alkalmazását rendeli. A bűncselekményt az követi el, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelmet okozva:

- jogosulatlanul vagy a céltól eltérően személyes adatot kezel,
- az adatok biztonságát szolgáló intézkedést elmulasztja, illetve
- aki az érintett tájékoztatására vonatkozó kötelezettségének nem tesz eleget, és ezzel más vagy mások érdekeit jelentősen sérti (a haszonszerzési céltól függetlenül).
- Súlyosabban büntetendő a különleges személyes adatokkal való visszaélés, valamint hivatalos személyként, közmegbízatás felhasználásával elkövetett bűncselekmény.

7.3. A Nemzeti Adatvédelmi és Információszabadság Hatóság

Az új adatvédelmi szabályozás kétségkívül legtöbb vitát kiváltó eleme az adatvédelem és információszabadság felügyeleti rendszerének újraszabályozása volt. A szabályozás lényege, hogy – megtartva több adatvédelmi biztosi jogosítványt – új hatósági jogkörökkel és bírságolási joggal kiegészülve felügyeleti hatóság jött létre, amelynek elnökét a

[44] Ez a szabályozás az adatkezelő felelősségét a polgári jog ún. veszélyes üzemi kárfelelősségi mércéje szerint szabályozza
[45] Infotv. 23. §

miniszterelnök javaslatára a köztársasági elnök nevezi ki. Az új hatóság 2012. január 1-i felállítása miatt az adatvédelmi biztos intézménye a hivatalban lévő adatvédelmi biztos mandátumának mintegy félidejénél megszűnt.[46]

A hatóság autonóm államigazgatási szerv, tevékenységéről minden év március 31-ig beszámol az Országgyűlésnek, és a szervezetrendszerrel kapcsolatban több rendelkezés is biztosítja a formális függetlenséget, pl. az elnök megbízása meglehetősen hosszú időre, kilenc évre szól, és a visszahívás feltételei korlátozottak és pontosan körülhatároltak. A törvény részletesen meghatározza a hatóság feladat- és hatásköreit és egyes hatásköröknél részletezi az eljárási szabályokat.

A hatóságnál bejelentéssel bárki *vizsgálatot* kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével, illetve a közérdekű adatok (közérdekből nyilvános adatok) megismeréséhez fűződő jogok gyakorlásával kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.[47] A hatóság – néhány kivételtől eltekintve – köteles a vizsgálatot lefolytatni,[48] az eljárás során a korábbi ombudsman jellegű hatáskörökkel azonos vizsgálati jogok illetik meg.[49] A vizsgálat nem minősül közigazgatási hatósági eljárásnak, arra a Ket. szabályait nem kell alkalmazni.[50] A vizsgálat végeztével – 2 hónapon belül – a hatóság felhívhatja az adatkezelőt a jogsérelem orvoslására, amelynek megtételéről, vagy arról, hogy az abban foglaltakkal nem ért egyet, az adatkezelő 30 napon belül köteles a hatóságot tájékoztatni.

Amennyiben ez nem vezet eredményre, úgy a hatóság ajánlást tehet a szerv felügyeleti szervének,[51] nyilvános jelentést készíthet az ügyről, illetve adatvédelmi hatósági eljárást kezdeményezhet vagy titokfelügyeleti hatósági eljárást kezdeményezhet.[52] E hatósági eljárást egyébként a hatóság felhívás és/vagy ajánlás kibocsátása nélkül is kezdeményezheti.

[46] Magyarország ezzel a jogalkotói megoldással az Európai Bíróság ítélete alapján megsértette az Európai Unió adatvédelmi irányelvének tagállami hatóságok függetlenségére vonatkozó szabályait.
[47] Infotv. 52. §
[48] A vizsgálat lehetséges elutasításának oka lehet pl. az, ha az ügyben bírósági eljárás van folyamatban. A további szabályokat ld. 53. § (2)-(3)
[49] Infotv. 54. §
[50] Infotv. 52. § (2)
[51] A felügyeleti szerv számára a jogsérelemre való közvetlen felhívás nélkül is tehet ajánlást.
[52] Infotv. 56, 58. §§

A hatóság ugyancsak a vizsgálat eredményeként ajánlást tehet jogszabály módosítására is, amennyiben a jogsérelem vagy annak közvetlen veszélye a jogi szabályozás hiányosságára vagy fölösleges, nem egyértelmű rendelkezésére vezethető vissza.[53]

Akár a vizsgálat eredményeként, akár vizsgálati eljárás nélkül is a NAIH *adatvédelmi hatósági eljárást* indít, ha valószínűsíthető a személyes adatok jogellenes kezelése, és a jogellenes adatkezelés személyek széles körét érinti, különleges adatokat érint, vagy nagy érdeksérelmet vagy kárveszélyt idézhet elő.[54] Az eljárás kizárólag hivatalból indítható, az akkor sem minősül kérelemre indult eljárásnak, ha bejelentésen alapuló vizsgálat előzte meg.[55]

Az adatvédelmi hatósági eljárásban szankciórendszere az EU adatvédelmi irányelvén alapul, kiegészítve a bírságolás lehetőségével. A hatóság határozatban:

- elrendelheti a valóságnak nem megfelelő személyes adat helyesbítését,
- elrendelheti a jogellenesen kezelt személyes adatok zárolását, törlését vagy megsemmisítését,
- megtilthatja a személyes adatok jogellenes kezelését vagy feldolgozását,
- megtilthatja a személyes adatok külföldre továbbítását,
- elrendelheti az érintett tájékoztatását, ha azt az adatkezelő jogellenesen tagadta meg,
- 100.000 Ft-tól 10.000.000 Ft-ig terjedő bírságot szabhat ki,[56]
- valamint a hatóság elrendelheti a határozat – az adatkezelő azonosító adatainak közzétételével történő – nyilvánosságra hozatalát, ha azt az adatvédelem érdekeinek, illetve nagyobb számú érintett jogainak védelme ezt megköveteli.[57]

A bírság összegével kapcsolatban megjegyezzük, hogy a kiszabható legnagyobb összeg európai összehasonlításban és egyes adatkezelőkkel: például multinacionális cégekkel szembeni visszatartó erőt figyelembe véve is meglehetősen alacsony.[58]

A fent részletezett eljárások mellett a hatóság többek között javaslatot tehet az adatvédelmet és információszabadságot érintő jogszabályok megalkotására és módosítására, véleményezi a

[53] Infotv. 57. §
[54] Infotv. 60. § (4)
[55] Ekkor azonban a bejelentőt az adatvédelmi hatósági eljárás megindításáról, illetve befejezéséről értesíteni kell. Ld. Infotv. 60. § (1)-(3), (5)
[56] A hatóság a bírság kiszabása során figyelembe veszi a jogsértéssel érintettek körének nagyságát, a jogsértés súlyát és a jogsértés ismétlődő jellegét. Infotv. 61. § (4)
[57] Infotv. 61. § (1)-(3)
[58] Polyák – Szőke im. pp. 168-169.

feladatkörét érintő jogszabályok tervezetét; általános jelleggel vagy meghatározott adatkezelő részére ajánlást bocsát ki; de akár az adatkezelő kérelmére adatvédelmi auditot is lefolytathat.

IV. AZ EURÓPAI UNIÓ ADATVÉDELMI REFORMJA

E fejezet célja röviden áttekinteni az Európai Unió jelenleg hatályos adatvédelmi irányelvét, majd vázolni az elfogadás előtt álló adatvédelmi reformcsomagjának legfontosabb újdonságait, mely olyan új – részben rendeleti formája miatt valamennyi, a közösségen belül működő adatkezelőre kötelező – előírásokat és adatvédelmi elveket tartalmaz, melyek a közeljövőben hazánkban is valamennyi belső adatvédelmi felelős számára alapvető fontosságúak lesznek.

1. Az Európai Unió adatvédelmi irányelve

A jelenleg hatályos uniós jogforrások közül a legfontosabb az Európai Parlament és a Tanács *95/46/EK irányelve* (Irányelv) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Bár az irányelvet 1995-ben fogadták el, az csupán 1997-ben lépett hatályba, mivel egyes kötelező részletszabályai miatt a tagállamoknak felül kellett vizsgálniuk adatvédelmi törvényeiket.

1.1. Rendeltetés és alapfogalmak

Mint a preambulumból kiolvasható, az irányelv megalkotása mellett szóló egyik legfontosabb szempont a *tagállamok közötti szabad adatáramlás* feltételeinek biztosítása volt, az adatvédelem értékeinek megtartása, minden tagállamban azonos szinten való garantálása mellett. Mivel a tagállamok belső jogukban kötelesek a közösségi jog szabályait követni, az évek során az adatvédelem szabályozása körében is az EU minden tagja az adatvédelmi irányelvhez igazodó, harmonizált nemzeti szabályozást alakított ki. Így elmondhatjuk, hogy a szabályozási koncepció, a jogpolitikai rendeltetés és az alapfogalmak tekintetében az irányelv nem különbözik lényegesen a hazai szabályozás fentebb ismertetett elemeitől. A személyes adat fogalma, az adatalany, az adatkezelő, az adatfeldolgozó szerepe, az adatalany jogai és a rendelkezésre álló jogorvoslatok tekintetében a magyar és az uniós jog azonos felfogást követ. Az adatkezelés jogalapjai tekintetében is ma már fedésbe hozható a magyar belső jog és a közösségi szabályozás, noha hosszú időn keresztül ezen a téren voltak lényeges eltérések is. Mivel a hazai és az uniós jog hasonlóan szabályozza a személyes adatok határokon átlépő áramlását, ezért nemzetközi jellegére tekintettel azt itt, az Irányelv elemzésével mutatjuk be részletesen.

1.2. Adattovábbítás az EU tagállamai között

Az adatvédelem klasszikus elvei és szabályai szerint személyes adat külföldre irányuló adattovábbításhoz, illetve külföldön történő adatkezeléshez, vagy külföldi adatfeldolgozó részére történő átadás esetében az adatalany beleegyezésére vagy törvény felhatalmazására van szükség. Vizsgálandó továbbá a célország – és az esetleges közbenső harmadik országok – adatvédelmi szabályainak és rendszerének milyensége. Az adattovábbítás csak akkor engedélyezhető, ha a hazai szabályoknak megfelelő törvényes adatminőség külföldön is biztosított.

Az Unió szervezetének és működésének logikájából, a szabályok harmonizáltságából azonban más következik. A 28 tagállam egymás közötti viszonyában nem kell külön vizsgálni az adatvédelmi rendszerek megfelelőségét, mert azt az Irányelv kötelező jellege, illetve ennek alapján a nemzeti szabályozások összehangoltsága – elvileg – automatikusan biztosítja.

1.3. Harmadik országba történő adattovábbítás

Az Európai Unión kívülre, azaz harmadik országba irányuló adattovábbítást az Irányelv sokkal részletesebben szabályozza. Az alapvető követelmény a védelmi szintek egyenlősége, azaz a célország adatvédelmi rezsimje az EU-tagállamok – illetve a közösségi jog – adatvédelmi elveivel azonos biztonságot kell, hogy garantáljon a személyes adatok számára. Ennek megállapítása és kimondása az EU Bizottságának hatáskörébe tartozik.

Amennyiben ezek a követelmények nem teljesülnek, a tagállamok kötelesek megakadályozni, hogy az adott típusú adatok a szóban forgó harmadik országba továbbításra kerüljenek. Az Irányelv a tagállamok és a Bizottság számára még szignalizációs kötelezettséget is előír. Ennek alapján a kötelezettek értesítik egymást azokról az esetekről, amelyekben úgy vélik, hogy valamely harmadik ország nem biztosít megfelelő védelmi szintet a személyes adatoknak.

Amennyiben a Bizottság azt állapítja meg, hogy valamely harmadik ország nem biztosítja a személyes adatok számára az EU jogrendszere által előírt és elvárt védelmi szintet, a tagállamok csak szigorú konjunktív feltételek mellett engedélyezhetik az adatok továbbítását.

Egyes adatkezelések esetében eseti adattovábbítási engedély kiadására is sor kerülhet, amennyiben a harmadik ország szerződésben vállal kötelezettséget arra, hogy az adatkezelő

megfelelő garanciákat teremt az egyének magánéletének, alapvető jogainak és szabadságainak védelmére, továbbá az érintett kapcsolódó jogainak gyakorlására.

Különösen fontos ezért például az online adatkezelésekkel kapcsolatban gyakran felmerülő felhő alapú szolgáltatások pontos ismerete (már azok igénybevétele, az adatkezelés megkezdése előtt), mivel ha az adatokat rögzítő, továbbító szerverek az Unión kívül helyezkednek el, akkor nem feltétlenül biztosított a személyes adatok védelme.

2. Az szabályozási reform okai

Az elmúlt évtized során a technológiai és társadalmi háttér változása újabb és egyre nagyobb kihívások elé állította a 90-es évek végére kialakult, jelenleg is hatályban lévő európai adatvédelmi szabályozást. A jogszabályi reformhoz vezető legfontosabb technológiai és társadalmi újdonságnak az internethasználat, valamint a kétezres évek közepétől kezdődően a web 2.0-es szolgáltatások folyamatos elterjedése tekinthető. Ezekkel alapjaiban megváltozott a tartalomszolgáltatás jellege, valamint előtérbe kerültek a felhasználók által generált tartalmak, például a személyes profiloldal egy közösségi oldalon, a blogbejegyzés, vagy akár az audiovizuális tartalmak megosztása. Amennyiben ezek a tartalmak más érintettek személyes adatainak nyilvánosságra hozatalával járnak, felhasználók tömege kerülhet adatkezelői pozícióba,[59] és válik így az adatvédelmi szabályozás kötelezettjévé.

A felhasználók által készített és közzétett tartalmaknak köszönhetően az online adatmennyiség korábban elképzelhetetlen mértékben és ütemben bővül. A technológiai szaksajtó a „Big Data” kifejezéstől hangos, amely az adatvédelmi szakirodalomban is megjelent. A hatalmas és gyorsuló ütemben bővülő adatmennyiség hasznosítása komoly üzleti lehetőségeket rejt, így középpontba került az adatbányászati technológiák fejlesztése is. E jelenség magánszférára gyakorolt hatása nem megkerülhető az adatvédelemről szóló szakmai viták során.

Nagymértékben változik a személyes adatok tárolásának módja is. A felhőalapú szolgáltatások terjedésével az érintettek (sőt, sokszor az adatkezelők is) minden korábbinál jobban elvesztik az adataik feletti „fizikai” ellenőrzés lehetőségét.[60] Érdemes figyelembe venni azt is, hogy az új technológiák és szolgáltatások új felhasználói viselkedésmintákkal

[59] Van Alsenoy, Brendan - Ballet, Joris – Kuczerawy Aleksandra – Dumortier Jos: Social networks and web 2.0: are users also bound by data protection regulations? Identity in the Information Society, 2009/1, doi: 10.1007/s12394-009-0017-3 [2015.03.20.] p. 70.
[60] Tene, Omer: Privacy: The new generations, International Data Privacy Law 20011/1. doi: 10.1093/idpl/ipq003 [2015.03.20.] pp. 16-20.

párosulnak. A felhasználók új generációjának a magánszférával kapcsolatos attitűdje eltér a korábbi generációiétól.[61]

Ezekre a tendenciákra reagálva elkerülhetetlenné vált egy az adatvédelmi jogszabályokat érintő Európai Uniós reform, amelynek keretében az EU új jogszabálycsomaggal kívánja felváltani a jelenleg hatályban lévő adatvédelmi irányelvet és kerethatározatokat.

3. Az Európai Bizottság adatvédelmi rendelet-tervezete[62]

A jogalkotási folyamat legfontosabb lépése az Európai Bizottság által 2012-ben kiadott általános adatvédelmi rendelet-tervezet[63] volt, amely számos újítást javasol az adatvédelmi jog területén. Ezek az újítások egy új generációs szabályozás alapjainak a megteremtését is jelentik, amely jelentős hangsúlyeltolódást hoz az adatvédelem területén. A javaslatot az Európai Parlament jogszabályalkotó bizottsága (LIBE) tovább szigorította, és a Parlament 2014 tavaszán már ezt a szigorított tervezetet küldte meg az Európai Tanácsnak. A jogszabály várhatóan még számos vita középpontjában áll majd, mivel a rendeleti forma határozottan beavatkozik a tagállami jogokba. Ennek következtében egyelőre nem lehet tudni, hogy mikor léphet hatályba az új szabályozás, azonban annak hatása jól érzékelhető az Unió jogalkotásának más területein is, az új adatvédelmi elveket már alkalmazzák az uniós jogban.

- 1. A szabályozás súlypontja az érintettek jogainak erősítése, további szélesítésével szemben az adatkezelők kötelezettségeinek növelése felé látszik eltolódni. Úgy tűnik, hogy az információs önrendelkezési jog egyéni jogérvényesítést és az érintett tudatosságát feltételező koncepciója mellett fokozottan előtérbe kerül az adatkezelők kötelezettségeit és felelősségét (elszámoltathatóságát) kidomborító megközelítés. Az Európai Bizottság az adatkezelők feladatává teszi a megfelelő policyk (eljárásrendek, szabályzatok) megalkotását, elfogadását, adatkezelési dokumentáció vezetését, adatbiztonsági intézkedések megtételét, adatvédelmi hatásvizsgálat lefolytatását, és egyes esetekben belső adatvédelmi felelős kijelölését.[64]

[61] Tene,Omer im. pp. 15, 21, 23. A felhasználói hozzáállás részletesebb vizsgálatához további kutatások szükségesek – amely elsősorban az elmúlt években készült közvélemény-kutatások eredményeinek feldolgozását igényli.
[62] E témakörről ld. részletesen Domokos N. Márton: Az EU új adatvédelmi szabályozásának várható következményei a gyakorlatban. Infokommunikáció és jog, 55 (2013:1). pp. 58-63.
[63] Európai Bizottság: Javaslat - Az Európai Parlament és a Tanács Rendelete a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (általános adatvédelmi rendelet) Brüsszel, 2012.1.25. COM(2012) 11 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:HU:PDF (2014.05.10)
[64] Rendelettervezet, IV. fejezet

- 2. Egy másik fontos jellemző a szabályozási terhek differenciálása az adatkezelők valamely jellemzője alapján. A Rendelettervezet az egyes, részletesen szabályozott kötelezettségeket csak bizonyos adatkezelők számára írja elő. A tervezet egyrészt az adatkezelés jellege (fő- vagy járulékos tevékenység) és kockázata alapján, másrészt az adatkezelő mérete alapján differenciál.
- 3. A szabályozás (újra) célul tűzi ki a technológia szabályozását, formálását. A jogalkotó felismerte ugyanis, hogy a technológia közvetlen hatással van a személyes adatok védelmére és az adatbiztonságra vonatkozó jogi követelményekre.[65] Hiába van pl. egy szervezetnél az adatvédelmi jogszabályoknak egyébként megfelelő belső szabályzat arra, hogy bizonyos adatokhoz csak meghatározott szervezeti egységek férhetnek hozzá, ha ezt nem támogatják az iktatórendszer jogosultsági beállításai, esetleg nem is lehet megadni jogosultsági korlátozásokat, akkor e szabály a gyakorlatban nem fog érvényesülni.

A technológia azonban kifejezetten segítheti is a magánszféra védelmét; a privátszférát erősítő technológiák[66] (PET) létrejöttének egyik oka, hogy a szabályozás, önszabályozás, és a jogalkalmazás sem tudnak elegendő védelmet nyújtani a felhasználóknak a tömegesen előforduló jogellenes adatkezelési gyakorlat, és az egyre újabb műszaki megoldások ellen.[67]

A fentiekre tekintettel – a PET koncepcióját is magába olvasztva – egyre többször jelenik meg jogszabályi követelményként is az ún. „Privacy by Design" elve, amely lényegében azt jelenti, hogy valamely új technológia illetve eljárás fejlesztése és/vagy bevezetése során már a tervezési szakasztól kezdve figyelemmel kell lenni az adatvédelemre vonatkozó jogi, és az adatbiztonságra vonatkozó jogi és technikai követelményekre, valamint műszakilag biztosítani kell az azoknak való megfelelést. Szintén új szabályként jelenik meg az új európai szabályozásban bizonyos szervezetek számára az adatvédelmi hatásvizsgálat (Data Protection Impact Assessment) követelménye, amely valamely intézkedés egyének magánszférájára gyakorolt hatásának elemzését jelenti.[68]

4. A fenti jellemzőkből következik az intézményi belső szabályozás szerepének erősödése. A Rendelettervezet jelen formában való elfogadásának véleményünk szerint egyértelműen az a várható hatása, hogy az egyes, különösen a nagyobb, vagy a személyes adatok kezelését

[65] E gondolatnak az első jogszabályi megfogalmazása már 1997-ben megjelent Németországban. Ld. Erről Jóri András: Adatvédelmi kézikönyv. Osiris, 2005, p. 65.
[66] Privacy Enhancing Technology (PET)
[67] Székely Iván: Privátszférát erősítő technológiák. In: Információs Társadalom, 2008. VIII. évf. 1. szám, http://pet-portal.eu/files/oldfiles/articles/2008/02/InfTars_PET.pdf [2015.03.20.], p. 22.
[68] Rendelettervezet, 23. és 33. cikk

elsődleges tevékenységként végző adatkezelők a korábbinál lényegesen nagyobb hangsúlyt kell, hogy fektessenek az adatvédelmet érintő folyamataik és annak várható hatásainak elemzésére, majd e folyamatok megtervezésére, dokumentálására és (belső) felügyeletére.

A Rendelettervezet jelenleg a Tanács általi elfogadásra vár – az Európai Parlament már nagy arányban megszavazta a koncepciót ez év tavaszán. Uniós adatvédelmi szakértők szerint az elfogadásra ettől függetlenül még éveket kell várni, legkorábban jövőre, 2015-ben várható a Rendelet megszületése, amely további két-három év múlva léphet hatályba. Addig is szükséges megismerni és felkészülni a változásokra, mert jelentőségüket tekintve alapjaiban változtathatják meg az eddig kialakult adatkezelési gyakorlatokat. A továbbiakban az egyes magánszférát védő új elvek, illetve eszközök, módszerek kerülnek bemutatásra.

4. A privátszférát erősítő technológiák[69]

A „Privacy Enhancing Technologies" (PETs) kifejezésre nem található általánosan elfogadott meghatározás,[70] az az egyén identitását, személyazonosságát védő technikai és szervezeti megoldások gyűjtőneve.[71] A nemzetközi jogirodalom egy gyakran hivatkozott megfogalmazása szerint a PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az információs magánszférát a személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, anélkül, hogy csökkentené az információs rendszer funkcionalitását.[72] Alkalmazásuknak különös jelentősége van minden olyan technológiai fejlesztés során, amelyek esetében magányszemélyek (érintettek) személyes adatait gyűjtik, elemzik, hasznosítják, tehát adatkezelés történik.

Ezen eszközök alapvető célja, hogy ne csak az adatokat általában, hanem az adatalanyokat, az érintetteket is védjék a visszaélések ellen, és elősegítsék az információs önrendelkezéshez való alkotmányos alapjog érvényesíthetőségét. A megoldások nem jogi védelmet nyújtanak,

[69] E témakörről ld. részletesen Kiss Attila: A privátszférát erősítő technológiák, *Infokommunikáció és jog*, 56 (2013:3).
[70] London Economics: *Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security*, 2010. 2. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [2015.03.20.]
[71] Burkert, Herbert: *Privacy-Enhancing Technologies: Typology, Critique, Vision*. In: Agre, Philip E. – Rotenberg, Marc (szerk.): *Technology And Privacy: The New Landscape*. MIT Press, 1997. p. 125.
[72] Blarkom, Gilles W. van - Borking, John J. - Olk, Eddy (szerk.): *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*. The Hague, PISA Consortium, 2003, p. 36

de alkalmazásuk tömegessé válása és ennek következményei miatt a jogi szabályozás tárgyaivá válhatnak.[73]

A privátszférát erősítő megoldások fejlesztésének egyik célja az, hogy a mai számítástechnikai megoldásokat segítségül hívva, azok összes előnyét megtartva, magával a technológiával mérsékeljék a privátszférát fenyegető káros hatásokat, megakadályozzák a jogszerűtlen adatkezeléseket, döntési lehetőséget biztosítsanak a felhasználóknak saját adataik sorsáról,[74] így helyreállítsák a felhasználók online szolgáltatásokba vetett bizalmát. A privátszférát erősítő megoldások egyrészt e megfigyelők ellenőrzése nélkül, a magánszféra megőrzése mellett teszi lehetővé az online kommunikációt, böngészést, internetes tranzakciókat,[75] másrészt ellenőrizési lehetőséget ad az érintetteknek, hogy az adatkezelők birtokában mely személyes adatok vannak, hogy azok felett a számukra biztosított jogi lehetőségekkel élve rendelkezhessenek.[76]

A Rendelettervezetben bár nevesítve nem szerepelnek a megoldások, de az új adatvédelmi célok érvényesítésében a beépített adatvédelem (Privacy by Design) elvnek kiemelt szerepet tulajdonít az európai jogalkotó, melynek egyik legfontosabb eleme a PET-ek alkalmazása és azok terjedésének elősegítése. E megoldásokat emellett külön nevesítik az egészségügyi adatkezelésre vonatkozó Európai Uniós jogszabály tervezetek is.

A privátszférát védő megoldások céljaként négy alapvető elvárást lehet megfogalmazni: az anonimitást, a pszeudonimitást, a megfigyelhetetlenséget, és az összeköthetetlenséget. Aktív felhasználók esetében ezek konjunktív teljesítésülése a cél, míg passzív felhasználók, mint érintettek esetében csak az első két elvárás kell, hogy érvényre jusson:

- Az anonimitás lényege, hogy „az adatokat, illetve az adatok kezelésével járó eseményeket, cselekvéseket nem tudjuk egy meghatározott személlyel kapcsolatba hozni.”
- A pszeudonimitás jelentése, hogy „van alanya az adatoknak, de az alany valós kilétét nem ismerjük; egy valós adatalanynak több fedőneve, profilja, virtuális személyisége is lehet.”

[73] Jóri, 2005, i. m., pp. 18-19.
[74] Társaság a Szabadságjogokért: PET Portál és Blog - Az első magyar fórum a privátszférát erősítő technológiákról http://tasz.hu/adatvedelem/33 [2015.03.20.]
[75] Goldberg, Ian: *Privacy-enhancing technologies for the Internet, II: Five years later*. In: Dingledine, R. – Syverson P. (szerk.): *Privacy Enhancing Technologies. Second International Workshop, PET 2002 San Francisco, CA, USA, April 14–15, 2002 Revised Papers.* Springer-Verlag, 2002. 1. http://freehaven.net/anonbib/papers/petfive.pdf [2015.03.20.]
[76] Társaság a Szabadságjogokért, im.

- A megfigyelhetetlenség alatt azt értjük, hogy „egy illetéktelen harmadik fél ne észlelhesse, hogy valaki egy távoli erőforrást használ, például nyílt hálózati kapcsolaton keresztül egy internetes folyóirat oldalait tölti le.”
- Az összeköthetetlenség akkor áll fenn, ha „az illetéktelen harmadik fél akár észlelheti is a távoli erőforrás valaki általi használatát, azonban nem tud kapcsolatot teremteni az aktuális használat és az ezt megelőző vagy követő használatok között. Az összeköthetetlenség tehát megakadályozza a felhasználók szokásainak megfigyelését, profilírozását.”[77]

Meg kell jegyezni, hogy a PET megoldások használata korántsem tömeges. A lassú elterjedés okai között meg kell említeni, hogy a PET-ek használatához szükséges informatikai, technológiai ismeretek többnyire hiányoznak az átlagfelhasználóknál,[78] illetve problémát jelenthet az is, hogy általában nincs kézzelfogható eredménye a privátszférát erősítő technológiák alkalmazásának, ezért alacsony azok népszerűsége, kevésbé tudatosul egy átlagos felhasználóban, ha visszaéltek személyes adataival, mintha a fizikai világban érné kár.[79] Ezeken a PET megoldások előnyeinek népszerűsítésével, a felhasználóbarát kialakítással, és a könnyű telepíthetőséggel lehetne segíteni.[80]

5. Kísérlet egy új szemlélet elterjesztésére: a beépített adatvédelem elve[81]

A Privacy by Design, azaz a beépített adatvédelem kidolgozása és a jog világában való elterjedése a 90-es években kezdődött, de mára vált igazán kiforrott elméleti megoldássá. A szakirodalom először egyértelműen a privátszférát erősítő technológiákkal foglalkozott, a beépített adatvédelem elve a PET eszközökkel kapcsolatos elméletek továbbgondolásaként, elvi szintre emeléseként jelent meg.

Egyes nézetek szerint a Privacy by Design lényegében egy filozófia, egy megközelítési mód, amely alapján a magánszféra-védelem szempontjait integrálni kell a különböző technológiák követelményrendszerébe, azaz az adatvédelmi szabályozás elveit be kell építeni az adatkezelési technológiákba, mind a tervezés, mind a működtetés során. A Privacy by Design elv abból indul ki, hogy az informatikai infrastruktúra nagymértékben meghatározza az

[77] Székely i. m., p. 25.
[78] Kolter, Jan Paul: *User-Centric Privacy. A Usable and Provider-Independent Privacy Infrastructure.* University of Regensburg, 2009. p. 2. http://www.ics.uci.edu/~kobsa/phds/kolter.pdf [2015.03.20.]
[79] Thiesse, Frederic: RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems*, 2007/2. 226.
[80] Goldberg, 2007, i. m., 10-11.
[81] E témakörről ld. részletesen Szőke Gergely László, Böröcz István: A beépített adatvédelem (privacy by design) elve, *Infokommunikáció és jog*, 56 (2013:3).

adatkezelő tényleges cselekvési szabadságát és lehetőségeit. Az elv ugyan eredetileg kifejezetten az infokommunikációs technológia kapcsán jelent meg, később azonban ez kiterjedt az üzleti folyamatok, sőt a fizikai tervezés területére is.[82] Az európai szabályozási tervekbe a beépített adatvédelem elve már kifejezetten e módosult hatókörrel került be: a követelményt nem csak a technológia kialakítása, de általában az adatkezelési folyamatok megtervezése során figyelembe kell venni, a gyakorlatban persze e kettő között igen szoros az összefüggés.

A Privacy by Design részletszabályainak kidolgozása alapvetően Ann Cavoukiannak, a kanadai Ontario állam adatvédelmi biztosának köszönhető. Az általa megalkotott hét alapelv több mint 30 nyelven érhető el, köztük magyarul is:[83]

- 1. *Reakció helyett proaktivitás, utólagos orvoslás helyett megelőzés.* Fontos kiindulópont, hogy előre számolni kell a személyek magánéletébe beavatkozó eseményekkel, és meg kell akadályozni ezek bekövetkeztét, azaz a káros hatásokat nem utólag kell enyhíteni, hanem meg kell előzni.
- 2. *Alapértelmezett adatvédelem.* Lényeges momentum, hogy automatikus beállításokkal (úgy hogy az egyénnek ezért semmilyen külön lépést nem kell tennie) kell maximális védelmet biztosítani a magászféra számára számítástechnikai környezetben vagy üzleti felhasználás során.
- 3. *Tervezés során beépített adatvédelem.* A Privacy by Design elv központi elemét adja az a követelmény, hogy a privacy védelem szempontjait nem utólagos kiegészítésként, hanem már a tervezéstől kezdve figyelembe kell venni, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy a funkcionalitást korlátozná.
- 4. *Teljes működőképesség.* A Privacy by Design elvének alkalmazása integrálja az összes jogos érdeket és célt úgy, hogy a veszteségek és a profit ne csak kiegyenlítsék egymást, hanem a végeredmény pozitív mérleggel záruljon.
- 5. *Teljes életciklusra kiterjedő védelem.* Ha a Privacy by Design már az adatgyűjtés megkezdését megelőzően érvényesül, a hatékony biztonsági előírások az adatkezelés teljes ciklusát átfogják a kezdettől a végig. Az elv alkalmazása tehát elősegíti egy információ életútjának megfelelő kezelését a keletkezésétől a megszűnéséig.

[82] Cavoukan, Ann: *Privacy by Design. …Take the challenge.* Information and Privacy Commissioner of Ontario, 2009. 3. http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf [2015.03.20.]
[83] Cavoukan, Ann: Privacy by Design. A hét alapelv (fordította Péterfalvi Attila és Sziklay Júlia). Ontario (Canada) Információs és Adatvédelmi Biztosa, 2013, http://www.privacybydesign.ca/content/uploads/2013/03/7foundationalprinciples-hungarian.pdf [2015.03.20.]

- 6. *Láthatóság és átláthatóság.* A Privacy by Design elv az adatkezelés valamennyi résztvevőjét az alkalmazott technológiától vagy üzleti megoldástól függetlenül arra sarkallja, hogy a megígért és kinyilvánított céloknak megfelelően járjon el (melyet független értékelésnek is alávethet). Az adatkezelési műveletek így a szolgáltató és a felhasználó számára is átláthatóak.
- 7. *A felhasználó magánszférájának tisztelete.* A Privacy by Design elve az adatkezelőtől egyértelműen azt követeli meg, hogy az érintett adatvédelmi érdekeit tartsa a legfontosabbnak, szigorú adatvédelmi előírások, megfelelő jelzések és felhasználóbarát megoldások használatával.[84]

Álláspontunk szerint a gyakorlati alkalmazás jelentős nehézséget okoz, mivel a megfogalmazott elvek sokkal inkább egy szemléletet, hozzáállást tükröznek, mintsem olyan normatív követelményrendszert, amelynek betartása vagy be nem tartása könnyedén megállapítható. A beépített és alapértelmezett adatvédelem elvének jogszabályi megjelenése az új európai adatvédelmi keretrendszerben várhatóan számos konkrét jogalkalmazási nehézséget vet majd fel, különösen a negyedik alapelv, a teljes működőképesség. Az elv lényege, hogy a szolgáltatás magában foglalja a különböző érdekeket (elsősorban gazdasági, politikai, valamint adatvédelmi), és a működés során pozitív eredményt hoz, mind gazdasági, mind pedig adatvédelmi szempontból, vagyis az érdek-összeütköztetés a szolgáltató számára anyagi, a felhasználó számára pedig magánszféra-védelem szempontjából pozitív kimenetelű.

A beépített adatvédelem fontosságát Peter Hustinx európai adatvédelmi biztos is kiemelte a határokon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről szóló európai parlamenti és tanácsi irányelvről szóló véleményében. Hustinx szerint minden egészségügyi ellátórendszer kialakításának és megvalósításának részét kell, hogy képezze, különösen az e-egészségügyi alkalmazások tekintetében.[85]

6. Adatvédelmi hatásvizsgálat[86]

A Privacy Impact Assessment (az EU jogi terminológiában Data Protection Impact Assessment, DPIA) az angolszász jogrendszerekben kialakult eljárás, amely a magánszférát

[84] Cavoukan, Ann: Privacy by Design. A hét alapelv, p. 2.
[85] Az európai adatvédelmi biztos véleménye a határokon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről szóló európai parlamenti és tanácsi irányelvről, 2009/C 128/03, 2009, http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52009XX0606%2803%29&rid=17#ntc12-C_2009128HU.01002001-E0012 [2015.03.20.]
[86] E témakörről ld. részletesen Balogh Zsolt György, Böröcz István, Kiss Attila, Polyák Gábor, Szőke Gergely László: Az adatvédelmi hatásvizsgálat módszertana. Médiakutató: Médiaelméleti Folyóirat 15:(4), 2014 pp. 77-95.

érintő, elsősorban a kormányzati, közigazgatási döntéshozatali, valamint egészségügyi eljárások részét képezi. Két alapvető tulajdonsága, hogy egyrészt a leendő adatkezelésre, illetve adatkezelést elrendelő jogalkotásra, új programokra, szolgáltatásokra és technológiákra egyaránt vonatkozik, másrészt nem szervezetre, hanem egyes projektekre vonatkozóan kell elkészíteni.

Célja, hogy a különböző projektekben a személyes adatok védelmét és a magánéletet érintő eljárások során a jogi szabályozásnak megfelelő rendszer kerüljön kiépítésre. Ezzel – a jogszerűség biztosítása mellett – a döntéshozatal átláthatósága és az érintettek tájékoztatása is megvalósítható. Tartalmát illetően azt vizsgálja, hogy az egyes – általában informatikai rendszerekkel megvalósított – személyes adatok kezelését igénylő rendszerek tervezése során sérül-e a magánszféra - amennyiben igen, akkor ez a sérelem mennyiben indokolt. Vizsgálja, hogy a megvalósítás a magánélet lehető legkisebb sérelmével jár-e és a megvalósításnak milyen várható hatásai lesznek, milyen kockázatok várhatóak és azok hogyan küszöbölhetők ki. Emellett arra is vonatkozik, hogy milyen kockázati tényezők mutathatók ki és milyen módosításokat kell végrehajtani a negatív hatások kiküszöbölése érdekében.

A PIA, mint fogalom nem ismeretlen Európában sem, habár az EU jogalkotása még nem szabályozta széles körben az egyes felügyeleti rendszerek kialakítását. A DPIA Európai Uniós bevezetésének lehetőségét vetítették előre az Európai Bizottság 2010-es állásfoglalásai az adatvédelmi reform előkészületei során.[87] A Bizottság ajánlásával összhangban a 29. cikk szerinti munkacsoport 2011 februárjában kidolgozta a rádiófrekvenciás azonosítás esetén a tagállamokban kötelezően alkalmazandó DPIA keretszabályozást.[88] Ezek a lépések előrevetítik annak lehetőségét, hogy az EU a jó gyakorlatokat felhasználva létrehozzon egy igazán hatékony és erős DPIA módszertant, amely képes jó irányba befolyásolni az információs társadalomban zajló folyamatokat.

A hatásvizsgálat a döntés-előkészítéstől a projekt végéig tart, azért, hogy az újabb megoldási módok vizsgálata is megtörténhessen. Fontos garanciális elem, hogy a vizsgálatot független szervezetek végzik, biztosítva ezzel a hitelességet és objektivitást. Az előzetes hatásvizsgálat

[87] European Commission, A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(2010) 609 final, Brussels, 4.11.2010. http://ec.europa.eu/justice/news/intro/news_intro_en.htm#20101104 [2014.06.20]

[88] 9/2011. számú vélemény a rádiófrekvenciás azonosítás (RFID) alkalmazásaira vonatkozó magánélet- és adatvédelmi hatásvizsgálati keretre irányuló felülvizsgált ágazati javaslatról 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_hu.pdf [2015.03.20.]

olyan korai szakaszban képes kimutatni az egyes kockázatokat, amivel a projekt kudarca, illetve a későbbi módosítási feladatok elkerülhetők.

A hatásvizsgálat jelentéssel zárul, ami magában foglalja a magánélet védelmének elveire és hatásaira vonatkozó megállapításokat; a kezelt személyes adatok körét; az adatkezelők körének meghatározását; annak az elemzését, hogy a javaslat megvalósítása milyen hatással lesz a személyes adatok védelmére; kockázatelemzést és annak hatásait; kockázatcsökkentési javaslatokat; megfelelő technikai és eljárási megoldásokra vonatkozó javaslatokat.

A hatásvizsgálat során cél az is, hogy a kötelezően teljesítendő adatkezelési, adatfeldolgozási kereteken túl az egyes kialakítandó rendszermegoldások közül az kerüljön kiválasztásra, amely a magánélet, így a személyes adatok védelmét a leginkább támogatja.[89]

7. Az adatvédelmi reform értékelése

Álláspontunk szerint a változás iránya megfelelő, mivel a beépített és alapértelmezett adatvédelem, valamint az adattakarékosság elve már alapelvi szinten is megjelenik követelményként, azokról nem csak az egyes szektorális jogszabályokban rendelkeznek. A privátszférát védő technológiák ezen elveknek való megfelelést szolgálják, és olyan konkrét eszközöket jelentenek, amelyek támogatása jogszabályi szinten – épp a technológiasemlegességre tekintettel – csak általános megfogalmazással lehetséges, akkor is, ha ez a gyakorlati alkalmazást nehezíti. Kívánatos ugyanakkor, hogy az adatvédelmi hatóságok egyedi, például épp a Privacy by Design elvét konkrét ügyben értelmező döntései nyomán kialakuló joggyakorlat, önszabályozó mechanizmusok (magatartási kódexek, szabványok), és az adatkezelők belső szabályai konkretizálják e szabályokat, és akár előírják konkrét PET alkalmazások használatát.

A privátszférát erősítő technológiáknak komoly szerepe lehet abban, hogy segítsék az adatvédelmi szabályok gyakorlati megvalósítását, ugyanakkor terjedésüket számos tényező hátráltatja – részben erre tekintettel e technológiák jogszabályok általi támogatását többen szorgalmazzák. A jogszabályi támogatás véleményünk szerint a beépített adatvédelem elvén keresztül valósulhat meg, a Privacy by Design megközelítés ugyanis annak biztosítására tesz kísérletet, hogy a technológia és jog, mint két szabályozórendszer ne kioltsa, hanem erősítse egymást, és egyértelműen a technológiát állítsa a – társadalmi elvárásokat végső soron kötelező normaként megjelenítő – jogi szabályozás szolgálatába, megtartva így a jogi

[89] Simon, Éva: Az adatvédelmi hatásvizsgálat bevezetésének lehetősége Magyarországon, In Szabó Máté Dániel – Székely Iván – Simon Éva: Szabad adatok, védett adatok 2. 2008, p 204.

szabályozás elsőbbségét. A privátszférát erősítő technológiák e célkitűzések megvalósításának első számú eszközei lehetnek, amely azonban álláspontunk szerint önmagában nem igényel külön jogszabályi szintű szabályozást – az adott adatkezelések során betöltött konkrét szerepüket az adatvédelmi joggyakorlat, önszabályozó mechanizmusok, mint az adatvédelmi hatásvizsgálat-, illetve az adatkezelők belső szabályai jelölhetik ki.

V. ADATBIZTONSÁGI MEGFONTOLÁSOK

E fejezet célja a személyes adatok, különösen a számítógépes adatbázisok kezelésére, üzemeltetésére vonatkozó legfontosabb jogi és szervezési, valamint műszaki követelmények áttekintése, valamint néhány gyakorlati megoldás bemutatása ezen elvárások belső szabályzatokban történő rögzítésére.

1. Jogszabályi előírások az adatbiztonságról

Az információ védelme, és az információ megszerzésére való törekvés egyidős az emberiséggel. Annak biztosítása, hogy a legbizalmasabb adatokat csak kisszámú, megbízható és védett személy ismerhesse meg vezetett el a szteganográfia (az üzenet elrejtése) és a kriptográfia (az üzenet titkosítása) kialakulásához.[90]

Általános követelményként jelent meg már az 1992-es adatvédelmi törvényünkben az adatbiztonság feltételeinek garantálása, mint a személyes adatok védelmének műszaki – biztonsági előfeltétele. Az összes adatkezelésre vonatkozó, általánosan meghatározott adatbiztonsági követelményeket az Infotv. tartalmazza, de emellett több szektorális adat- és információbiztonságra vonatkozó jogszabályi előírás található a magyar jogrendszerben.

A minősített adat védelméről szóló 2009. évi CLV. törvény rögzíti a közszféra által nagy mennyiségben kezelt minősített adatok védelmével kapcsolatos biztonsági alapelveket, többek között definiálja a személyi biztonsági tanúsítványt, a titoktartási nyilatkozatot, a felhasználói engedélyt, valamint a megismerési engedélyt is.

Ki kell emelnünk továbbá az állami és önkormányzati szervek (valamint a létfontosságú rendszerek és létesítmények) adatbiztonságára vonatkozó speciális feltételeket, melyeket az Ibtv.[91] és kapcsolódó végrehajtási rendeletei tartalmazzák. Az ezredfordulóra az információs társadalomhoz kapcsolódó széleskörű szolgáltatásokhoz kapcsolódóan számos olyan új veszély jelent meg, amely fenyegetések miatt Magyarország (csakúgy mint az Európai Unió

[90] Muha – Krasznay 2014 im. p. 5.
[91] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (a továbbiakban: Ibtv.)

számos tagországa) már kiemelt feladatként jelölte meg a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonságának garantálását.

Az adatvédelem területét emellett széles jogkörökkel rendelkező felügyelő hatóság a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) is felügyeli.[92]

2. Információbiztonság, informatikai biztonság és adatbiztonság

Az elektronikus információs rendszer biztonságával kapcsolatban értelmeznünk kell a gyakran szinonimaként megjelenő információbiztonság, informatikai biztonság és adatbiztonság, (illetve néha helytelenül ide sorolt adatvédelem) kifejezéseket. Ezt az elhatárolást számos, a témában megjelent ajánlás, szakirodalmi publikáció alkalmazta már az utóbbi évtizedben is, és ezt a felosztást követi az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény (Ibtv.),[93] és a hozzá kapcsolódó jogszabályokból átvett fogalommagyarázat is.

Az *információbiztonság* (information security) tágabb fogalom, mint az informatikai biztonság. Az elektronikus, informatikai rendszerben, vagy más módon kezelt adatok védelmét egyaránt ideértjük, az a folyamat, melynek során az információkat megvédjük a nem engedélyezett hozzáféréstől, használattól, felfedéstől, kiszivárgástól, megsemmisítéstől, módosítástól, vagy megzavarástól.[94] A védelem tehát eszköze annak, hogy a biztonság, mint kedvező állapot létrejöjjön és tartósan megmaradjon.

Az *informatikai biztonság* (Information Security, InfoSec) fentinek csak részhalmaza, tulajdonképpen a számítógépes biztonság. Az informatikai rendszerekben kezelt adatok védelmén túl az adatokat kezelő, tároló, továbbító rendszer védelmét is jelenti. A Közigazgatási Informatikai Bizottság 25. számú ajánlásában ennél pontosabb meghatározását láthatjuk, „*informatikai biztonság az informatikai rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelynek védelme az infokommunikációs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek*

[92] A NEIH-ről részletesebben lásd. Kodaj Katalin: A Nemzeti Elektronikus Információbiztonsági Hatóság, 2013. http://kifu.gov.hu/kifu/sites/default/files/NFM_Ibtv_NEIH_2013_12_18.pdf [2015.03.20.]
[93] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (a továbbiakban: Ibtv.)
[94] László Gábor: Kockázatértékelés, kockázatmenedzsment. Budapest, 2014. http://eiv.uni-nke.hu/uploads/media_items/kockazatertekeles-kockazatmenedzsment.original.pdf [2015.03.20.] p. 4.

sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos."[95]

Az Ibtv. mindkét fogalmat alkalmazza, ám ezektől el kell még határolnunk az *adatbiztonság* (data security) fogalmát, mely az informatikai védelemnek csupán az adatot a középpontjába állító megközelítése. Ez azonban a fenti fogalmaktól eltérően valójában nem biztonsági, hanem védelmi kategória, nem cél, hanem az adatalany védelme érdekében az adat védelmének műszaki, technikai eszköze.[96] A szakirodalmi álláspont szerint az adatbiztonság „*az adatok elérhetőségét, sértetlenségét és a jogosultaknak az előírt módon való hozzáférését biztosító előírások, szabványok betartásának eredményeképp elért információrendszer-állapot*"-ot jelöli, de a gyakorlatban az adatok biztonsága a megelőzésen túl a már megtörtént károk hatásainak csökkentésére is kiterjed, ami sikeressége esetén a hiba kijavításához vezethet.[97]

Az Infotv. 7.§ szintén az adatbiztonság kifejezést alkalmazza a személyes adatok kezelésének biztonsági követelményeivel kapcsolatban is, de eltérő jelentéssel és tartalommal, emiatt a szóhasználat miatt a biztonság technikusok időnként eltérően alkalmazzák a fogalmakat. Az adatvédelmi törvény kimondja, hogy az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét. Ez tulajdonképpen a beépített adatvédelem (Privacy by Design) elvének törvénybe foglalása, melyet az EU adatvédelmi reformjáról szóló fejezetben elemzünk részletesen.

A törvény elvi szinten rögzíti a technológia állásának figyelembevételét is, de a törvényben nincs külön utalás a kockázatarányos védelem elvére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek. Az adatbiztonsági szabályok megsértése esetén az adatvédelmi jog teljes szankciórendszere felhívható.

Meg kell jegyezni, hogy a közigazgatás egyes területén a jogalkotó az informatikai biztonság szabályozásában jelentősen továbbmegy az Infotv. szabályain. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény az informatikai

[95] Közigazgatási Informatikai Bizottság 25. számú Ajánlása. Magyar Informatikai Biztonsági Ajánlások (MIBA). 2008. www.ekk.gov.hu/hu/kib/KIB-25-0_MIBA_v1_vegl.pdf [2015.03.20.] p. 23.
[96] Törley Gábor: Adatbiztonság a közigazgatásban. Egyetemi jegyzet, Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kar, Budapest, 2013. p. 11.
[97] Szenes Katalin (szerk.): Az informatikai biztonság kézikönyve. 27. aktualizálás. Verlag Dashofer, 2007. p. 123.

biztonság területén részletes szabályrendszert és felügyeleti szervezetrendszert állapít meg, amelyek természetesen nagyban hozzájárulnak az adatbiztonság szintjének növeléséhez, így egyes adatkezelések során ezt is figyelembe kell venni.

2.1. Az informatikai rendszer és az adatok

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket. Az adat felől nézve ez az informatikai biztonsági környezet, ide tartozik valamennyi, az adatot logikailag és fizikailag körülvevő eszköz, tárgy, objektum, intézkedés. Ilyen, az informatikai rendszerre ható tényezők a környezeti infrastruktúra; a hardver elemek; az adathordozók; a dokumentumok; a szoftver elemek; az adatok; a rendszerelemekkel kapcsolatba kerülő személyek.

A védelmi intézkedések tárgyai lehetnek:

- az alkalmazott hardver eszközök és azok működési biztonsága,
- az informatikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk,
- az adatok és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,
- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára.[98]

Az Ibtv. 5.§-a különbséget tesz a rendszerben kezelt adatok, és a rendszer vagy rendszerelem biztonsága között. Ez a védelem az adatokat kezelő, tároló, továbbító rendszer védelmén túl jogi értelembe véve több, az adatgazda által akár egyszerre, párhuzamosan kezelt adatkört is érint:

- A különféle adatbázisokban található személyes adatokat, ezzel összefüggésben az érintettek magánszférájának, információs önrendelkezési jogának biztosítását (adatvédelem);
- A külön törvényben meghatározott feltételek alapján minősített adatok védelmét (korábbi elnevezésük állam- és szolgálati titok volt)
- A rendszerekben kezelt üzleti titkokat, egyéb bizalmas dokumentumokat;

[98] A Nyíregyházi Főiskola Informatikai Biztonsági Szabályzata. http://www.nyf.hu/sites/default/files/u5/EGYEB_INFORMACIOK/adminisztracio/szabalyzatok/37_informatika_biztonsagi.pdf [2015.03.20.] p. 5.

- Más gazdasági értékkel bíró, például a szellemi tulajdon védelme alatt álló adatokat (pl. szerzői jogilag védett adatbázisok);
- A közérdekű adatok vagy közérdekből nyilvános adatokat (pl. pályázati szerződések, az intézmény költségvetésére vonatkozó adatok, vezető beosztású munkavállalók adatai).

2.2. Alapelvek

A terület legfontosabb fogalmait az Ibtv. első szakaszában találjuk, melyek már egységesen illeszkednek hazánk és az Európai Unió legújabb kiberbiztonsági és információbiztonsági stratégiájába – függetlenül attól, hogy az általunk vizsgált adatkezelők tevékenysége a fenti jogszabályok hatálya alá esik-e. Már az Ibtv. preambulumában megtalálható a jogi szabályozás keretét alkotó megelőzés, a biztonság és a védelem klasszikus alapelvei hármasa, de ezek mellett megtalálhatjuk az információbiztonság alappilléreinek tekintett *bizalmasság* (Confidentiality), *sértetlenség* (Integrity), és *rendelkezésre állás* (Availability) meghatározását is. A legfrissebb megközelítések ezt a modellt kiegészítik a *felelősségre vonhatóság, elszámoltathatóság* (Accountability) tényezőjével, ami a tevékenységek nyomon követhetőségének szükségességét jelenti a felelős forrásig,[99] ez jelenik meg már az Ibtv koncepciójában is.

A bizalmasság az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

A sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

A rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.[100]

[99] Wheeler, Evan: Security Risk Management. Syngress, 2011. pp. 10-11.
[100] László Gábor: Kockázatértékelés, kockázatmenedzsment (egyetemi jegyzet). Nemzeti Közszolgálati Egyetem, 2014. http://eiv.uni-nke.hu/uploads/media_items/kockazatertekeles-kockazatmenedzsment.original.pdf [2015.03.20.] p. 5.

A hatályos törvények értelmében alapvető társadalmi elvárás a nemzeti elektronikus adatvagyon, valamint az ezeket kezelő információs rendszerek biztonsága, a digitális adatok és információk bizalmasságának, sérthetetlenségének és rendelkezésre állásának *zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítása*.

Ezen előírás egyes elemeit külön-külön megvizsgálva megállapíthatjuk, hogy zárt védelemről az összes releváns fenyegetést figyelembe vevő védelem esetén beszélhetünk.

A teljes körű védelem azt jelenti, hogy a védelmi intézkedések a rendszer összes elemére kiterjednek. Ennek részét képezi többek között a személyi biztonság, a fizikai védelem, a kibervédelem, az adminisztratív biztonság, a logikai védelem, valamint a zárt védelem is.

Folytonos védelem az időben változó körülmények és viszonyok ellenére is megszakítás nélkül valósul meg, a teljes életciklus (life cycle) az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését is magába foglaló időtartam.

A kockázattal arányos védelem esetén egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel,[101] azaz a védelemre akkora összeget és oly módon fordítanak, hogy ezzel a kockázat a védő számára még elviselhető vagy annál kisebb.[102]

A védelem biztosítása emellett olyan alapkövetelmény, amely indokolja, hogy az Ibtv. magát a védelmi feladatokat is rögzítse, így a védelmi feladatok alatt az értelmező rendelkezésekben kiemeli a megelőzést, a korai figyelmeztetést, az észlelést, a reagálást, és az eseménykezelést, azaz a gyakorlatban bevett kifejezéssel élve a PreDeCo (Preventive-Detective-Corrective) elvet is előírja a jogszabály. Az elvárt védelmi hatás eléréséhez három összefüggő és egymást kiegészítő részre, a megelőző (preventív), a felismerő (detektív) és az elhárító (korrektív) intézkedésekre helyezi a hangsúlyt.[103]

A következő lépésként a jogalkotó elérendő célként határozza meg egy olyan biztonsági kultúra megteremtését Magyarországon, amely garantálja az adatok bizalmasságának

[101] A kockázat (risk) információhiányt jelöl. Az Ibtv. 1. § (1) 28. pontja szerint az informatikai kockázat (R) a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének, W) és az ez által okozott kár nagyságának vagy súlyosságának (K) a függvénye. Matematikai megközelítésben: $R = W \times K$.

[102] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem, Budapest 2014. https://opac.uni-nke.hu/webview?infile=&sobj=9696&source=webvd&cgimime=application%2Fpdf%0D%0A [2015.03.20.] pp. 6-9.

[103] Lásd bővebben Bodó Attila Pál: Jogi és közigazgatási ismeretek elektronikus információbiztonsági vezető szakirányú hallgatóknak (egyetemi jegyzet). Nemzeti Közszolgálati Egyetem, 2014. http://eiv.uni-nke.hu/uploads/media_items/jogi-es-kozigazgatasi-ismeretek.original.pdf [2015.03.20.]

megfelelő szintű informatikai (technikai) védelmét (tűzfal, vírusvédelem, titkosított kommunikáció stb.), adminisztratív eszközeit (Informatikai Biztonságpolitika, Stratégia és a kapcsolódó szabályzatok előírása) de ezzel összhangban gondoskodik a közszférában dolgozó személyek biztonsági tudatosságának magas fokáról is (humán faktor).

3. Alkalmazható szabványok

A műszaki követelmények tekintetében javasoljuk két magyar (és egyben nemzetközi) szabványban ajánlott adatbiztonsági kontrollok betartását. Ezek az MSZ ISO/IEC 27002:2011 *Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve*. Ezek a szabványok mind a fizikai, a logikai és adminisztratív védelem tekintetében tartalmaznak követelményeket. Javasolt a fejlesztőnek, rendszerintegrátornak is a saját működése tekintetében is betartani ezeket a követelményeket, akkor is, ha külön törvényi kötelezettségük erre nincs is. Mindamellett, hogy jelen dokumentumban elsősorban követelményekről beszélünk, de ezek önkéntesen vállalt követelmények. Figyelembe kell vennünk, hogy az idézett szabványok nem normatívak, a szabványalkotó ajánlásnak szánta őket.

Információbiztonsági politika. A vezetőség egyértelmű álláspontot alakítson ki a működési célokkal összhangban és mutasson támogatást és elkötelezettséget az információbiztonság iránt azáltal, hogy információbiztonsági politikát bocsát ki és tart fenn az egész szervezetben. [MSZ ISO/IEC 27002:2011 5.1.]

Az információbiztonság belső szervezete. Egy irányítási keretrendszert kell létrehozni, hogy kialakítsa és szabályozza az információbiztonság bevezetését a szervezeten belül. A vezetőség hagyja jóvá az információbiztonsági politikát, jelölje ki a biztonsági feladatköröket, koordinálja és vizsgálja át a biztonság bevezetését a szervezetbe.

Ha szükséges, információbiztonsági tanácsot adó szakértők erőforrását hozzák létre, tegyék elérhetővé a vállalaton belül. Fejlesszenek ki kapcsolatokat a külső biztonsági szakértőkkel vagy csoportokkal, beleértve az illetékes jogosított szervezeteket, hogy lépést tartsanak az ágazati irányzatokkal, figyeljék a szabványokat és a felmérési módszereket, és megfelelő kapcsolódási pontokat nyújtsanak, amikor információbiztonsági incidenseket kezelnek. Bátorítani kell az információbiztonság több szakterület szerinti megközelítését. [MSZ ISO/IEC 27002:2011 6.1.]

Az adatbiztonsági felelős az információbiztonságban és főképp az informatikai biztonságban járatos személy lehet, aki felsőfokú iskolai végzettséggel és informatikai, műszaki szakképzettséggel vagy középiskolai végzettséggel és legalább emelt szintű informatikai szakképesítéssel (OKJ) rendelkezik. Javasolt az adatbiztonság területén valamely nemzetközi szakvizsga teljesítése (pl. CISA, CISM, CISSP). Adatbiztonsági felelős lehet az adatvédelmi felelős is, amennyiben a követelményeknek megfelel.

Az információbiztonság külső szervezete. Minden hozzáférés a szervezet információ-feldolgozó eszközeihez és az információ külső felek általi feldolgozása és közlése szabályozva legyen.

Ha működési igény van külső felekkel való munkára, amely a szervezet információs és információ-feldolgozó eszközeihez való hozzáférést igényelhet, vagy egy termék megszerzését vagy szolgáltatás nyújtását egy külső féltől vagy egy külső félnek, kockázatfelmérést kell végezni, hogy meghatározzák a biztonsági kihatásokat és az intézkedési követelményeket. Az intézkedésekben egyezzenek meg és azokat a külső féllel való megállapodásban határozzák meg. [MSZ ISO/IEC 27002:2011 6.2.]

Emberi erőforrások biztonsága az alkalmazás előtt. A biztonsági felelősségekkel az alkalmazás előtt kell foglalkozni megfelelő munkaköri leírásokban és az alkalmazási feltételekkel megadva. Minden alkalmazásra jelöltet, a szerződő feleket és a használó harmadik felet megfelelően világítsanak át, különösen érzékeny munkakörökben. Az alkalmazottak, a szerződő felek és az információ feldolgozó berendezéseket használó harmadik fél írjanak alá egy megállapodást a biztonsági feladatokról és felelősségekről. [MSZ ISO/IEC 27002:2011 8.1.]

Emberi erőforrások biztonsága az alkalmazás alatt. Biztosítsák, hogy az alkalmazottak, szerződő felek és a használó harmadik fél tudatában legyenek az információbiztonsági fenyegetéseknek és gondoknak, felelősségüknek, kötelezettségüknek és legyenek felszerelve, hogy támogassák a szervezeti biztonsági politikát rendes munkájuk alatt, és csökkentsék az emberi tévedés kockázatát. A vezetőség felelősségét határozzák meg és gondoskodjanak, hogy a biztonságot alkalmazzák az egyén alkalmazása során a szervezetben. Megfelelő szintű tudatosságot, a biztonsági eljárásokban való képzést és oktatást, és az információ-feldolgozó eszközök helyes használatát biztosítsák minden alkalmazottnak, szerződő félnek és használó harmadik félnek, a lehetséges biztonsági kockázatok legkisebbre szorítása céljából. Létre kell

hozni egy hivatalos fegyelmi folyamatot a biztonság megsértésének kezelésére. [MSZ ISO/IEC 27002:2011 8.2.]

Emberi erőforrások biztonsága az alkalmazás megszűnése vagy változtatása esetén. A felelősségeket úgy alakítsák ki, hogy biztosítsák, hogy az alkalmazottak, a szerződő felek vagy a használó harmadik fél távozását a szervezetből úgy intézzék, hogy az összes berendezés visszaküldése és minden hozzáférési jog visszavonása a szervezetben befejeződjék. A felelősségek vagy alkalmazások változtatását egy szervezeten belül kezeljék úgy, mint amikor az illető felelősség vagy alkalmazás ezzel a fejezettel összhangban befejeződik és az új felelősségeket vagy alkalmazást kezeljék az új munkatársa vonatkozóak szerint. [MSZ ISO/IEC 27002:2011 8.3.]

Az információbiztonsági események kezelése. Hivatalos eseményjelentési és kiterjesztési eljárások álljanak rendelkezésre. Minden alkalmazott, szerződő fél és használó harmadik fél ismerje a különböző fajta, a szervezeti vagyontárgyak biztonságára esetleg hatást gyakorló esemény és gyenge pont jelentési eljárásait. Ezektől kívánják meg, hogy bármely információbiztonsági eseményt és a gyenge pontokat a lehető leggyorsabban jelentsék a kijelölt kapcsolati helynek. [MSZ ISO/IEC 27002:2011 13.1.]

Az információbiztonsági eseményeket a lehető leggyorsabban jelentsék a megfelelő vezetőségi csatornákon. [MSZ ISO/IEC 27002:2011 13.1.1.]

Az információs rendszerek és szolgáltatások minden alkalmazottól, szerződő féltől és használó harmadik féltől megkívánják, hogy a rendszerekben vagy szolgáltatásokban található, bármely megfigyelt vagy gyanított biztonsági gyenge pontot feljegyezzenek és jelentsenek. [MSZ ISO/IEC 27002:2011 13.1.2.]

Felelősségek és eljárások álljanak rendelkezésre, hogy eredményesen kezeljék az információbiztonsági eseményeket és gyengeségeket, ha már egyszer jelentették. Folyamatos fejlesztési folyamatot alkalmazzanak az információbiztonsági incidensekre való válaszként, azok figyelemmel kísérésére, és átfogó kezelésére. Ha bizonyíték szükséges, össze kell gyűjteni, hogy biztosítsák a jogi követelményeknek való megfelelést. [MSZ ISO/IEC 27002:2011 13.2.]

Vezetőségi felelősségeket és eljárásokat kell kialakítani, hogy gyors, eredményes és szabályos választ biztosítsanak az információbiztonsági incidensekre. [MSZ ISO/IEC 27002:2011 13.2.1.]

Legyenek kész mechanizmusok, hogy lehetővé tegyék az információbiztonsági incidensek fajtái, mennyiségei és költségei számszerűsítését és figyelemmel kísérését. [MSZ ISO/IEC 27002:2011 13.2.2.]

Ha egy követő tevékenység egy személlyel vagy szervezettel szemben egy információbiztonsági incidens után jogi pert foglal magában (polgári vagy büntető), bizonyítékot gyűjtsenek, tartsanak meg és mutassanak be, hogy megfeleljenek a vonatkozó jogszabály(ok)ban lefektetett bizonyítási szabályoknak. [MSZ ISO/IEC 27002:2011 13.2.3.]

VI. ZÁRÓ GONDOLATOK

A tanulmányban bemutattuk a jelenleg hatályos szabályozás mellett a várható változásokat és a legfontosabb adatvédelmi elvárásokat. Jól látható, hogy számos adatkezelési gyakorlat tekinthető technológiai, társadalmi, és ezek következtében jogi szempontból is gyorsan változó és bizonytalan megítélésű területnek, ezért a bemutatott rendelet-tervezet, vagy éppen az adatvédelmi hatóságok nemzetközi konferenciájának eredményei is hatással vannak az adatok kezelésével kapcsolatos kutatásokra.

VII. A BELSŐ ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Az Infotv. 24. §-a egyes szervezetek esetében előírja, a belső adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Adatvédelmi Szabályzat) elkészítését. Kinek kell szabályzatot elkészítenie, és milyen adattartalomal?

1. Az alábbi szerveknek írja elő kötelezően az Infotv. az Adatvédelmi Szabályzat elkészítését

- Országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelő, illetve feldolgozó adatkezelők és adatfeldolgozók,
- a pénzügyi szervezetek,
- az elektronikus hírközlési szolgáltatók,
- a közüzemi szolgáltatók,
- állami adatkezelők,
- önkormányzati adatkezelők.

2. A szabályzat felépítése, tartalma

A törvény nem ad útmutatást arra vonatkozóan, milyen rendelkezéseket tartalmazzon az Adatvédelmi Szabályzat. A tananyag a legfontosabb elemeket emeli ki.

- A szabályzat célja és hatálya,
- Kapcsolat az adatkezelő egyéb szabályzataival,
- Értelmező rendelkezések,
- Az adatkezelő adatai,
- Az adatkezelőre vonatkozó alapvető általános szabályok, alapelvek,
- Szervezeten belüli felelősségek meghatározása,
- A belső adatvédelmi felelős,
- A munkavállalók személyes kötelezettségei,
- Adatok tárolására vonatkozó szabályok,
- Adatbiztonsággal kapcsolatos adminisztratív teendők,
- Adatok felhasználására vonatkozó főbb szabályok,
- Adatfeldolgozás, kiszervezés,
- Az érintett jogai gyakorlásának biztosítása,
- Adattovábbítás, hatósági adatszolgáltatás,
- Adattovábbítási nyilvántartás,
- A jogellenes adatkezelés következményei,
- Eljárási szabályok, záró rendelkezések.

A részek természetesen még bővülhetnek, mivel minden adatkezelő szervnek van speciális csak a szervezetére vonatkozó adatkezelése, amelynek helyet kell kapnia az Adatvédelmi Szabályzatban.

A belső adatvédelmi felelős az Infotv. 24. § (2) bekezdés d) pontja alapján előkészíti az Adatvédelmi Szabályzatot. A törvény nem írja elő, hogy ki aktualizálja a hatályban lévő Adatvédelmi Szabályzatot, de egyértelműnek tűnik, hogy a belső adatvédelmi felelős a legalkalmasabb személy erre a feladatra, így az erre vonatkozó szabályozást a belső szabályozásban lehet megjeleníteni.

A belső adatvédelmi felelős személyét és szervezeti elhelyezkedését az Adatvédelmi Szabályzat tartalmazhatja, de egy esetleges változás esetén a szabályozást módosítani kell. Fontos azonban, hogy amennyiben a belső adatvédelmi felelősnek az Infotv-ben meghatározott feladatoknál bővebb vagy speciálisabb feladatköre van, az részletesen kerüljön

szabályozásra. A belső adatvédelmi felelős jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező személy lehet. Az Infotv. előírja, hogy a belső adatvédelmi felelősnek az adatkezelő vagy az adatfeldolgozó szerv szervezetén belül a szerv vezetőjének közvetlen felügyelete alatt kell állnia. Ettől eltérően megbízási szerződéssel is foglakoztatnak belső adatvédelmi felelősöket szervek. A legjellemzőbb, hogy a feladatkört a munkáltató részfeladatként határozza meg, és valamely jogi munkát végző szakembert nevez ki. Amelyet természetesen a szerzők nem helyeselnek. A belső adatvédelem feladatköre az adott szerv egészére kiterjed és számos részterületet is magában foglal, így pl az információszabadság nem képzelhető el információs önrendelkezés nélkül és a közzététel is megkívánja a belső adatvédelmi felelős ellenőrzését. Az véleményem szerint a belső adatvédelem komplexen a három terület egymásba kapcsolódásával végezhető hatékonyan.

A szabályzatot a szerv vezetője szabályzatban (utasításban) adja ki. A szabályzat alapvetően belső dokumentum, de az állami, önkormányzati, vagy jogszabályban meghatározott egyéb közfeladatot ellátó adatkezelők kötelesek honlapjuk "közérdekű adatok" menüjében közzétenni.

VIII. BELSŐ ADATVÉDELMI NYILVÁNTARTÁS

A közfeladatot ellátó szervezet számtalan adatkezeléssel rendelkezik. Ezek az adatbázisok a napi munkához szükséges – a különböző szakterületeknek megfelelő – adattartalommal bírnak, azokat vagy a készítő saját elhatározásra, vagy valamilyen szabályozó által meghatározott követelmények szerint és tartalommal hozza létre.

Ahhoz, hogy a belső adatvédelmi felelős tisztában legyen szervezete minden adatkezelésével szerteágazó és következetes tevékenységre van szükség. Elengedhetetlen feltétele az adatvédelmi nyilvántartás összeállításának a szervezet minden részletre kiterjedő megismerése. Ehhez az adatvédelmi felelősősnek mindenképpen tájékozódnia kell. Meg kell ismernie a szervezet alapító okiratát, szervezeti és működési szabályzatát, az egyes szervezeti egységek ügyrendjét, és egyéb, a működést befolyásoló okmányt. Ezek után az egyéni interjúk lefolytatásán van a sor. Az interjúk során az egyes szervezeti egységek vezetőivel le kell modellezni a szervezeti egység adatkezeléseit, melynek során végül helyszíni betekintéssel fizikailag is meg kell tekintetni a különböző kartotékokat vagy lajstromokat. A kétfajta nyilvántartás között az a legnagyobb különbség, hogy míg a kartotékokat valamilyen előre kialakított rend szerint - például betűrend – alapján állítják sorrendbe, addig a lajstromos

nyilvántartás elemei időrendben követik egymást. Természetszerűen ma az információs társadalomban élve a nyilvántartások nagy része, néhol a döntő többsége elektronikus. Ettől függetlenül ezek a nyilvántartások is – a meghatározott esetben – részesei a belső adatvédelmi nyilvántartásnak. De melyek ezek a meghatározott esetek?

A belső adatvédelmi nyilvántartás elkészítőjének el kell tudnia az egyes adatkezeléseket különítenie egymástól. Ehhez meg kell tudnia különböztetni a személyes adatokat tartalmazó nyilvántartásokat, azoktól, mely ilyen adatokat nem tartalmaznak. Ehhez mindenképpen tisztában kell lennie azokkal az alapvető fogalmakkal, melyeket az Infotv. 3. § a határoz meg. Ezek többek között a következők:

Személyes adat fogalma: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés[104].

Különleges adat fogalma

A faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat.

Az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.[105]

Bűnügyi személyes adat fogalma

A büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.[106]

A fenti fogalmakat takaró adatok a közfeladatot ellátó szervezet mindennapjaiban előfordulnak. A belső adatvédelmi nyilvántartásba csak azok az adatkezelések tartoznak, melyek során személyes adatok kezelése folyik. Egy közfeladatot ellátó szervezet két módon lehet személyes adatok kezelője, kifejezett illetékességből eredően, illetőleg beleértett illetékességből. Kifejezett illetékesség esetén az adatkezelő személyét az adatkezelésről szóló

[104] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 2. pont
[105] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 3. pont
[106] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 4. pont

törvény határozza meg. Beleértett illetékesség alatt azt értjük, hogy törvény konkrétan nem rendelkezik az adatkezelőről, hanem az a meglévő hagyományos szerepek alapján (pl. munkáltató) válik adatkezelővé. Általában egy ilyen szervezetnél mindkét típusú adatkezelés előfordul.

A belső adatvédelmi nyilvántartás elkészítésének és folyamatos pontosításának alapvető célja, hogy az adatkezelő (a közfeladatot ellátós szervezet vezetője, aki az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja)

- tisztában legyen a szervezet minden olyan adatkezelésével, melyek személyes adatok kezelésére vonatkoznak,
- be tudjon jelentkezni a Nemzeti Adatvédelmi és Információszabadság Hatóság adatvédelmi nyilvántartásba, a már bejelentett adatkezelések módosulása esetén változásbejegyzési kérelmet tudjon készíteni,
- a személyes adatokat tartalmazó adatkezelései jogszerűségének ellenőrzése, a jogszerű gyakorlat kialakítása.

Ezen felül, fontos funkciója még az adatvédelmi nyilvántartásnak, hogy nyilvánvalóan alapja kell hogy legyen a szervezet adatvédelmi és adatbiztonsági szabályzatának.

A korábban felsorolt eljárási elemek (információgyűjtés, interjú, személyes betekintés) megtörténte után kezdődhet meg ténylegesen a belső adatvédelmi nyilvántartás elkészítése. A nyilvántartás adatköre tekintetében javasolt, hogy az feleljen meg annak az adatkörnek, mely a hatóság által vezetett adatvédelmi nyilvántartás adatkörének megfelel, ebben az esetben ugyanis a bejelentkezéskor kisebb időráfordítással eleget lehet tenni a törvényi kötelezettségnek.

Emellett az adatvédelmi nyilvántartás adatköre meglehetősen tágabb, mint az Infotv. 20. §-a által meghatározottak, mely szerint az érintettet az adatkezelés megkezdése előtt az alábbiakról kell egyértelműen és részletesen tájékoztatni:

- az adatkezelés céljáról és jogalapjáról,
- az adatkezelésre és az adatfeldolgozásra jogosult személyéről, illetve
- kik ismerhetik meg az adatokat.
- adatkezeléssel kapcsolatos jogok és jogorvoslati lehetőségek.

Amennyiben az érintettet tájékoztatása lehetetlen vagy aránytalan költséggel járna, a tájékoztatás megtörténhet az adatgyűjtés tényének, az érintettek körének, az adatgyűjtés céljának, az adatkezelés időtartamának, az adatok megismerésére jogosult lehetséges adatkezelők személyének, az érintettek adatkezeléssel kapcsolatos jogainak és jogorvoslati lehetőségeinek ismertetésének és amennyiben az adatkezelést hatósági nyilvántartásba vettek, a hatósági nyilvántartás számának ismertetésével.

Nem elég hangsúlyozni, hogy a szervezet adatvédelmi nyilvántartását kellő odafigyeléssel és megalapozott szakmaisággal kell elkészíteni, hogy megfeleltethető legyen a hatósági nyilvántartásnak, elkerülendő, hogy a Hatóság azt hiánypótlásra vagy kijavításra visszaküldje az adatkezelő szervezet részére. Jelenleg a hatóság nyilvántartásába két módon lehet bejelentkezni. Az egyszerűbb az online, míg kissé bonyolultabb a papír alapú bejelentkezés. A gyakorlat azt mutatja, hogy a papír alapú nyomtatvány rendelkezik azokkal a sajátosságokkal, melyek alapján megnyugtatóan kezelni tudjuk adatkezeléseinket. Ezen végighaladva a szervezet adatkezeléseit megfelelő konstellációban tudjuk látni, és nagy segítséget jelent eligazodnunk az egyes területek között.

Fontos és nem lehet eléggé hangsúlyozni, hogy adatkezelésenként külön-külön kell űrlapot kitölteni. minden egyes adatkezelés külön célt szolgál és ezen a cél mentén tudjuk ezeket különválasztani. Lássuk lépésről lépésre ezt a nyomtatványt.

Az 1. pont az adatkezelőt pontosítja. Az adatkezelő az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja[107]. E tekintetben viszonylag könnyű dolgunk van. Az adatkezelő az a szervezet ahol az adatkezelés folyik.

Az 1. pont az adatlapon a következőképpen fest:

1. Adatkezelő

1.1. Az adatkezelő megnevezése:

1.2. Címe:

1.3. Telefonszáma:

[107] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 9. pont

1.4. Belső adatvédelmi felelős neve, elérhetőségei

A kitöltése értelemszerűen történik, a szervezet címét, központi telefonszámát, valamint a belső adatvédelmi felelős nevét és elérhetőségét kell a megfelelő helyre beírni.

Az 1.5. pontokat kizárólag akkor szükséges megjeleníteni, amennyiben változásjelentésről beszélünk, tehát, ha egy már regisztrált adatkezelés valamilyen okból megváltozik.

1.5. Előző adatkezelés

1.5.1. Az adatkezelő megváltozásának jogcíme:

1.5.2. Előző nyilvántartási azonosító:

Az 1.5.1. esetében a megváltozás jogcíme törvénymódosulás lehet, tehát, hogy a törvény már nem annak az eddigi adatkezelőnek ad felhatalmazást az adatkezelésre, hanem egy másik adatkezelőnek. Előfordulhat, hogy maga az adatkezelő személye változik meg (pl. jogutódlás, átalakítás stb.) ebben az esetben ezt az aktust kell rögzíteni a nyomtatványon. Az 1.5.2. pont csak abban az esetben értelmezhető, amennyiben az adatkezelés a NAIH részére bejelentésre került és kapott nyilvántartási azonosítót. Amennyiben ilyen nincs üresen kell hagyni ezt a helyet.

A következő részek kitöltése viszont sokszor a gyakorlott adatvédelmi szakembereknek is gondot okoz.

1.6. Az adatkezelés megnevezése:

Ennél a pontnál az a feladat, hogy az adatkezelés elnevezésre kerüljön. Sokszor előfordul, hogy hasonló adatkezeléseket ugyanazzal a megnevezéssel illetnek, mely a későbbiekben komoly problémákat eredményezhet. Az adatkezeléseknek el kell különülniük és ennek az első lépése a megnevezés helyes megválasztása. A példa kedvéért belépési engedélyek nyilvántartását el kell tudni különíteni a belépési engedélyeknek a belépésre vonatkozó adatainak nyilvántartásától. Az egyik nyilvántartásnak a célja magának az engedélynek a kiállítása, a másiknak pedig az, hogy a munkáltató adott esetben ellenőrizze a munkavállalók be és kilépésének idejét. Ebben az esetben elkülönül a cél, és elkülönül a betekintésre jogosult kör is.

1.7. Az adatkezelés célja, időtartama:

Ez talán az egyik legnehezebben kitölthető pont. Abban az esetben lehet könnyebb a dolgunk, ha az adatkezelést törvény rendeli el, és az Infotv. rendelkezéseinek megfelelően ez a törvény rendelkezik az adatkezelés céljáról és az időtartamáról is. Sajnos sok esetben ez az elrendelő törvény esetében erről nem beszélhetünk. Ilyen esetben jobb híján magunknak kell meghatározni azt a célt, amit a törvényalkotó el szeretett volna érni az adatkezeléssel. Amennyiben a törvényben az időpont nincs meghatározva, abban az esetben a megőrzési időt egyéb jogszabályok által megszabottak szerint kell megállapítani, vagy a szervezet iratmegőrzési szabályait kell segítségül hívnunk. Jóval nehezebb dolgunk van a hozzájárulások alapuló adatkezelések tekintetében. Ebben az esetben még az adatkezelés elkezdése előtt el kell dönteni az adatkezelés célját, és azt, hogy az adatokat meddig kezeljük. Ez természetesen nem önkényes döntés függvénye kell, hogy legyen, mert adatot kezelni csak az adatkezelés céljának, illetve egyéb esetekben más kötelezettségek teljesítésének megvalósulásáig lehet. Amennyiben szervezetünk nem rendelkezik adatvédelmi nyilvántartással, abban az esetben az adatlapot a már fennálló, de eddig nem rögzített adatkezelések esetén fel kell venni. Ekkor utólag kell a már „működő" adatkezelések tekintetében az adatkezelés célját a nyomtatványon rögzíteni.

1.8. Az adatkezelés jogalapja

1.8.1. Jogszabályhely vagy más jogalap:

Klasszikus értelemben két jogalapja lehet az adatkezeléseinknek. Az első az érintett hozzájárulása. A korábban már tárgyalt érintetti hozzájárulás hiányában adatot, csak törvényben vagy, törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendeletben lehet elrendelni, de csak abban az esetben, az adatkezelés célja közérdeken alapul. Fontos az adatkezelések felmérésekor annak eldöntése, hogy egyes adatkezeléseink mely jogalapon alapulnak. Nem lehet eléggé hangsúlyozni, hogy adatkezelést kizárólag törvény rendelhet el, illetve egy viszonylag keskeny szegmens tekintetében önkormányzati rendelet. E helyütt soha nem lehet adatkezelés céljaként közjogi szervezetszabályozó eszközt, ad abszurdum belső rendelkezést megjelölni. Hangsúlyozni szükséges, hogy nem elegendő csupán a jogszabály címe és a száma, pontos jogszabályhelyi hivatkozás szükséges a helyes kitöltéshez (szakasz, bekezdés, esetleg pont).

Az Infotv. ismer további – korábban szintén említett – speciális jogalapokat, azonban ezen jogalapok is csak különleges helyzetekben adhatnak okot adatkezelésekre. Ebben az esetben meg kell felelni a törvényben meghatározott feltételeknek, miszerint akkor is lehet adatot

kezelni, ha az érintett hozzájárulásának beszerzése lehetetlen vagy az adatkezeléssel összefüggésben aránytalan költséggel járna, ám ezen felül az alábbi feltételek valamelyikének fent kel állni. Ezek a feltételek a következők: az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítése, vagy az adatkezelő vagy harmadik személy jogos érdekinek érvényesítése céljából szükséges. Tovább lehet folytatni az adatkezelést, amennyiben korábban volt érintetti hozzájárulás, azonban azt az érintett visszavonta, amennyiben ez az adatkezelő a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából – ha ezen érdekek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll – szükséges.

1.8.2. Jogszabály címe:

Értelemszerűen ez a pontot csak abban az esetben kell kitölteni, ha törvény (vagy önkormányzati rendelet) rendeli el az adatkezelést. Ebben az esetben viszont annak elnevezését és számát is fel kell tüntetni.

1.9. A tényleges adatkezelés helye:

A nyomtatvány következő pontja, hogy meg kell adnunk az adatkezelés konkrét helyét. Ennek abban rejlik a jelentősége, hogy a nyilvántartás birtokában pontosan be tudjuk azonosítani az adatkezelések fizikai megvalósulásának helyét. Itt nem feltétlenül a pontos irodaszámot kell érteni az adatkezelés helye tekintetében, hanem azt, hogy a szervezet mely szervezeti egysége kezeli az adatokat. pl. pénzügyi osztály. Ez a pont a belső adatvédelmi felelősöknek is pontos tájékoztatást tud adni arra az esetre, hogy hol kell fokozottabban figyelni az adatkezeléseket.

1.10. Az adatkezelés automatizáltsága:

Az adatkezelések lehetnek papír és számítástechnikai alapúak, de előfordul, hogy vegyesen használják mindkettőt. Az adatkezelések automatizáltsága attól függ, hogy az adatkezelő részéről igényel-e manuális beavatkozást vagy sem. Amennyiben nem akkor az adatkezelés automatizált, amennyiben van beavatkozásra lehetőség akkor félig automatizált az adatkezelés, és ha kizárólag emberi adatfelvitel történik, akkor az adatkezelés nem automatizált.

Az űrlap 2. pontja tekintetében fel kell eleveníteni az adatfeldolgozásról korábban tanultakat. Az adatfeldolgozás az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az

alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik.108 Az adatfeldolgozó az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.109

Nagyon fontos tudni, hogy az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az Infotv., valamint az adatkezelésre vonatkozó külön törvények keretei között az adatkezelő határozza meg. Az általa adott utasítások jogszerűségéért az adatkezelő felel. Korábban az volt a szabály, hogy az adatfeldolgozó további adatfeldolgozót nem vehet igénybe, ám a jelenlegi szabályozás ezt lehetővé teszi, amennyiben az adatkezelő így rendelkezik. Ez a kitétel azért fontos, mert döntési helyzetben mindig az adatkezelő van.

Az adatfeldolgozást írásos szerződésbe kell foglalni.

2.1. Az adatfeldolgozó megnevezése:

2.2. Címe:

2.3. Telefonszáma:

2.4. Belső adatvédelmi felelős neve, elérhetőségei:

Ezekbe a pontokba annak az adatfeldolgozónak nevét, címét és telefonszámát kell beírni, aki vagy amely az adatfeldolgozásról szóló szerződésben nevesítve van. Természetesen a belső adatvédelmi felelős e tekintetben az adatfeldolgozó belső adatvédelmi felelőse lesz.

A 3. pont megint meglehetősen bonyolult és megalapozott munkát igényel. A nyilvántartás arra keres választ, hogy mi az kezelt adatok forrása, és ami még ennél is fontosabb, hogy mi az kezelt adatok köre. Ennél a pontnál derül ki, hogy honnan szerezzük be az adatokat, mi annak a jogcíme, az adatok törlési határideje. Az űrlap ezen a ponton véleményem szerint ismétlésekbe bocsátkozik a tekintetben, hogy annak 1.7. pontja már tárgyalja az adatkezelés időtartamát, másrészt az 1.8. pont pedig megtárgyalta annak jogalapját, vagyis a törvényi helyet. Ezen túltéve magunkat, elemezzük ki, hogyan kell ezt a pontot helyesen kitölteni.

3.1. Adatfajta megnevezése:

[108] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 17. pont
[109] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 18. pont

Csak olyan adatokat lehet kezelni, melyet törvény, vagy önkormányzati rendelet meghatároz, vagy amihez az érintett a hozzájárulását adta. Ezen túlterjeszkedni nem lehet, tehát csak és kizárólag azokat az adatokat kezelhetjük, melyre megtörtént a felhatalmazás. Példaként említeném a következőket: név, anyja neve, születési hely, lakcím, testtömeg, e-mail cím, forgalmi rendszám és így tovább. Amennyiben mégis bővíteni vagy szűkíteni szeretnénk a kezelt adatok körét, akkor egy módosított adatlapot kell kitölteni és adott esetben a hatóságnak megküldeni.

3.2. Adatforrás megnevezése:

3.3. Adatfelvétel (átvétel) jogalapja

3.3.1. Jogszabályhely vagy más jogalap

3.3.2. Jogszabály címe

Az adatkezelés átfogó megismeréséhez tudni kell, hogy az általunk kezelt adat honnan származik. Általában magától az érintettől szerezzük be az adatotokat, ám gyakran előfordul, hogy más forrásból, más szervezettől kapjuk meg a kezelendő adatokat. ennek megfelelően kell kitölteni ezt a helyet. Az adatátvétel jogalapja megegyezik magának az adatkezelésnek a jogalapjával, így az esetek döntő többségében ugyanazt a jogszabályt és jogszabályi helyet kell megjelölni, amelyet az 1.8 pontban már megtettünk. Természetesen, ha az adatkezelés jogalapja az érintett hozzájárulása volt, akkor ide is azt kell beírni.

3.4. Adatfelvétel (átvétel) módja:

Ennél a pontnál konkrétan meg kell jelölni az adatok gyűjtésének, felvételének, átvételének konkrét módját, pl.: kérdőív, formanyomtatvány kitöltése, címlista átvétele, stb.

3.5. Az adat törlési határideje:

Törvényen alapuló adatkezelés esetén a jogszabályban meghatározott határidő jelölendő meg. Hozzájáruláson alapuló adatkezelés esetén e határidő nem térhet el az 1.7. alpontban megjelölt időtartam záró dátumától.

4. Adattovábbítás(ok)

Az űrlap kitöltésnek egyik neuralgikus pontja ez. Az adattovábbítás önmagában egy adatkezelésnek minősülő eljárás, mely az adat meghatározott harmadik személy számára történő hozzáférhetővé tételét jelenti. Szót kell ejteni az adattovábbítási nyilvántartásról is. Az

adatkezelőnek az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást kell vezetnie, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat. Ennek az adatkezelésnek a jogalapja sem lehet más, mint a már korábban megfogalmazottak, miszerint azt csak az érintett hozzájárulásával, vagy törvénnyel illetve erre feljogosított önkormányzati rendelettel lehetséges megtenni. A nagyon sok olyan adatkezelés van, ahol nincsen adattovábbítás. Ezek azok az adatkezelések, melyek során kizárólag a szervezet megfogalmazott adatkezelési céljainak megfelelően saját számára kezel adatokat a szervezet. Ilyen egy a szervezet által megrendezett rendezvény során kezelt adatok köre. Olykor már az adatkezelés megkezdésekor tudott, hogy az adatok továbbításra kerülnek, például amikor egy pályázat nyertesinek adatait megküldik a kifizetőhely részére. Előfordul olyan is, hogy az adatokat nem továbbítják alapvetően, azonban valamilyen esemény bekövetkeztekor az arra jogszabályban feljogosított hatóság részére kötelező továbbítani. Ilyen tipikusan az elektronikus megfigyelőrendszerek (kamerák) adatkezelése. Alapesetben ezek az adatok a megfelelő idő eltelte után törlésre kerülnek, amennyiben azonban valamilyen esemény, tipikusan bűncselekmény történik, a kamerák adatai továbbításra kerülhetnek az esemény vizsgáló hatóság részére.

Ide azokat az adatokat kell értelemszerűen tételesen beírni, melyek továbbításra kerülnek.

4.2. Címzett neve

A címzett az adattovábbítás címzettje, akinek jogszerűen az adatot tovább kell vagy lehet továbbítani.

4.3. Az adattovábbítás jogalapja

4.3.1. Jogszabályhely vagy más jogalap

4.3.2. Jogszabály címe

A fentiek tekintetében ugyanaz az elv, mint a 1.8.1. és az 1.8.2. pontok tekintetében.

4.4. Az adattovábbítás módja

Az adattovábbítás módja alatt azt értjük, hogy konkrétan hogyan kerül át az adat az egyik szervezettől a másikig. Ez rendkívül sokféle lehet a postától az elektronikus adattovábbításig. A megfelelőt kell itt megjeleníteni.

4.5. Az adattovábbítás időpontja

Az adattovábbítási nyilvántartás fontos része ez, ám ebben az esetben az konkrét előre megszabott adattovábbítási határidőket tudjuk megfogalmazni. Így lehet eseti, vagy naptári napban meghatározott időpont.

5. Érintettek

Az érintett fogalmával korábban foglalkoztunk. Az űrlap utolsó pontja velük foglalkozik, azokkal, akiknek az adatai kezelésre kerültek.

5.1. Az érintettekre vonatkozó adatok leírása:

Ebben a tekintetben az érintettek körét kell meghatározni, akikre kiterjed az adatkezelés, pl. a szervezet munkavállalói, továbbá konkrétan megjeleníteni, hogy az esetleges eltérő csoportok, pl. szülők, gyermekek esetében milyen konkrét adatokat kezelünk.

5.2. Érintettek száma:

Amennyiben tudjuk a megfelelő számot, akkor az kell megjeleníteni, amennyiben az változó, vagy előre nem meghatározható, akkor ennek megfelelően kell ezt a pontot kitölteni.

Az űrlap utolsó pontjába (egyéb) az adatkezeléssel összefüggő esetleges további információkat szükséges beírni.

Ezzel egy adatkezelés felmérése, rögzítése meg is történt. Amennyiben a fentiek szerint járunk el, akkor feltérképezésre kerül a szervezet összes adatkezelése. A feladat azonban ennyivel még nem ér véget. Az adatkezelések egy részét ugyanis be kell jelenteni a NAIH részére. Ezzel a következő részben foglalkozunk.

IX. BEJELENTKEZÉS AZ ADATVÉDELMI NYILVÁNTARTÁSBA

Mi is ez az adatvédelmi nyilvántartás? Ki vezeti? Miért van rá szükség? Minden adatkezelésünk et tartalmazza?

Az adatvédelmi nyilvántartás egy hatósági nyilvántartás, mely az adatkezelők személyes adatokra vonatkozó adatkezeléseit tartalmazza. Maga az intézmény nem új keletű, már az Infotv.-t megelőző Avtv. is ismerte. Az adatvédelmi nyilvántartást a NAIH vezeti és mára elmondhatjuk, hogy a nyilvántartásba történő bejelentkezés sokkal rugalmasabb és hatékonyabb, mint korábban az adatvédelmi biztos idejében, ennek okáról a későbbiekben lesz szó.

Az adatvédelmi nyilvántartásnak az Infotv. által deklarált célja az érintettek tájékoztatásának elősegítése. Jelenleg ez elég nehézkes, lévén elektronikus felületen a nyilvántartás nem elérhető, de egyébként is kétséges, hogy az érintettek az adatkezelési célonként elkülönített adatkezeléseket át tudják látni, és abból meg tudják állapítani, ki milyen adatot kezel róla.

Mindezek ellenére a nyilvántartásba való bejelentkezés kötelező, mégpedig ahogy korában már említettem, adatkezelési célonként külön-külön kell bejelentkezni. Külön szerencse, hogy a saját nyilvántartásunkat is ilyen módon készítettük el. A bejelentett és a NAIH által befogadott nyilvántartás nyilvántartási számot kap, melyet az adatkezelés során mindig fel kell tüntetni.

Az adatvédelmi nyilvántartásba történő bejelentkezésnek azonban van egy nagyon fontos és hasznos hozadéka. Amennyiben az adatkezelő a bejelentkezéshez szükséges űrlapot, mellyel korábban már foglalkoztunk kitölti, akkor jó eséllyel át is gondolta saját adatkezelését, és bizonyos kontrollt valósít meg az adatkezelő részére e tekintetben. Véleményem szerint összességében segíti az adatkezelők helyes adatkezelési gyakorlatának megvalósulását.

Az Intotv. hatálya alá tartozó minden adatkezelően be kell jelenteni az adatkezeléseit a nyilvántartásba. A bejelentésben a következőknek kell szerepelnie:

- adatkezelés céljának;
- adatkezelés jogalapjának;
- az érintettek körének;
- az érintettekre vonatkozó adatok leírásának;
- az adatok forrásának;
- az adatok kezelésének időtartamának;
- a továbbított adatok fajtájának, címzettjének, és a továbbítás jogalapjának;
- az adatkezelő, valamint az adatfeldolgozó nevének, címének a tényleges adatkezelés vagy adatfeldolgozás helyének és az adatfeldolgozónak az adatkezeléssel kapcsolatos tevékenységének;
- az alkalmazott adatfeldolgozási technológia jellegének;
- illetőleg amennyiben foglalkoztat belső adatvédelmi felelőst (számos adatkezelőnek kötelező ilyet foglalkoztatni), az ő nevét és elérhetőségi adatait.

Fontos rögzíteni, hogy nem minden adatkezelést kell bejelenteni. Melyek ez? Sajnos taxatívan fel kell sorolni azokat az adatkezeléseket, melyeket nem kell bejelenteni, ugyanis csak ezek esetében tekint el az Infotv. a Hatósági nyilvántartásba történő bejelentkezéstől.

Nem kell bejelenteni a Hatóság részére a következő adatkezeléseket:

- az adatkezelővel munkaviszonyban, tagsági viszonyban, óvodai nevelésben való részvételre irányuló, tanulói vagy tanulószerződéses jogviszonyban, kollégiumi tagsági viszonyban vagy – a pénzügyi szervezetek, közüzemi szolgáltatók, elektronikus hírközlési szolgáltatók ügyfelei kivételével – ügyfélkapcsolatban álló személyek adataira vonatkozik;
- a bevett egyház belső szabálya szerint történik;
- az egészségügyi ellátásban kezelt személy betegségével, egészségi állapotával kapcsolatos személyes adatokra vonatkozik gyógykezelés vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;
- az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik;
- a hatósági, az ügyészségi és a bírósági eljárás által érintett személyeknek az eljárás lefolytatásával kapcsolatos személyes adataira, vagy a büntetés-végrehajtás során a büntetés-végrehajtással összefüggésben kezelt személyes adatokra vonatkozik;
- a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve hogy – törvényben meghatározottak szerint – az adatok érintettel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;
- a médiaszolgáltatásokról és a tömegkommunikációról szóló törvény szerinti médiatartalom-szolgáltató olyan adatait tartalmazza, amelyek kizárólag saját tájékoztatási tevékenységét szolgálják;
- a tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra,
- a levéltári őrizetbe vett iratokkal összefüggésben valósul meg.[110]

Minden más ettől eltérő adatkezelés be kell jelenteni a NAIH részére. A bejelentkezéseket azonban még mindig el kell különíteni a kötelező és a nem kötelező adatkezelések tekintetében.

A kötelező, tehát törvény vagy önkormányzati rendelet által elrendelt adatkezelések regisztrálását az elrendelő törvény hatálybalépését követő húsz napon belül kell kérvényezi a Hatóságnál. A hozzájáruláson alapuló adatkezelések esetében az adatkezelés megkezdése előtt kell a nyilvántartásba bejelentkezni, addig jogszerűen az adatkezelés nem kezdhető meg

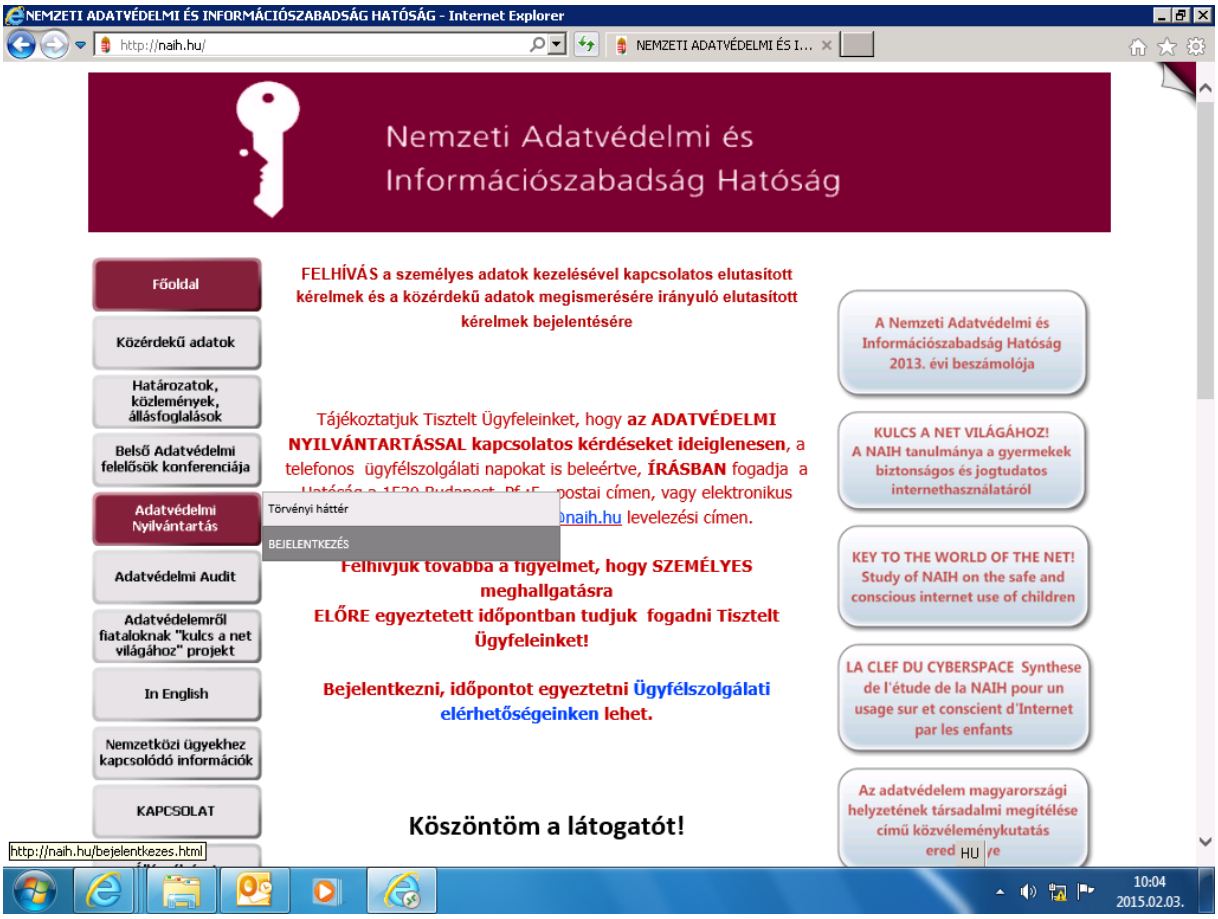
[110] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 65. § (3) bekezdés

és nem folytatható. Amennyiben változást akarunk bejelenteni, akkor a változást követő nyolc napon belül kell ezt megtenni.

Elkülönítettük tehát, hogy mely adatkezeléseket kell bejelentenünk, és azt mikor kell megtennünk. Hogyan lehet azonban magát a bejelentést megtenni?

Az adatvédelmi nyilvántartásba történő bejelentést két módon tehetjük meg. Az egyik a papír alapú bejelentkezés, a másik az elektronikus. A papír alapú bejelentkezés tekintetében az előző részben részletezett űrlapot kell kitölteni és postai úton megküldeni a NAIH részére. A Hatóság már első hivatali évében kidolgozott egy elektronikus bejelentkezési lehetőséget, melyet azóta is preferál. Az elektronikus bejelentkezés viszonylag egyszerű, azonban, hogy egyértelmű legyen, végigvezetem Önöket a folyamaton:

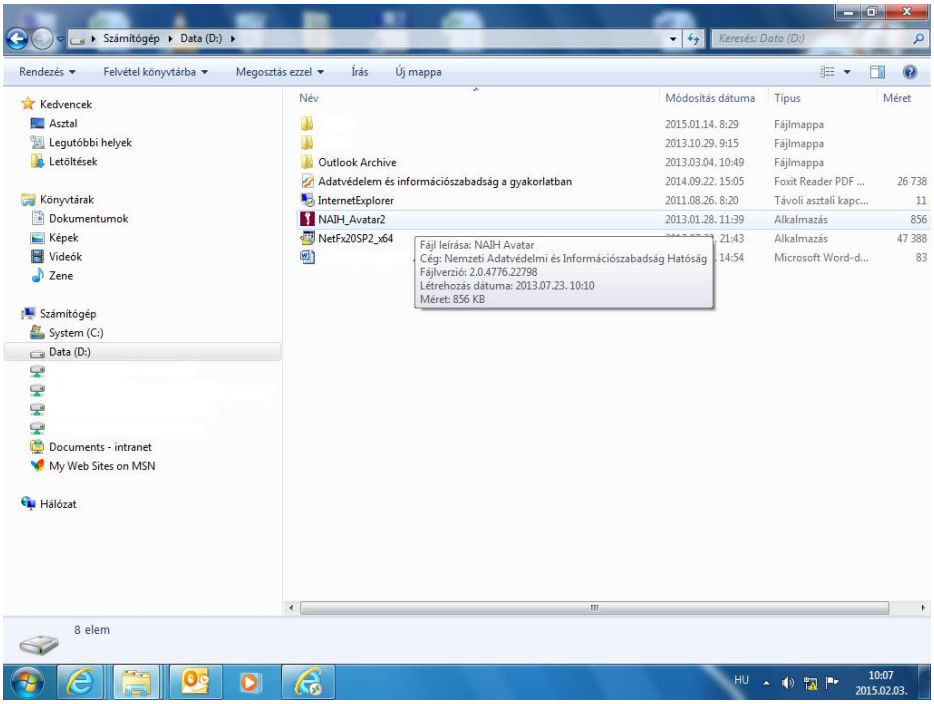
Az első teendők felkeresni az NAIH honlapját. Ezt a www.naih.hu webcímen tehetjük meg.



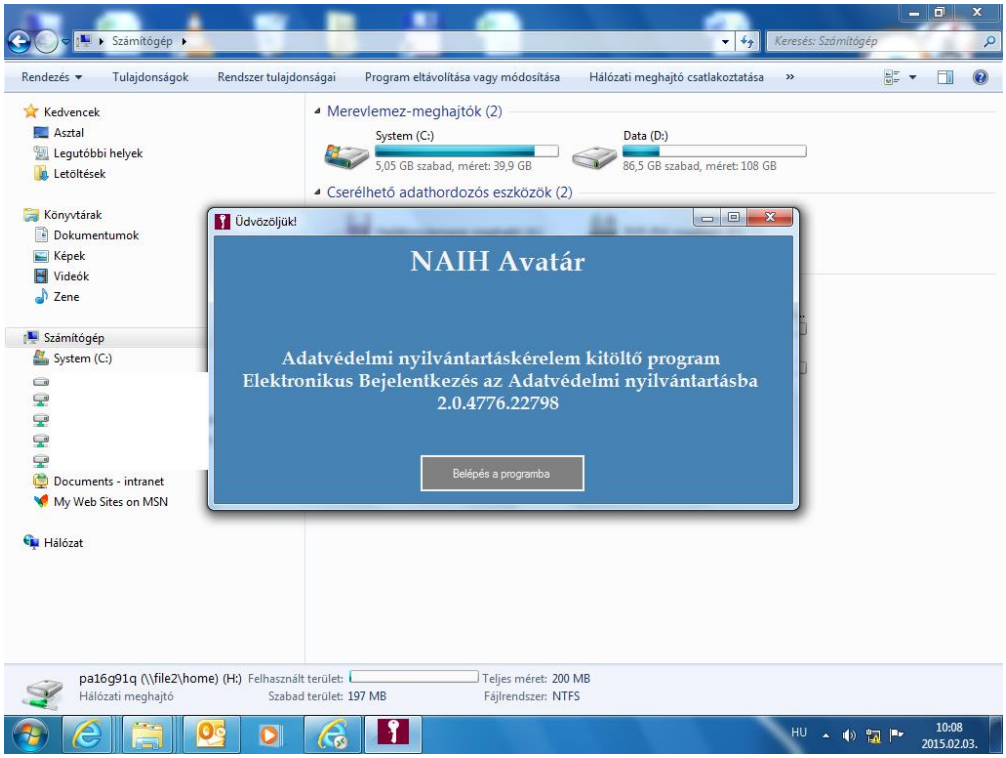
Itt a főoldalon már el is tudjuk kezdeni a munkát. Ahogyan a fenti képen látható, a főoldalról tudunk az „Adatvédelmi Nyilvántartás” fülhöz jutni, melyen két lehetőségünk van. Az egyik

az adatvédelmi nyilvántartás törvényi hátterét adja meg a látogatónak. A mi szempontunkból a „Bejelentkezés” fül a lényeges. Amennyiben erre rákattintunk a következő felületre jutunk:

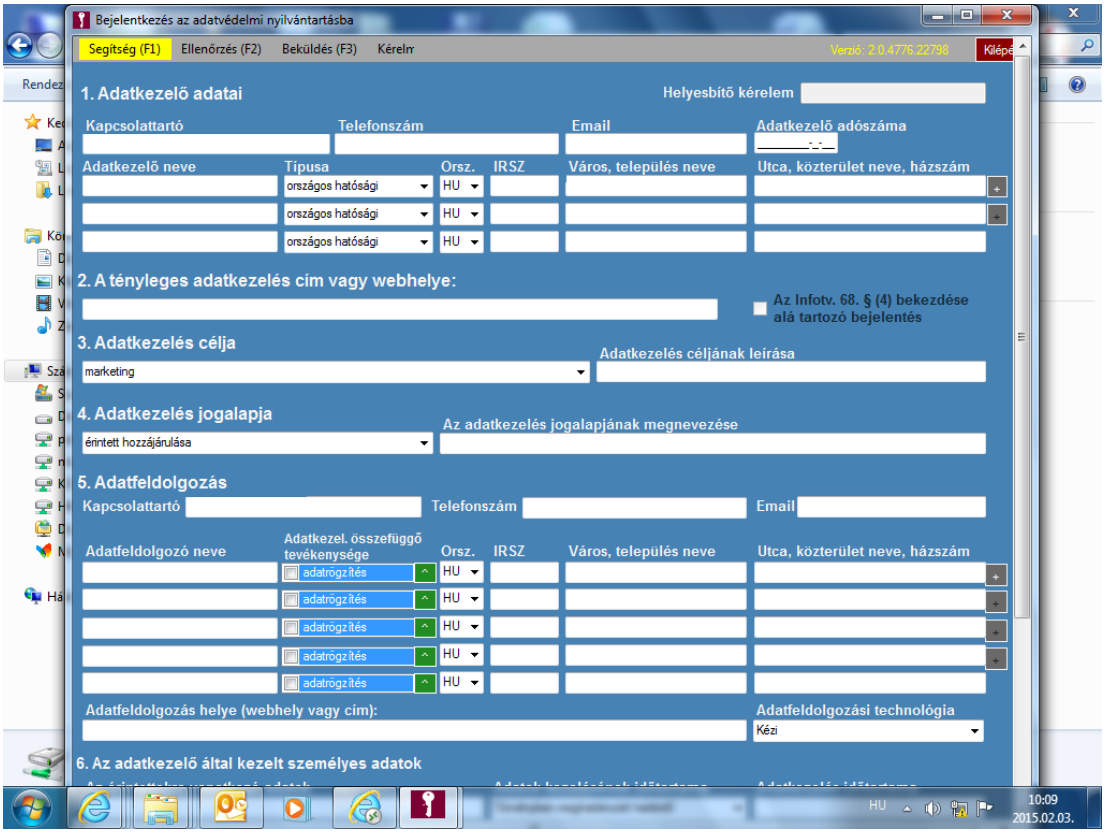
Ezen a felületen tudjuk megszerezni a bejelentkezéshez szükséges keretprogramot, illetőleg a program futtatásához szükséges szoftvert. Amennyiben a letöltés megtörtént, akkor a kijelölt meghajtón látni fogjuk a NAIH avatart a lentiek szerint:



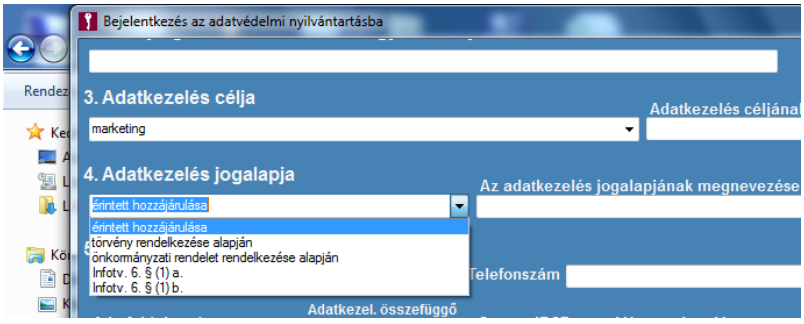
Amennyiben a NAIH avatar ikonra rákattintunk, el is indul a program, és már csak be kell lépni:



Amennyiben beléptünk a következő felület fogad bennünket, ahol el is tudjuk kezdeni az érdemi munkát.



Az első két pont kitöltése értelemszerűen történik. Azonban a harmadik pont esetében már egy legördülő menüből tudjuk kiválasztani az adatkezelés célját. Esetünkben ez a „marketing” lett. Az adatkezelés céljának leírását ebben az esetben is nekünk kell megfogalmaznunk, ugyanazok a feltételek, mint amit az adatvédelmi nyilvántartás részben részletesen kifejtettem. A következő pont az adatkezelés jogalapja, melyet a lenti módon tudunk megjeleníteni:

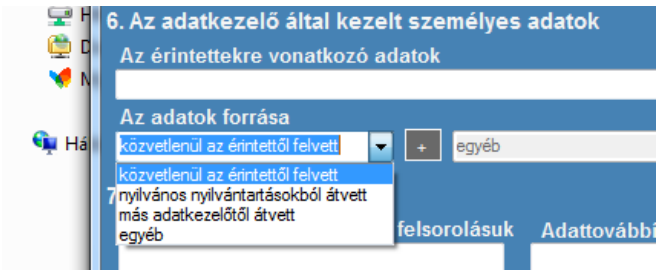


Látható, hogy öt lehetőség adott. Az első három (érintett hozzájárulása, törvény, önkormányzati rendelet) opciót az korábbiakban részletesebben megtárgyaltuk, ezek egyértelműek, az Infotv. 6. § (1) bekezdés a), és a 6. § (1) bekezdés b) pontjai pedig a szintén

megtárgyalásra került olyan adatkezelések, ahol a hozzájárulás beszerzése lehetetlen vagy aránytalan költséggel járna. Az a) pont esetén az adatkezelő jogi kötelezettségének teljesítése az elérendő cél, míg a b) pontban az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges az adatkezelés. A példánkban az érintett hozzájárulását választottuk. Az adatkezelés jogalapjának megnevezésénél a konkrét jogszabályt és annak pontos helyét kell meghatározni, természetesen, ha itt hozzájáruláson alapul az adatkezelés, akkor ezt a részt üresen kell hagyni.

A felület következő (5.) pontja az Adatfeldolgozás. Ennek a pontnak a kitörlésében segítséget jelentenek a korábban tanultak, de e tekintetben nagyon egyszerű és pontosan kitölthető felületek állnak rendelkezésre.

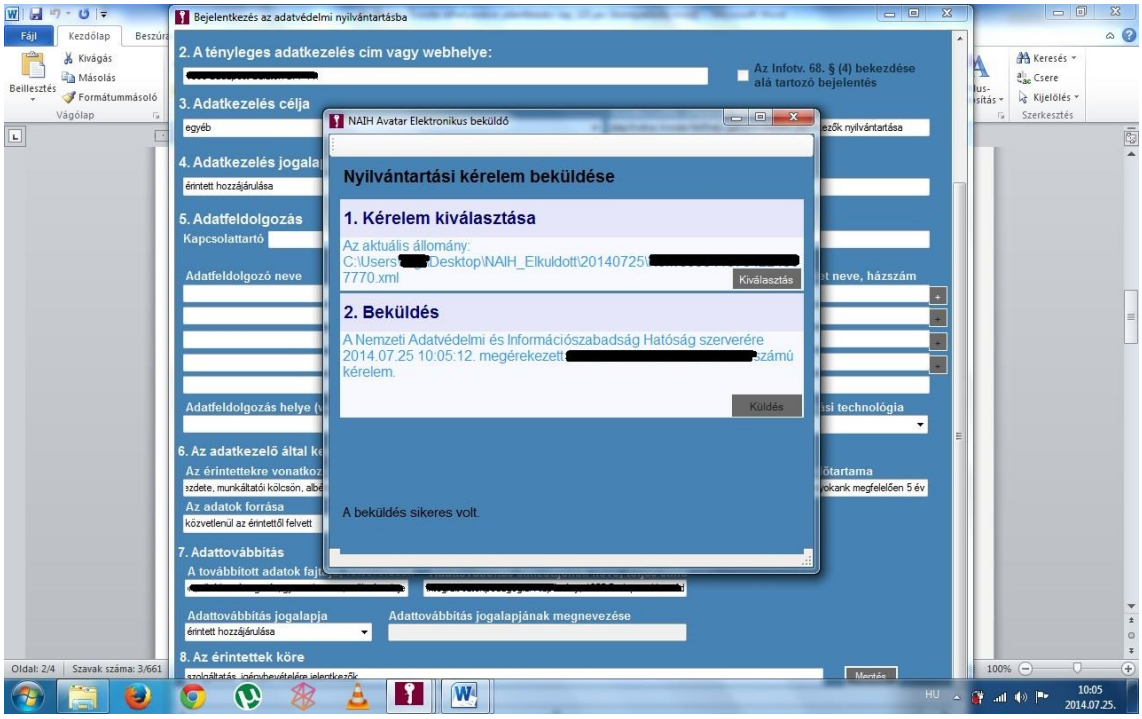
A keretprogram 6. pontja az adatkezelő által kezelt személyes adatok címet viseli. A korábban tanultak alapján ez a rész is könnyen kitölthető. Az első kérdés az érintettre vonatkozó adatok, mely megegyezik az űrlap hasonló pontjával (5.1.), így ugyanaz vonatkozik a kitöltésére itt is. Az adatok forrása szintén legördülő menüből választható ki, az alábbiak szerint:



Látható, hogy a „+” jellel több lehetőséget is megjelölhetünk.

A program további pontjainak kitöltése értelemszerűen, illetőleg az űrlap megfeleltethető pontjai esetében elmondottaknak megfelelően történik.

Amennyiben sikeresen kitöltöttük az összes felületet, az adatlap készen áll arra, hogy beküldjük a Hatóság részére. Ezt olyan számítógéppel lehet elérni, amin internetelérés van, ugyanis a beküldés online történik. Sikeres beküldés esetén a következő „választ” kapjuk:



A papíralapú vagy az elektronikus belejelentkezésnek a Hatósághoz történő beérkezését követően a NAIH-nak nyolc napja van, hogy a kérelmet elbírálja. Amennyiben ez megtörténik, a Hatóság a nyilvántartási szám megküldésével értesíti az adatkezelőt, aki így megkezdheti az adatkezelést. Abban az esetben, ha a Hatóság a nyolc nap eltelte után nem értesíti az adatkezelőt, az adatkezelés megkezdhető.

Felmerül a kérdés, hogy milyen hatályúnak tekinthető az adatvédelmi hatósági nyilvántartás. Két eset lehetséges. Az egyik, hogy a nyilvántartás konstitutív, tehát a jogviszonyt maga a közhatalmi aktus hozza létre, módosítja, illetve szünteti meg. A másik a deklaratív hatályú nyilvántartás, mely a jogviszony keletkezésére, módosulására, megszűnésére nem hatnak ki, csupán megállapítják ezeket a tényeket és alkalmasak a jogi helyzet tanúsítására. Az adatvédelmi nyilvántartás deklaratív, mert nem a bejegyzés hozza létre az adatkezelést, a nyilvántartási szám az adatkezelés azonosítására szolgál, és nem tanúsítja a nyilvántartásba vett adatkezelés jogszerűségét. A nyilvántartási szám birtokában lévő adatkezelők sokszor magát a számot az adatkezelés engedélyező számaként definiálják, azonban ez nincs így.

A Hatóságtól megkapott nyilvántartási számot az adatkezelőnek az adatok minden továbbításánál, nyilvánosságra hozatalánál, és az érintettnek való kiadásakor fel kell tüntetni.

Fontos tudnivaló, hogy a Hatósági nyilvántartásba vétel az Infotv. szerint a kötelező adatkezelések kivételével díjköteles, ám a szolgáltatási díjról szóló kormányrendelet kiadásáig díjat nem kell fizetni.

X. KÖZÉRDEKŰ ADATOK

Az Infotv. értelmező rendelkezéseiben találjuk meg a meghatározását, melynek alapján *közérdekű adat:* az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

A meghatározásból az alábbiak állapíthatók meg:

- állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv, amelyet rövidítsünk, közfeladatot ellátó szervnek
- a fenti szerv kezelésében lévő és keletkezett adatok, bármilyen formában és módon rögzített és kezelt információ és ismeret,
- személyes adat fogalma alá nem eső adat
- teljesség igénye nélküli felsorolás: így különösen, hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésre, birtokolt adatfajtákra, működést szabályzó jogszabályokra, gazdálkodásra és a megkötött szerződések

A közérdekű adatokat felsorolás szintjén nem is lehet meghatározni, és nem is lehet általános mindenkor használható szabályokat felállítani rá, egyszerűbb és célravezetőbb, ha a kivételeket állapítjuk meg, nevezzük őket a megismerés korlátainak. Az egyik ilyen korlát ebben az értelmező szabályban jelenik meg, „személyes adat fogalma alá nem tartozó." Megállapíthatjuk tehát, hogy a személyes adatok főszabályként nem közérdekű adatok, de erre még visszatérek, hiszen a közérdekből nyilvános adatok csoportjánál meglátjuk, hogy azok között mégiscsak találunk személyes adatokat. A közérdekből nyilvános adat meghatározása ennél a pontnál, azért válik fontossá, mert a közérdekű adatok megismerése című fejezetben a közérdekű adatok mellett párhuzamosan megjelenik a közérdekből

nyilvános adat is, és ugyanazon szabályok vonatkoznak rá, mint az előzőekben kiemelt adatcsoportra.

Ahogy már megtanultuk az információszabadság alapjog, melyet az Alaptörvény szabályoz. Az alaptörvényi szabályozás az Infotv. 26. § (1) bekezdésben jelenik meg, az alábbiak szerint:

Az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szervnek vagy személynek (a továbbiakban együtt: közfeladatot ellátó szerv) lehetővé kell tennie, hogy a kezelésében lévő közérdekű adatot és közérdekből nyilvános adatot - az e törvényben meghatározott kivételekkel - erre irányuló igény alapján bárki megismerhesse.

Az Infotv. kísérletet tesz arra, hogy a közérdekből nyilvános adat határait kijelölje részben a taxative felsorolással, részben más törvények megjelölésével

Közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja. A közérdekből nyilvános személyes adatok a célhoz kötött adatkezelés elvének tiszteletben tartásával terjeszthetőek. A közérdekből nyilvános személyes adatok honlapon történő közzétételére az 1. melléklet és a közfeladatot ellátó személy jogállására vonatkozó külön törvény rendelkezései irányadóak

A személyes adatok tehát, akkor válnak közérdekből nyilvános adattá, ha azt az Infotv. 26. (2) bekezdése, vagy a közfeladatot ellátó szerv működésére vonatkozó, nevezzük „ágazati" törvénye ezt meghatározza.

1. A közérdekű adatok megismerési korlátai

Az Infotv. 27. § (1)-(8) bekezdés tartalmazza a közérdekű adat megismerésének korlátait. Az előzőekben az említett személyes adatok kategóriáján kívül elsődleges szerepet kap a minősített adat védelméről szóló törvény szerinti minősített adat. A Mavtv[111] törvény váltotta fel a nevében ismerős fogalmakat takaró államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvényt. A Mavtv. eltérő minősítési szinteket határoz meg, mind jogelődje. Amely mindkét törvényben azonos, hogy a minősítéssel védhető közérdeket védi. Olyan adatokat véd tehát a törvény, amely a közérdekű vagy a közérdekből nyilvános adatok csoportjába tartozik,

[111] A minősített adat védelméről szóló 2009. évi. C. tv.

de a minősítőnek az adattartalma miatt védenie kell. Melyek tartoznak a minősítéssel védhető közérdek kategóriájába?

Magyarország szuverenitása, területi integritása, alkotmányos rendje, honvédelmi, nemzetbiztonsági, bűnüldözési és bűnmegelőzési tevékenysége, igazságszolgáltatási, központi pénzügyi, gazdasági tevékenysége, külügyi vagy nemzetközi kapcsolatai, állami szerve illetéktelen külső befolyástól mentes, zavartalan működésének biztosítása.

A minősítési szintek az alábbiak szerint változnak: amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele.

- - rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor „**Szigorúan titkos!”,**
- - súlyosan károsítja a minősítéssel védhető közérdeket, akkor „**Titkos!”,**
- - károsítja a minősítéssel védhető közérdeket, akkor „**Bizalmas!”,**
- - hátrányosan érinti a minősítéssel védhető közérdeket, akkor „**Korlátozott terjesztésű**!”
- minősítési szintű.

A kármérték meghatározásához irányadó szempontokat a törvény 1. számú melléklete tartalmazza.

Az érvényességi idő:

- - „Szigorúan titkos!” és „Titkos!” minősítési szintű adat esetén legfeljebb 30 év,
- - „Bizalmas!” minősítési szintű adat esetén legfeljebb 20 év,
- - „Korlátozott terjesztésű!” minősítési szintű adat esetén legfeljebb 10 év

A következő megismerési korlát, ha az adatfajták meghatározásával törvény az alábbi cél érdekében elrendeli a korlátozást.

- honvédelmi érdekből;
- nemzetbiztonsági érdekből;
- bűncselekmények üldözése vagy megelőzése érdekében;
- környezet- vagy természetvédelmi érdekből;
- központi pénzügyi vagy devizapolitikai érdekből;
- külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra tekintettel;

Fontos szem előtt tartani, hogy nem elég, hogy a korlátozás célja megfelelő legyen, vagyis tényleg nemzetbiztonsági vagy bűnmegelőzési érdek álljon fenn, hanem azt törvénynek konkrétan kell tartalmaznia. Nem általános korlát, hanem konkrét törvényben jelölt cél érdekében használható.

További megismerési korlátokat jelent, ha a bírósági vagy közigazgatási hatósági eljárás van folyamatban valamint a szellemi tulajdonhoz fűződő jogra tekintettel is korlátozható az adatok megismerése.

A bírósági vagy közigazgatási hatósági eljárásra és a szellemi tulajdonhoz fűződő jogra tekintettel történő korlátozás is csak konkrét adatigényeknél, a közérdekű adat birtokában lehet figyelembe venni.

Az üzleti titok meghatározása a korábbi Polgári Törvénykönyvben kapott helyet, az Új Polgári Törvénykönyv a rá vonatkozó szabályozásokat már csak fogalmi szinten alkalmazta, és ezzel egy időben a konkrét szabályozás az Infotv-ben[112] kapott helyet. Ennek értelmében a közérdekből nyilvános adatként nem minősül üzleti titoknak a központi és a helyi önkormányzati költségvetés, illetve az európai uniós támogatás felhasználásával, költségvetést érintő juttatással, kedvezménnyel, az állami és önkormányzati vagyon kezelésével, birtoklásával, használatával, hasznosításával, az azzal való rendelkezéssel, annak megterhelésével, az ilyen vagyont érintő bármilyen jog megszerzésével kapcsolatos adat, valamint az az adat, amelynek megismerését vagy nyilvánosságra hozatalát külön törvény közérdekből elrendeli. A nyilvánosságra hozatal azonban nem eredményezheti az olyan adatokhoz - így különösen a védett ismerethez - való hozzáférést, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségé

A módosítás értelmében a közfeladatot ellátó szervezetnek nem lehet üzleti titka, kivételt képez az új ismeret, ennek a megismerésénél a szükségesség arányosság elvének alkalmazásával kell mérlegelni, hogy az adott ismeret megismerhető-e.

A közérdekű adatok megismerése korlátozható uniós jogi aktus alapján az Európai Unió jelentős pénzügy- vagy gazdaságpolitikai érdekére tekintettel, beleértve a monetáris, a költségvetési és az adópolitikai érdeket is[113].

[112] Infotv.27. § (3) bekezdés
[113] Infotv. 27. § (4) bekezdés

Talán legtöbbször használt korlát a döntés előkészítésére, a döntésmegalapozását szolgáló iratokra való hivatkozás[114].

A közfeladatot ellátó szerv feladat- és hatáskörébe tartozó döntés meghozatalára irányuló eljárás során készített vagy rögzített, a döntés megalapozását szolgáló adat a keletkezésétől számított tíz évig nem nyilvános. Ezen adatok megismerését - az adat megismeréséhez és a megismerhetőség kizárásához fűződő közérdek súlyának mérlegelésével - az azt kezelő szerv vezetője engedélyezheti.

A közfeladatot ellátó szervnek a döntés megalapozását szolgáló adata 10 évig nem nyilvános, megismerését a szerv vezetője a szükségesség arányosság elvének mérlegelésével engedélyezheti. A jogszabály külön szabályozza azt az esetet, mikor a döntés már megszületett és ezt követően kerülne sor a döntés megalapozását szolgáló adatok korlátozására. Ilyenkor ugyanis a megismerés már csak akkor korlátozható, ha az adat megismerése a közfeladatot ellátó szerv törvényes működési rendjét vagy feladat – és hatáskörének illetéktelen külső befolyásolástól mentes ellátása, így különösen az adatot keletkeztető álláspontjának a döntések előkészítése során történő szabad kifejtését veszélyeztetné.

A mérlegelés tehát itt a közérdek nyilvánossága és a közérdek törvényes működése között zajlik. Ez még a közérdekű perekben döntő bíróságok számára sem egyszerű feladat. gyakorlati tapasztalatom szerint csak nagyon kis százalékban sikerül a megismerés korlátozását erre a bekezdésre alapozni. Amennyiben a megismerés tárgya maga a döntés, az Infotv. nem is szól, tehát maga a döntés korlátozása ennek alapján nem lehetséges.

Jogszabály a döntés megalapozását szolgáló egyes adatok megismerhetőségének korlátozására a 10 évnél rövidebb időtartamot állapíthat meg.

2. Közérdekű adat megismerése iránti igény

A közérdekű adat megismerése iránt szóban, írásban vagy elektronikus úton bárki igényt nyújthat be[115].

Bárki és bárhogy, röviden így definiálhatjuk a szabályt. Ennek a pontos meghatározására szabályokat kell alkotnunk, amelyben rögzíteni kell, hogy pontosan szóban mely szervezeti egységnél, elektronikusan, mely email címen, írásban mely postai címre kell küldenie. A

[114] Infotv. 27. § (5)-(6) bekezdés
[115] Infotv. 28. §(1) bekezdés

szabályokat azért érdemes meghatározni, mert ebben az esetben a szervezethez érkező adatigényeket át lehet látni, egységesen lehet kezelni. A közérdekű adat megismerésére vonatkozó szabályokat a szervezetnek a honlapján közzé kell tennie az Infotv. általános közzétételi listája alapján. A szabályok meghatározhatnak külön e-mail címet az adatigények fogadására. Tekintettel arra, hogy az e-mailek fogadása sok esetben auomatikus válaszadással történik, az adatigénylő értesítést kap az adatigényének fogadásáról. Amennyiben ez az e-mail cím kizárólag az Infotv. szerinti adatigények fogadására van fenntartva, az automatikus üzenet további használható információkat tartalmazhat, pl meghatározhatja a megválaszolására illetékes szervezeti egységet és a határidőt is.

Mi történik akkor, ha egy adatigény nem honlapon közzétett módon érkezik be az adott adatkezelő szervhez? Például elképzelhető, hogy az adatigénylő egy szervezeti egység e-mail címére vagy postai címére küldi be az adatigényét. Hivatkozhat az adatkezelő szerv arra, hogy nem az általa meghatározott módon érkezett be az adatigény? Azt kell mondanom, hogy csekély eséllyel hivatkozhat rá, mivel a törvény előzőekben idézett bekezdése bárkit feljogosít arra, hogy szóban, írásban, elektronikusan adatigényt nyújtson be. A belső szabályozás akkor érvényes, ha azt az érintett felek megismerhetik a honlapon. Ha azonban valaki nem tud arról, hogy vannak belső szabályok és csak az Infotv.-t ismeri vagy az Alaptörvényben foglaltakról hallott, akkor is jogában áll közérdekű adat megismerésére igényt benyújtani az általa választott szervezethez. Ezért a szervezet belső adatvédelmi felelősének, vagy a közérdekű adatok megismerésére kijelölt személynek kellő tájékoztatást kell adnia a szervezet minden szervezeti egységének, hogy az ily módon beérkezett adatigényeket felismerjék és az Infotv. szerinti szabályok alapján válaszolják meg. Korábban már említettem, hogy a belső adatvédelmi felelősnek minden szervezeti egység munkájára rá kell látnia, ez éppen egy ilyen kapcsolódási pont.

Érdemes ismételten kitérni a közérdekből nyilvános adatokra, mivel a megismerésükre a közérdekű adatok megismerésére vonatkozó rendelkezéseket kell alkalmazni. Ha tehát egy közérdekű adatigény közérdekből nyilvános adat megismerésére terjed ki a választ a fenti szabályok alapján kell teljesíteni.

Az adatigénylő személyes adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez és a másolatkészítésért megállapított költségtérítés megfizetéséhez szükséges. Az igény teljesítését, illetve a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell.

A közérdekű adatigényekről a belső adatvédelmi felelős nyilvántartást vezet. A fentiekre tekintettel az adatigények tárgyát és idejét célszerű feltüntetni a nyilvántartásban, mivel az adatigénylő neve a teljesítést követően nem kezelhető.

3. Az adatigény megvizsgálása, teljesítése vagy elutasítása

Az adatigényt a megérkezést követően be kell iktatni az adott szerv iratkezelő rendszerébe (papír vagy elektronikus). Az iktatás a szerv belső iratkezelés szabályzata alapján kell, hogy megtörténjen. Az iktatásnak főszabályként legkésőbb a következő munkanapon meg kell történnie. Amennyiben az adatigény munkaszüneti nap előtt érkezik munkaidőben, az adatigényt aznap be kell iktatni, ha azonban munkaidőn kívül érkezik, elég, ha a munkaszüneti napot követő első munkanapon történik az iktatás. Ez azért nagyon fontos, mert a határidő számítás ettől a naptól kezdődik. És amennyiben az elutasítást követő megismerési perben a felperes a határidő számítással nem ért egyet, az iratkezelési szabályzatra tudunk hivatkozni.

Meg kell vizsgálni, hogy az adatigény egyértelmű-e, mert ha nem, akkor az akkor érdemes az adatigénylőt a pontosításra felhívni. A pontosítást olyan módon kérjük, ahogy az igénylő a válasz megküldését kérte, ennek hiányában, ahogyan az adatigény megérkezett.

Tekintettel arra, hogy az Infotv. nem rendelkezik arról, hogy ez halasztó hatályú-e a válaszadásra, érdemes írásban az igénylőt tájékoztatni, hogy a pontosítást mondjuk 8 napon belül nyújthatja be és ennek elmaradása esetén az adatigényt visszavontnak tekinti az adatkezelő szerv. Itt nagyon fontos, hogy a pontosítás nélkül valóban értelmezhetetlen legyen az igény. A pontosítás megérkezésekor a 15 napos határidő újból indul.

Az Infotv. módosításai 2015. október 1-én lépnek hatályba, amelynek legfontosabb eleme az adatigénylésekért megállapítható költségek bevezetése. Eddig is lehetséges volt az adatkezelő szerv számára költségeinek a felszámolása, de a törvényalkotó nem szabályozta annak mértékét. Így egy esetleges jogvitában a bíróság vagy a NAIH döntött. A költségek megállapításának részleteit az előkészítés alatt álló végrehajtási rendelet fogja szabályozni. Új fogalomként jelenik meg a módosításban a „munkaerőforrás „Ennek értelmében[116], ha az adatigénylés jelentős terjedelmű, illetve nagyszámú adatra vonatkozik, vagy az adatigénylés teljesítése a közfeladatot ellátó szerv alaptevékenységének ellátásához szükséges munkaerőforrás aránytalan mértékű igénybevételével jár, a határidő egy alkalommal 15

[116] Megállapította: 2015. évi CXXIX. törvény 5. § (4). Hatályos: 2015. X. 1-től.

nappal meghosszabbítható. Erről az igénylőt az igény beérkezését követő 15 napon belül tájékoztatni kell. Fontos változás még, hogy erről az igénylőt az igény beérkezését követő 15 napon belül kell tájékoztatni, és nem az eddig megszokott 8 napon belül.

A jelenlegi szabályozás az alábbiakat tartalmazza.

Az Infotv 29. § (3) bekezdése értelmében az adatokat tartalmazó dokumentumról vagy dokumentumrészről, annak tárolási módjától függetlenül az igénylő másolatot kaphat. A másolási költség felszámolása két esetben lehetséges az Infotv. alapján. Az első esetben a törvényalkotó, csak a lehetőségét körvonalazza, és nem fűz hozzá mennyiségi korlátozást, míg a másik esetben akkor teszi lehetővé költség megfizettetését, ha az igényelt adat jelentős terjedelmű.

Mindkét esetben az adatigénylőt a másolatkészítés során felmerülő költségekről és ezeknek a megfizetéséről írásban 8 napon belül tájékoztatni kell. A költség felszámolása a módosítás után sem lesz kötelező, természetesen a dilemma a nagy terjedelmű adatszolgáltatásoknál lesz. Mondjuk több ezer oldalas pályázati anyag megküldése esetén a papír és egyéb költség már tetemes költségre rúghat. Ilyenkor lehet érvényesíteni a költségeket.

A jogszabályi meghatározásra szükség volt a költségek megállapításánál, hiszen a NAIH által vizsgált esetek is arról tanúskodnak, hogy az adatkezelők nagyon különbözően értelmezték a költségek megállapítását. Ezekről a NAIH határozataiban olvashatunk.[117]

A saját gyakorlati tapasztalatom alapján a munkáltatóm a közérdekű adat megismerésére vonatkozó adatigény teljesítésekor még nem állapított meg költséget, figyelemmel arra, hogy a költség megállapításáról szóló tájékoztatás és a költség mértéke meghosszabbítaná az adatigénylés teljesítésének határidejét és korlátokat szabna bizonyos adatigénylők vonatkozásában.

Ez azonban nem jelenti azt, hogy kirívó példák esetében költségfelszámítást ne tartanánk elfogadottnak.

A költségek megállapításánál azonban időszerűnek találom megemlíteni az anonimizálással járó feladatokat és ezek fontosságát. Ennek a feladatnak a lelkiismeretes ellátása során az adott dokumentumot nagy figyelemmel át kell olvasni és meg kell állapítani, hogy mely

[117] http://www.naih.hu/hatosagi-hatarozatok---vegzesek.html

adatok ismerhetők meg belőle és melyek korlátozhatók. Maradjunk a pályázat példájánál, egy ilyen esetben is felmerülhetnek személyes adatok a dokumentumokban, amelyeket tételesen fel kell tárni. Példa: A pályázó megnevezi az általa foglalkoztatni kívánt személyeket név szerint. Az adatok felismerhetetlenné tétele szaktudást kíván meg, ezért mikor arról döntenek a törvényalkotók, hogy mely intézménynek mekkora a jelentős terjedelmű dokumentum, akkor azt is vegyék figyelembe, hogy az adatszolgáltatást nem az intézmény által foglalkoztatott személyek összessége végzi, hanem 1-2 fő. Így a 100 db mindenkinek 100 db. Az adatszolgáltatások során felmerülő dokumentumok kiadása nem futószalagszerűen automatizált gépekkel történnek, hanem megelőzik őket tartalmi vizsgálat.

Ahogy tehát példával illusztráltam az adatigény tárgyát képező dokumentum meg nem ismerhető adatait anonimizálni kell. Hiszen arra az adatkezelő nem hivatkozhat megtagadása során, hogy azért nem adja ki az adatokat, mert azok meg nem ismerhető adatokat is tartalmaznak.

Az Infotv. módosításában már szerepel a munkaerőforrás aránytalan igénybe vétele kifejezés, de úgy tűnik, hogy ez konkrétan nem tartalmazza az anonimizálással járó munkaidőt. Nem vonom kétségbe, hogy ezen tevékenységet bele lehet érteni a munkaerőforrás fogalmába, de a konkrét alkalmazhatóságot véleményem szerint így is csak a gyakorlat fogja meghozni.

Jelenlegi szabályozás szerint az adatigénylést közérthető formában, amennyiben aránytalan nagy költséggel nem jár az adatkezelő szervezetnek az igénylő által kért formában kell megküldeni. Amennyiben az adatokat már nyilvánosságra hozták, az Infotv lehetővé teszi, hogy az adatigényt a nyilvános forrás megjelölésével teljesüljön. Azonnal felmerül egy kérdés, mit takar a nyilvánosságra hozták kifejezés. Természetesen vannak olyan nyilvánosságra hozott dokumentumok, amelyek hivatalos formában kerülnek közzétételre, pl jogszabályok stb. Ha azonban a közzététel nem hiteles forrásból történt, adott esetben egy másik szerv hozta nyilvánosságra, és esetleg az adott dokumentum rendelkezésre állását sem lehet megállapítani, célszerűbb, ha az adatkezelő szerv a hiteles forrásból küldi meg a kért adatokat. Szakmailag és az adat rendelkezésre állása szempontjából is szükséges megvizsgálni a kért adatokat vagy a nyilvános forrást.

Megtagadás: az igény teljesítésének megtagadásáról, annak indokaival az adatigénylőt 8 napon belül írásban tájékoztatni kell az Infotv-ben[118] megjelölt jogorvoslati lehetőségek felsorolásával együtt.

4. Megtagadás indokai

1. nem állnak rendelkezésre az adatok
2. nem létezik az adat
3. megismerés korlátai vonatkoznak rá, pl: Mavtv., új ismeret, személyes adat stb.,
4. nem abban a formában teljesítik az adatigényt

Az első két megtagadás, különösebb indokolást nem igényel, mert amely tényleges nincsen a szerv kezelésében, azt nem lehet megküldeni. Saját véleményemet osztom meg, mikor itt hivatkozom az Infotv. 26. § (1) bekezdésében foglaltakra, amely azt mondja, hogy a közfeladatot ellátó szervnek lehetővé kell tennie a kezelésében lévő közérdekű és közérdekből nyilvános adatok megismerését. Vagyis csak a kezelésében lévő adatok megismerését kell elősegíteni, amely adat nincsen a kezelésében azt nem. Egy esetleges közérdekű adatigény perben, az ilyen megtagadás esetében a felperesre, azaz az igénylőre hárul annak bizonyítása, hogy az igényelt adat közérdekű vagy közérdekből nyilvános és az adatkezelő szerv kezelésében van. A kezelésében kifejezés értelmezésével is gondok vannak, a kérdés az, hogy birtokolni kell-e a közérdekű adatot adatkezelés közben. A bírósági gyakorlat azt mutatja, hogy a kezelés tényleges birtoklást jelent.

Amennyiben a megtagadás azért következik be, mert a megismerésnek az Infotv.-ben meghatározott korlátai vannak, az indokolásnak ki kell térni a megtagadás részleteire, a megtagadás alapját szűken kell értelmezni, és a közérdekű adat megismerésére irányuló igény teljesítése kizárólag abban az esetben tagadható meg, ha a megtagadás alapjául szolgáló közérdek nagyobb súlyú a közérdekű adat megismerésére irányuló igény teljesítéséhez fűződő közérdeknél.

A megtagadott adatigényekről nyilvántartást kell vezetni a szervnek és minden év január 31-ig az erről szóló tájékoztatót meg kell küldeni a Hatóság részére.

[118] Infotv. 31. §

Bírósághoz fordulhat az adatigénylő:

- megtagadás esetén,
- a teljesítési határidő eredménytelen eltelte után,
- költségtérítés került megállapítva és ennek mértékével nem ért egyet.

A határidők elteltét követő 30 napon belül kell a pert megindítani.

A megtagadás jogszerűségét és a költségtérítés mértékének megalapozottságát az adatkezelő szervnek kell bizonyítani. Kivételt képez, ha az adat nem létezik, vagy nem áll az adott szerv kezelésében, mert akkor az előzőekben már leírtak alapján az igénylőt terheli a bizonyítási kötelezettség.

5. Eljáró bíróságok:

- Törvényszék
- Járásbíróságok
- Pesti Központi Kerületi Bíróság

A perbe a Hatóság beavatkozhat.

Főszabályként a közérdekű adat megtagadása ügyében az igénylő a Hatósághoz is fordulhat sortartás nélkül.

A Hatóságnak az Infotv. speciális eljárást biztosít azokban az esetekben, mikor a közfeladatot ellátó szerv gazdálkodásának átfogó, számlaszintű, illetve tételes ellenőrzésére irányuló adatmegismerés elutasításra kerül, az adatigénylő az Infotv. 52. § alapján a Hatóságnál bejelentéssel vizsgálatot kezdeményezhet.

6. A közérdekű adat megismerése iránti igény (példa)

A közérdekű adatigénylő az adott közfeladatot ellátó szervhez az alábbi kérdést intézi.

Kérem, hogy az Infotv. 28. § alapján küldje meg e-mail címemre az Integritás tanácsadó 2. pályázattal kapcsolatos tananyagfejlesztéseket és az erre vonatkozó szerződéseket.”

Elsősorban azt kell megvizsgálni minden adatigénynél, hogy a címzett szerv kezeli –e a kért adatokat. Amennyiben az adatigény, ahhoz a szervhez érkezett be, amely a tananyagot megrendelte, vagy a pályázatot kiírta és amely az arra vonatkozó szerződést megkötötte, akkor a címzett az adatkezelő szerv. Második lépésben azt kell megállapítani, hogy az adatok valóban rendelkezésre állnak-és megismerhetők-e. Meg kell tehát állapítani, hogy melyik szervezeti egység feladat és hatáskörébe tartozik a kérdés, ebben az Szervezet Működési Szabályzat is segít. Az adott főosztály lesz, tehát az adatkezelő, aki az adatokat szolgáltatja. Az adatigény megválaszolása történhet közvetlenül az adatkezelő szervezeti egységen keresztül, míg az adott szerv közérdekű adatokra vonatkozó szabályzata alapján a belső adatvédelmi felelős feladatkörébe is tartozhat a válaszadás. Olyan feladat megosztás is elképzelhető, ahol a belső adatvédelmi felelős az adatigény megválaszolására javaslatot tesz, amelyet az adatkezelő szerv figyelembe vesz és teljesíti vagy nem teljesíti az adatok kiadását. Azt azonban mindenképen ajánlom, hogy a belső adatvédelmi felelős tájékoztatást kapjon a beérkezett és megválaszolt adatigényekről, tekintettel arra, hogy az Infotv. 30. § (3) bekezdése értelmében a Hatóságnak az elutasított adatigényekről tárgyévet követően január 15-ig tájékoztatást kell küldeni az adott adatkezelő szervnek. Ennek a nyilvántartása és határidőre történő megküldése egységes rálátás és feladatkört igényel, amelyet a belső adatvédelmi felelős tud elvégezni.

Harmadik feladatként jelentkezik a meglévő adatok megismerési korlátainak a megállapítása az Infotv. 27. § alapján. Meg kell állapítani, hogy a kért adat a Mavtv. szerint nem minősített adat-e.

A korlátozást az adatfajták meghatározásával törvény is előírhatja. Ebben az esetben mindig konkrét törvényi hivatkozásra van szükség, nem elegendő, hogy bűncselekmények üldözése vagy megelőzése legyen a korlátozó ok, az adott ágazati törvényben szerepelni kell a korlátozásnak. Ilyen konkrét törvényben megfogalmazott korlátozás olvasható a honvédelmi törvényben, amely lehetővé teszi az adatok megismerésének korlátozását honvédelmi érdekből 30 év időtartamra A nemzetbiztonsági törvény szintén tartalmaz megismerési korlátokat bizonyos adatcsoportokra.

Az üzleti titok közpénzek felhasználásánál nehezen képzelhető el. Az üzleti titok fogalma alá nem eső védett ismeret fogalmát a régi Ptk. eddig is ismerte, az Infotv- be azonban az Új Ptk. hatálybalépése után került be. Vagyis védett ismeretre lehet hivatkozni közpénzek felhasználásnál is, de az nem képzelhető el, hogy egy pályázat teljes anyag vagy egy

szerződés csak a védett ismeretről szóljon tehát a megismerési korlát ilyen esetben a védendő dokumentum egyes részeire terjed ki. A korlátozást mindig indokolni kell, hogy az adatkérő számára érthető legyen, hogy miért képez védett ismeretet a dokumentum. A pályázati anyagoknál vagy szerződéseknél fordul elő ilyen adat tartalom. Ilyen esetben a szerződő felet vagy pályázót a dokumentumok beadásakor nyilatkoztatni lehet a védett ismeretről és annak tartalmi megjelenéséről. Ezen nyilatkozat sokat segít a későbbi jogviták elkerülése végett is.

Az adatok megismerését korlátozni lehet uniós jogi aktus alapján az Európai Unió jelentős pénzügyi- vagy gazdaságpolitikai érdekére tekintettel.

A döntés megalapozását szolgáló adatok a döntés megszületése előtti időszakban nem nyilvánosak. A „nem nyilvános" megjelölés kiadói utasítás, azt jelenti, hogy csak a feladat és hatáskörben eljáró személyek ismerhetik meg. Nem szabad összekeverni a Mavtv. szerinti korlátozott terjesztésű minősítési szinttel. A „nem nyilvános" megjelölésű adat, egyfajta tervezet, még nem tükrözi az adatkezelő szerv kialakult véleményét az adott témakörben, ezért az adatot védeni kell. A megismerést a szerv vezetője engedélyezheti a megismerés kizáráshoz fűződő közérdek súlyának mérlegelésével.

Főszabályként tehát a közfeladatot ellátó szerv kezelésében lévő döntésmeglapozását szolgáló adatok is közérdekű adatok, de mivel még nem tükrözik teljes mértékben az adott szerv véleményét, ezért nem nyilvánosak. A jogalkotó azonban itt is lehetővé akarta tenni, hogy megismerhetők legyenek az adatok, de kizárólag a szerv vezetőjének engedélyével. A megismerést akkor lehet engedélyezni, ha a megismerhetőség kizárásához fűződő közérdek korlátozása súlyosabb, mint a megismeréshez fűződő közérdek. Vagyis az elképzelt mérleg nyelve a megismerés felé billen. Ilyen dokumentumok lehetnek a feljegyzések, tervezetek, javaslatok, vélemények. Amennyiben a döntés már megszületett az adott szervnél, a megismerési szabályok is megváltoznak, így amennyiben az adatigény döntésmegalapozását szolgáló adatra vonatkozik, de már a döntés megszületett az adatigény akkor utasítható el, ha a megismerés a közfeladatot ellátó szerv törvényes rendjét, feladat és hatáskörének illetéktelen befolyástól mentes ellátását veszélyeztetné. A mérlegelésre itt is van lehetőség az Infotv. szerint. Ebben az esetben, azonban már nagyobb súly gördül az adatkezelő szervre, mivel konkrét érveivel kell alátámasztani az érdeksérelmét. És mivel a mérleg mindkét nyelvén közérdek egyes aspektusai vannak, az egyik oldalon az információszabadság a másik oldalon, pedig az adott szerv törvényes működése, nem kétséges, hogy a bíróság előtti adatigény perekben vagy a Hatóság eljárásában az információs szabadsághoz fűződő érdek

legtöbbször nagyobb hangsúly kap. Ettől eltérő mérlegelést tesz lehetővé a, ha az egyik serpenyőben a közérdek a másik serpenyőben a magánérdek, vagyis a személyes adatok védelme kap helyet. Ez akkor képzelhető el, ha az adatigény közérdekből nyilvános személyes adatokra vonatkoznak, példának okául az adatigénylő az adott szerv teljes foglalkoztatotti állományát kéri név és telefonszám feltüntetése mellett. A mérlegelést itt a közérdek és a magánérdek, mint védendő érték képezi Az adatigény teljesítésénél mérlegelni kell az Alaptörvényben foglalt közérdekű adatok megismeréséhez és a személyes adatok védelméhez fűződő alapjogok egymással szemben történő érvényesülését. Tekintettel arra, hogy mindkét jog az Alaptörvény VI. cikk. (2) bekezdése szerint információs alapjog, az Alaptörvény I. cikk (1) bekezdése értelmében feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozhatók.

Az Alaptörvény VI. cikk (2) bekezdése értelmében mindenkinek joga van a közérdekű adatok megismeréséhez és terjesztéséhez. A közérdekből nyilvános személyes adatok tekintetében fontos kiemelni, hogy megismerésükre ugyan a közérdekű adatok megismerésére vonatkozó szabályokat kell alkalmazni, de ezen adatok személyes jellege a nyilvánosság ellenére megmarad, így az adatvédelem legfontosabb garanciáját, a célhoz kötött adatkezelés elvének követelményeit változatlanul be kell tartani.

Az adatkezelés célja jelen esetben is a közhatalom gyakorlásának, a közügyek intézésének és ezzel összefüggésében a közpénzek felhasználásának átláthatósága és nyilvánosság általi kontrolja. E célok tehát korlátot szabnak a közérdekből nyilvános személyes adatok nyilvánosságának.

A közérdekből nyilvános adatok széles körének megismerhetősége nem eredményezheti a közfeladat ellátásához nem kapcsolódó magánszféra kiszolgáltatottságát.

Véleményem szerint az átláthatóság és az ellenőrizhetőség – mint közérdek – kiemelt fontosságú. Ugyanakkor az információszabadságnak és az információs önrendelkezési jognak egymásra tekintettel kell érvényesülnie, így a fentiekben leírtak alapján a kormánytisztviselő személyes adatainak, azaz nevének, elérhetőségének a közlése, túlmutat az adott közfeladatot ellátó szerv átláthatóságán és egyben aránytalanul sérti az egyes kormánytisztviselő magánszférájához való alapjogát.

A fentieket támasztja alá a NAIH 2013. évi beszámolójában (122. o.) megfogalmazottakat, miszerint: „A személyes adatok nyilvánossága csak a közfeladat ellátása körében és

alkotmányosan csak olyan mértékig indokolt, amely a cél eléréséhez szükséges. Az Infotv. szellemiségével nem az ilyen, az Alkotmánybíróság által „készletező adatkezelésnek" minősülő személyes adatok megismerése áll összhangban. Az adott szerv gazdálkodását az állampolgárok anélkül is képesek ellenőrizni, hogy a közalkalmazottakat megalázó helyzetbe hoznák, és belőlük ellenérzést váltsanak ki az ilyesfajta listázásokkal. A cél megvalósítható a lista név nélküli kiadásával, illetőleg az adatok szolgáltatásával is."

A konkrét példa megválaszolása érdekében számba vettük a lehetséges korlátokat.. Megállapítottuk, hogy a kért pályázati anyagok a címzett adatkezelő szerv kezelésében van. A tananyagfejlesztésre a szerződést ugyancsak a szervezet kötötte az oktatókkal. A szerződések és a tananyag a Mavtv. szerint nem minősített. A kért adtok nem tartalmaznak üzleti titkot és védett ismeretet. A tananyag azonban előkészítés alatt van, nem lektorálták még, tartalmilag változhat. Az adatok megismerését tehát az adatkezelő szerv vezetője engedélyezheti. A másik kérdés a megkötött szerződésekre vonatkozik, amelyek megismerés szempontjából elválnak a tananyagtól, hiszen hatályosak, az előző szempontokat figyelembe véve üzleti titkot nem tartalmazhatnak, és a közzétételi szabályok alapján az Infotv. 1. számú melléklete alapján közzé kell tenni a szerv honlapján és a közadattárban a keletkezéstől számított 60 napon belül a szerződések leíró adatait. Amennyiben tehát az adatigénylő nem elégszik meg a honlapon közzétett szerződések adataival, szerződők neve, szerződés tárgya, összege, határideje, a konkrét szerződéseket meg kell küldeni az adatkérőnek. A szerződéseket tartalmilag azonban át kell nézni, mivel a szerződő természetes személy nevén és munkahelyén kívüli személyes adatok nem közérdekből nyilvános adatok, ezért ezen adatokat felismerhetetlenné kell tenni a kiadandó dokumentumokon.

A lehetséges megoldás tehát: a tananyag korlátozása, döntés megalapozását szolgáló adatra való hivatkozással és a szerződések anonimizált formájának kiadása, ahol csak a szerződő neve és jelenlegi munkahelye ismerhető meg.

XI. AZ ELEKTRONIKUS KÖZZÉTÉTEL SZABÁLYAI ÉS GYAKORLATI MEGVALÓSÍTÁSA

Az állampolgárnak, illetve rajta keresztül a társadalomnak van joga megismerni a közérdekű adatokat, illetve azokat mindenki számára ismerhetővé tenni. Ez a jog mindenkit megillet. Az információszabadság nem politikai jelszó, hanem szakkifejezés, azoknak a jogintézményeknek az összefoglaló neve, amelyek a mai viszonyok között akarnak valódi

esélyt adni a vélemény- és sajtószabadságnak, valamint a polgárok "informált részvételének" a társadalom ügyeiben, és mindezek érdekében az állami szervek információit nyilvánossá teszik.

Melyek is a közérdekű adatok? A közérdekű adatok fogalmát tulajdonképpen még az Avtv. elfogadása előtt az Alkotmánybíróság határozta meg a 32/1992. (V. 29.) AB határozatában, mely kimondta, hogy „az információ csak akkor nem tekinthető közérdekűnek, ha az személyes adat.” Ez tulajdonképpen az információs önrendelkezési jog és az információszabadság szétválasztása volt. E fogalomból alakult ki és került az Avtv.-be a definíció, mely szerint az állami vagy helyi önkormányzati feladatot ellátó szerv kezelésében levő, a személyes adat fogalma alá nem eső és a törvényben meghatározott kivételek körébe nem tartozó adat.

A fogalom az évek folyamán változott. A hatályos Infotv.-beli megfogalmazás pedig a következő: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

2004. január elsején lett a hatályos joganyag része a közérdekből nyilvános adat – némileg ellentmondásos – fogalma. Az Avtv. 2005-ös módosítása a fogalommal kapcsolatos számos dogmatikai probléma egy részét megszüntette, mert kikerült belőle két definíciós elem: a természetes és jogi személyek, illetve jogi személyiséggel nem rendelkező szervezetek, mint az adatot kezelők, valamint mint az adatok alanyai. Az Infotv. a definíciót minimális változtatással átvette, mely így szól: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

Az Infotv., és korábban az Avtv. még egy helyen foglalkozik, foglalkozott a közérdekből nyilvános adatokkal, és a következőket rendeli el: közérdekből nyilvános adat a közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői

megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja .

A közérdekű és közérdekből nyilvános adatok megismerésének az Infotv. két módját szabályozza:

- egyedi adatigénylés alapján történő adatszolgáltatás
- egyedi adatszolgáltatás nélküli, elektronikus közzététel

Most az utóbbival az elektronikus közzététellel foglalkozunk részletesebben.

A közfeladatot ellátó szervek a szervezeti, személyzeti, tevékenységükre, működésükre vonatkozó és gazdálkodási adataikat az interneten, honlapon közzéteszik. A hozzáférés nem köthető regisztrációhoz és díjfizetéshez. Az adatokat úgy kell közzétenni, hogy azok kinyomtathatóak és részletekben is kimásolhatóak legyenek. Az egyedi adatigénylésekhez hasonlóan az elektronikus információszabadság esetében is a közfeladatot ellátó szerv kötelezettsége, hogy az adatokat bárki, személyes adatok közlése, kezelése nélkül megismerhesse, letölthesse.

Az általános közzétételi kötelezettség két fórumon, honlapon: a saját honlapon és az egységes közadatkereső oldalon (www.kozadat.hu) való közzétételt jelent azok számára, akik az Infotv. szerint kötelesek saját honlapot működtetni (pl. Köztársasági Elnöki Hivatal, az Alkotmánybíróság Hivatala, Országgyűlés Hivatala, Állami Számvevőszék, fővárosi és megyei kormányhivatalok, stb.).

Azon szervek, amelyek nem kötelesek saját honlapot működtetni, választhatnak, hogy a közzétételi kötelezettségnek

- saját,
- társulásaik által közösen működtetett,
- a felügyeleti, szakmai irányításukat vagy működésükkel kapcsolatos koordinációt ellátó szervek által fenntartott,
- valamint az erre a célra létrehozott központi honlapon (www.kozadat.hu) való közzétételnek tesznek eleget.

Az Infotv. általános közzétételi listát tartalmazó 1. számú melléklete írja elő a közfeladatot ellátó szervek részére, hogy mely adatokat kötelesek közzétenni külön adatigénylés nélkül.

A közfeladatot ellátó szerv vezetője, főleg a korábbi időszak közérdekű adatkéréseit alapul véve – a NAIH véleményének kikérésével – további kötelezően közzéteendő adatkört határozhat meg (egyedi közzétételi lista). Egyes ágazati jogszabályok a közfeladatot ellátó szervtípusra vonatkozóan meghatározhatnak további közzéteendő adatokat is (különös közzétételi lista).

Az általános közzétételi listában szereplő adatok három nagy egységre oszthatók:

- szervezeti- személyzeti adatok;
- tevékenységre, működésre vonatkozó adatok és
- a gazdálkodási adatok.

Ezeken a csoportokon belül további közzétételi egységek találhatóak. A törvény nem csak a közzéteendő adatokat határozza meg, hanem az adatok frissítésére és az adatok megőrzésére vonatkozó szabályt is megállapít.

A szervezeti- személyzeti adatok foglalják magukba a szervre vonatkozó alapvető információkat (pl. a szerv hivatalos neve, elérhetősége, a szerv vezetőjére vonatkozó adatok, a szerv tulajdonában lévő gazdasági társaságra vonatkozó alapadatok, a felettes szerv adatai, stb.)

A tevékenységre, működésre vonatkozó adatok között fellelhető többek között pl. a szerv feladatát, hatáskörét és alaptevékenységét meghatározó jogszabályok, illetve szabályozások szövege, az ügymenetre (hatósági eljárásra) vonatkozó tájékoztatás, az ügyintézéshez szükséges dokumentumok, okmányok, eljárási illetékek meghatározása és az ügyintézést megkönnyítő letölthető űrlapok, nyomtatványok.

A gazdálkodási adatok tartalmazzák pl. a szerv költségvetését, a számviteli törvény szerinti beszámolóját, közbeszerzésre vonatkozó adatokat, a támogatások és a közfeladatot ellátó szerv által kötött szerződések adatait.

Az elektronikusan közzétett adatok – ha az Infotv. vagy más jogszabály eltérően nem rendelkezik - a honlapról nem távolíthatóak el. A szerv megszűnése esetén a közzétételi kötelezettség a szerv jogutódját terheli.

A közzétételi honlapon tájékoztatást kell adni a közérdekű adatok egyedi igénylésének szabályairól. A tájékoztatásnak tartalmaznia kell az igénybe vehető jogorvoslati lehetőségek ismertetését is.

A közzétételi listákon szereplő adatok pontos, naprakész és folyamatos közzétételéről, az adatközlőnek való megküldéséről az adatfelelős szerv vezetője gondoskodik, a megküldött adatok közzétételéért, hozzáférhetőségéért, hitelességéért és az adatok frissességéért az adatközlő a felelős.

Adatfelelős szerv: az a közfeladatot ellátó szerv, mely a kötelezően közzéteendő közérdekű adatot előállította, illetve amelynek a működése során ez az adat keletkezett.

Adatközlő: az a közfeladatot ellátó szerv, amely – ha az adatfelelős nem maga teszi közzé az adatot – az adatfelelős által hozzá eljuttatott adatait a honlapon közzéteszi.

Ezek az elmélet percei voltak, azonban a gyakorlatban nem ilyen egyszerű a dolgunk. A törvény által leírtakon túl további jogszabályoknak is meg kell felelnünk az elektronikus információszabadság terén. Nézzük ezeket kicsit részletesebben:

Az állampolgárok tájékozódását elősegítendő az Infotv. előírja, hogy az informatikáért felelős miniszter egységes közadatkeresőt működtet.

A közadatkereső révén az állampolgár egységes felületen közvetlenül hozzáférhet bármely közzétételre kötelezett szerv közzétett adataihoz (pontosabban az arra utaló hivatkozáshoz). Ennek a megvalósításához az egyes szerveknél nem csak a közzétett adatokat kell elkészíteni, hanem létre kell hozni olyan leíró adatokat (metaadatokat) is, amelyeket begyűjtve a közadatkereső el tudja dönteni, hogy az állampolgár által keresett közzétett adatok milyen megjelenítési egységekben (dokumentumokban, a 18/2005. IHM rendelet- a továbbiakban: IHM rendelet - szerint „közzétételi egységekben") érhetőek el, azaz mely hivatkozást kell az állampolgárnak találatként megadnia.

A szervek honlapjának nyitóoldalán el kell helyezni egy Közérdekű adatok menüpontot, ami a közzétételre előírt adatokat, az azokat megjelenítő közzétételi egységeket vagy az ezek hivatkozásait tartalmazza.

Ahhoz, hogy az érdeklődő állampolgárok magasabb szinteken azonos szerkezeti egységeken belül találhassák meg az egyes közzétett adatokat, az IHM rendelet előírja ennek a jegyzéknek a meghatározott szerkezet szerinti, magas szintű tagolását is.

A közadatkereső működőképessége miatt azt is biztosítani kell, hogy egy adott közzétételi egységet és annak tartalmát egyértelműen meghatározza az úgynevezet URL címe. Csak e korlátozás mellett használható közzétételi egységként aktív vagy dinamikus tartalmú dokumentum, mivel nem megengedhető, hogy egyazon URL cím által beazonosított

közzétételi egység más és más tartalmat adjon. Ez igaz az aktualizált dokumentumokra is, tehát mindaddig, amíg fennáll a közzétett adatok archívumban tartásának kötelezettsége, nem lehet ugyanazt az URL-t más, akár csak az aktualizált változatot tartalmazó dokumentumra felhasználni.

Ez alól egyetlen kivétel van: ha téves közzétett adat jelenik meg, mivel azt a közadatkereső számára nem lehet elérhetővé tenni, ez esetben a javított adatot tartalmazó közzétételi egység URL címe azonos lehet az eredeti, még hibás adatot tartalmazó közzétételi egység URL címével.

Alapvetően a szervek maguk határozzák meg, hogy mely közzéteendő adatot, milyen közzétételi egységben kívánnak megjeleníteni, mivel csoportosítják őket, de ennek van egy fontos korlátja: az IHM rendelet 2. melléklete különféle közzétételi „mintaegységeket" határoz meg arra, hogy milyen adatokat is kell önálló közzétételi egységbe belefoglalni, és miket nem lehet egybe foglalni.

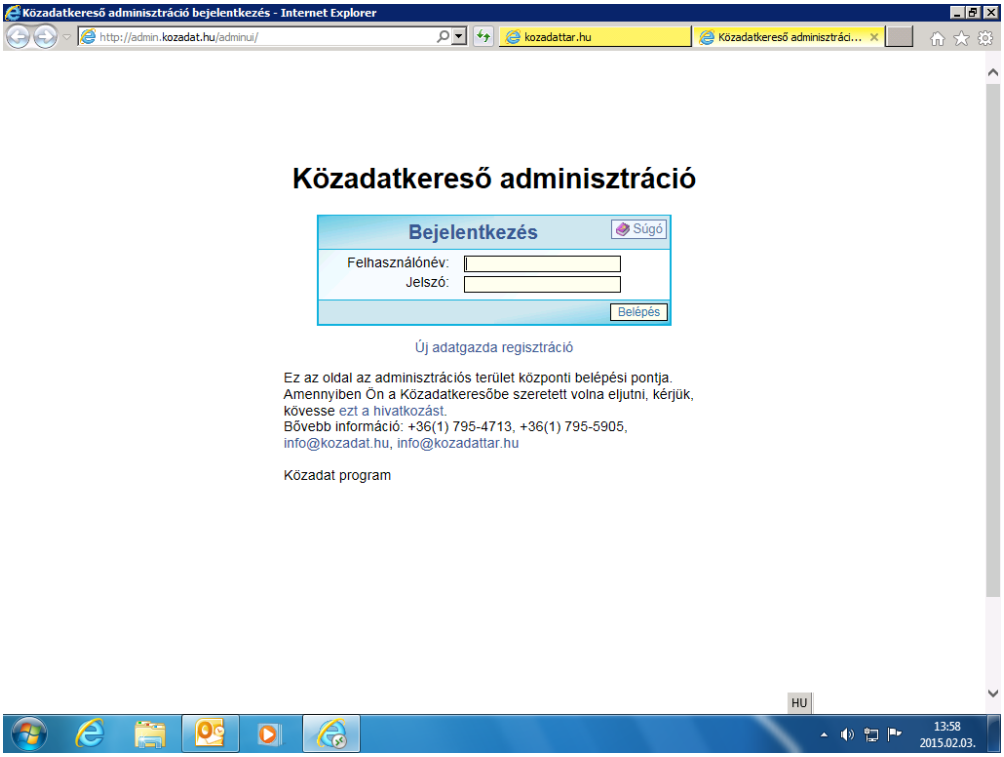
E tilalom hiányában egy szerv úgy is eleget tehetne a közzétételi kötelezettségének, hogy az összes létező adatot egyetlen dokumentumban (közzétételi egységben) jeleníti meg, amikor egy közzétételi egység lenne csak, és ezért nem lenne érdemben használható a közadatkereső, hiszen megfelelő metaadat hiányában nem fog tudni találatot kiadni az adott szerv közzétett adatairól (közzétételi egységeiről).

Végül kiemelendő a szervek közzétételi szabályzat-készítési kötelezettsége, amely szabályzat elsődleges szerepe, hogy részletesen leírja a közzétételi kötelezettség teljesítésének szervezeten belüli szabályait (feladatok, azokhoz tartozó munkakörök, ezek együttműködése).

A jogszabályban definiált közérdekű adatok központi elektronikus jegyzéke és az egységes közadatkereső rendszer működtetését – a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005. (XII. 25.) Korm. rendelet (továbbiakban: Korm. rendelet) 12. § (1) bekezdés előírása szerint – a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter (nemzeti fejlesztési miniszter) megbízásából a Nemzeti Infokommunikációs Szolgáltató Zrt. keretein belül működő Közadat program végzi.

Nézzük, mik a feladatai a közfeladatot ellátó szerv összekötőjének, aki általában a belső adatvédelmi felelős

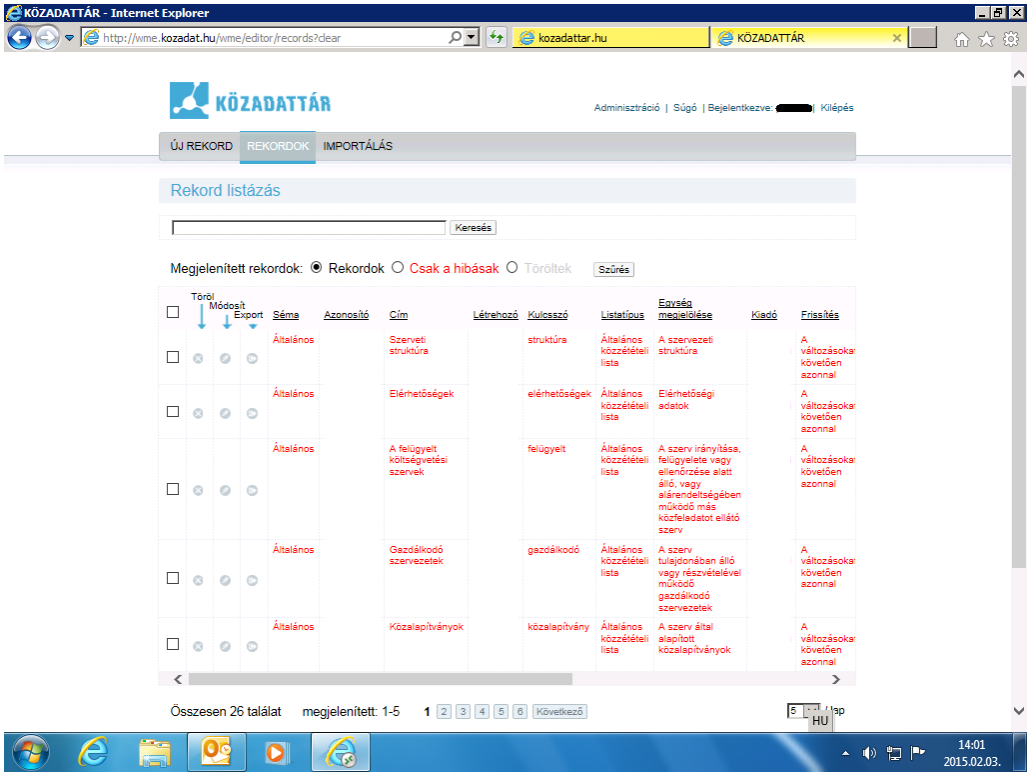
Ennek a személynek regisztrálnia szükséges, az alábbiak szerint:



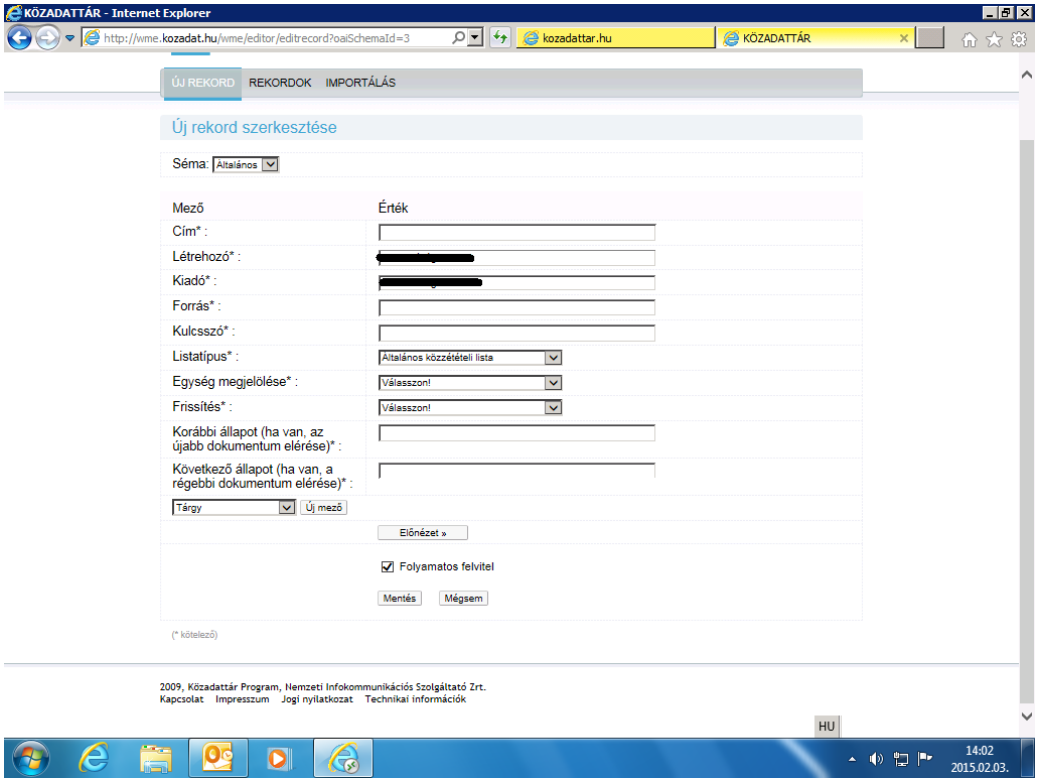
Ezen a felülten meg kell adni az intézményi adatokat, meg kell nevezni az adatfelelőst és a kapcsolattartót. Ezt követően a NISZ honlapján megtalálható fax-számra vagy e-mail címre el kell küldeni az aláír regisztrációs adatokat.

A rendszer kialakítása után indítható az adminisztrációs felületen a tesztaratás. Amennyiben sikeres volt az aratás, akkor kérhető az aktiválás, melynek eredményeként a közzétett közérdekű adatokról elkészített metaadatok kereshetővé válnak az egységes közadatkereső rendszerben.

A regisztráció megtörténte után kezdődhet meg az adatok feltöltése a közadatkereső rendszerbe. A közadatkereső teljes mértékben leköveti mind az Infotv. közzétételi listáját, mind a IHM rendelet közzétételi egységeit. A következő képen jól látható a közadattár struktúrája, a kapcsolattartó ezzel a képpel fog találkozni a munkája során.



A rekordok szerkesztése is elég felhasználóbarát. Pontosan és lekövethető módon lehet kitölteni a különböző alpontokat. Maga a kezelőfelületet a következőképpen fog kinézni:



Az adatok első feltöltése időigényes a nagy koncentrációt igényel, azonban az adatok frissen tartása, a felület folyamatos felügyelete sem kisebb feladat.

A jó állam transzparens tehát átlátható, és az elektronikus közzététel az egyik nagyon fontos eszköze, hogy az állampolgárok bizalma megszilárduljon az államszervezettel kapcsolatosan, továbbá korrupció megelőzésének hatékony fegyvere is egyben.

XII. INTEGRITÁS BEJELENTÉS ADATVÉDELMI KÉRDÉSEI

Elsődlegesen a bejelentések adatkezelésének jogalapját kell megvizsgálnunk. Az integritás bejelentéseket az államigazgatási szervek integritásirányítási rendszeréről és az érdekérvényesítők fogadásának rendjéről szóló 50/2013. (II. 25.) Kormányrendelet szabályozza. Erre épülnek az egyes szervek által alkotott saját szabályozások.

Ahogy látható, az adott jogszabály nem törvény, így az Infotv. 5. § (1) bekezdés b. pontja alapján az adatkezelés jogalapja nem származhat a kormányrendeletből. A Kormányrendelet alapján megalkotott belső szabályzatok, így az előzőekre figyelemmel sem tartalmazhatnak konkrét felhatalmazáson alapuló adatkezelési szabályokat. így azt sem pl, hogy a bejelentő adatait a bejelentést fogadó szerv-e jogszabály alapján kezelheti, vagy pl, hogy az integritás

eljárás során meghallgatott személyek nevét, születési dátumát, munkahelyi címét a kormányrendelet alapján tartja nyilván.

Az adatkezelési jogalap ezen esetben az érintett fél hozzájárulása lesz. A hozzájárulás többformában is megadható. Az Infotv[119].a személyes adatok kezelésénél nem teszi kötelezővé az érintett fél írásbeli hozzájárulását, ezért ez megvalósulhat ráutaló magatartással. Pl, ha belépünk egy nyilvánosság előtt megnyitott magánterületre, ahol kamerarendszer van felszerelve, akkor a belépésünkkel megadjuk a hozzájárulást a rólunk készült fényképfelvételek kezelésére. Amely azonban előfeltétele a hozzájárulásnak, hogy a belépés előtt tájékoztatást kapjunk arról, hogy az adott területen kamerarendszer működik, milyen célból ki az adatkezelője stb. Ennek tudatában el tudjuk dönteni, hogy ezekkel a feltételekkel is be szeretnék e lépni az adott területre. Jelen esetünkre alkalmazva, ha az integritás bejelentés a bejelentő szándékából indult, akkor az általa megadott saját személyes adatainak kezeléséhez a hozzájárulást vélelmezni kell a szervezetnek.

A bejelentő adatainak kezelése a bejelentést fogadó szerv felelőssége. A szervnek az alábbi adatkezelési kérdéseket kell átgondolnia:

- milyen adatokat lehet a bejelentőről nyilvántartani?
- milyen rendszerben lehet az adatokat nyilvántartani?
- ki férhet hozzá az adatokhoz?
- meddig lehet kezelni az adatokat?
- a bejelentő meghallgatásának a helye hol legyen?
- szükséges-e az adatkezelési tájékoztató?
- az eljárásban érintett más személyek adatainak adatkezelési joglapaja?
- mennyi ideig lehet kezelni az adatokat?

1. Milyen adatokat lehet a bejelentőről nyilvántartani?

A kérdés, az, hogy milyen adatok szükségesek a cél érdekében, azaz az integritási bejelentés kivizsgálásához. Erre az Infotv. 4. § (2) bekezdés ad részletszabályokat. Végig kell tehát gondolni, hogy milyen adatok kellenek ahhoz, hogy az integritás előadó a bejelentést szakmailag el tudja bírálni. Elsődlegesen a bejelentő neve, és valamilyen elérhetősége, így a lakcíme, vagy az e-mail címe. A többi adata véleményem szerint a cél elérése érdekében

[119] Infotv. 5. §

érdektelen, de nem teszem lehetetlenné, hogy valamely bejelentésnél más személyes adatok is szükségessé válhatnak.

2. Milyen rendszerben lehet az adatokat nyilván tartani?

Az iratkezelés megvalósulhat papíralapon, de ez mára már nem kizárólagos, vagyis mindig követi elektronikus nyilvántartás. A kormányzati törekvések alapján pedig nem kizárt az elektronikusrendszerek elsődlegessége. Az iktatás és az iratok kezelése is egy olyan iktató könyvbe, elektronikus rendszerbe történjen, ahol az adatokat más egyéb iktatásoktól el lehet különíteni. Vagyis külön erre az ügyiratfajtákra létrehozott iktató könyvbe vagy rendszerbe legyen iktatva az irat. Szándékosan használom az irat és iratkezelés kifejezéseket az adat és adatkezelés kifejezés helyett, hiszen az adatkezelésünket csak az iratkezelés szabályainak segítségével tudjuk biztosítani. A probléma megoldása érdekében ennél a kérdésnél javaslom az adott szerv iratkezeléssel foglalkozó szervezeti egységének a bevonását.

3. Ki férhet hozzá?

A hozzáférési jogosultságokat ebben az esetben a legszűkebben kell érvényesíteni. Hozzáféréssel rendelkezzen az iktatást végző személy az integritás tanácsadó, közvetlen felettesei. A hozzáférések leszűkítésében az informatikával foglalkozó szervezeti egységek bevonását javaslom. Egyszerűbb esetben a hozzáférést a dokumentumok egyedi titkosításával is meg lehet oldani. Ezen esetben ügyelni kell arra, hogy a bejelentések iktatásánál az iktató rendszerbe megadott keresőszavak között ne szerepelje a bejelentő neve vagy egyéb személyes adata vagy a konkrét tárgyra vonatkozó azonosítható adatok. pl. ne szerepelje ilyen adat az iktatásban: Minta János bejelentése a pénzügyi főosztályvezető személye és tevékenysége ellen. Mint ahogy látjuk nem csak a név lehet személyes adat, hanem adott esetben a személy a beosztása által is azonosítható bizonyos társadalmi körben, így a munkahelyen.

4. A bejelentő meghallgatásának a helye hol legyen?

Az integritás bejelentés kivizsgálása során sor kerülhet a bejelentő meghallgatására. Ezen esetben a szervezet vezetőjének biztosítani kell olyan helyiséget, ahol az integritás tanácsadó négyszemközt tudja meghallgatni a bejelentőt. Erre azért kell hangsúlyt fektetni, mert a tanácsadók sok esetben más feladatkört is betöltenek és nem egyedül ülnek egy szobában.

Amennyiben a meghallgatás más illetéktelen személy előtt vagy annak halló körzetében történik a szervezet nem biztosítja az integritás bejelentés és a bejelentő sértetlenségét és ezzel a meghallgatás pozitív kimenetelét is veszélyezteti.

A szervezetnek kell eldöntenie, hogy a meghallgatásra adott esetben egy külön elkülönített helyiségben vagy egy semleges helyszínen kerüljön sor. nehéz kiválasztani egy adott szervnél a legjobb helyszínt a meghallhatásra, mindig figyelemmel kell leni a bejelentő személyére és a bejelentés tárgyára.

5. Szükséges-e az adatkezelési tájékoztató?

Az előzőekben leírtak alapján az integritás bejelentés alapján felvett adatokat a szervezet hozzájárulás alapján fogja kezelni. A felhozott példa alapján a szükséges, hogy amikor a bejelentő az adatait a meghallgatás során ismételten megadja tájékoztatást kapjon arról, hogy milyen célból, mennyi ideig kezelik az adatait, és ki ismerheti meg azokat. A meghallgatási jegyzőkönyvben a személyes adatokon kívül már különleges adatok is rögzítése kerülhetnek, ezen adatoknak a kezeléséhez pedig írásbeli hozzájárulásra van szükség. A jegyzőkönyv tehát mindenképpen tartalmazzon konkrét adatkezelési tájékoztatást, amelyet a meghallgatott személy külön aláírásával elfogad.

6. Az eljárásban érintett más személyek adatainak adatkezelési joglapaja?

A bejelentés kivizsgálásához a szükséges adatokat az érintett szervezeti egység vezetőjének az integritási tanácsadó részére rendelkezésre kell bocsátania. Amennyiben szükség van a szervezeten belül egyéb személy meghallgatására az integritási bejelentés eljárásán belül a kérdés ismételten az, hogy az adott személy adatainak adatkezelési jogalapja honnan fog származni. Az eddigi okfejtést figyelembe véve, mivel törvényi felhatalmazás nincsen az adatkezelésre, az adatfelvétel csak önkéntes hozzájáruláson alapulhat. Nagyon kényes a szituáció, amikor munkáltató jogviszonyban álló személyt a munkáltató megbízásából hallgatnak meg. Maga a jogviszony fennállása a dolgozó számára azt a következtetést alapozza meg, hogy számára a nyilatkozat megtétele kötelező. Ez azonban nincsen így és erre szükséges a dolgozó figyelmének a felhívása. A meghallgatási jegyzőkönyven az adatkezelési hozzájárulás közvetlenül az adatfelvételt követően külön aláírással szerepeljen. Nem elégséges, ha a tájékoztatás általánosan az Infotv-re hivatkozik, így pl. az adatait az Infotv.-ben foglaltak szerint kell kezelni. Konkrét tájékoztatást kell adjon a dolgozónak, hogy az adatait milyen célból, milyen hosszú ideig, és főleg hogy milyen jogalap alapján kezelik. A

dolgozónak szabad választást kell biztosítania, hogy szabadon döntsön, kíván-e nyilatkozatot tenni az adott ügyben vagy sem.

7. Mennyi ideig lehet kezelni az adatokat?

Az eljárás lezárulásáig, az összefoglaló jelentés elkészítéséig mindenképpen szükség van az adatokra. Az adatokat az iratkezelési szabályok figyelembe vétele mellett 5 évig őrizzük meg. Amennyiben a megállapított adatok alapján egy másik eljárás indul, mondjuk fegyelmi, szabálysértési vagy bűntető eljárás, az adatok őrzési idejét meg kell hosszabbítani az új eljárásra vonatkozó adatkezelési idővel.

8. A jegyzőkönyv

Jegyzőkönyvet lehet felvenni a bejelentések és a meghallgatások során. Legfőképpen a különbségeket szeretném bemutatni egy – egy példával. Különös figyelemmel a tájékoztatási kötelezettségre. A jegyzőkönyvek az 1. számú mellékletben olvashatóak.

XIII. FÜGGELÉK

1. számú melléklet
Bejelentés integritási ügyekben

Bejelentést felvevő szerv elnevezése::

Bejelentés helye:

Bejelentés ideje:

A bejelentő neve:

Születési helye és ideje:*

Anyja neve:*

Lakcíme:

Elérhetőségei (telefon, e-mail):*

A csillaggal jelölt részt nem kötelező kitölteni, de a név nélküli vagy azonosíthatatlan bejelentő által megtett bejelentés vizsgálata mellőzhető.

Hozzájárul-e személyes adatai továbbításához a bejelentés alapján kezdeményezett eljárás lefolytatására hatáskörrel rendelkező szerv részére:

igen *nem*

Kéri-e adatai zártan kezelését:

igen *nem*

Az esemény rövid, tényszerű leírása:

A rendelkezésre álló bizonyítékok, dokumentumok felsorolása, annak megjelölésével, hogy azok kinek a birtokában találhatóak:

Az esetleges tanúk neve és elérhetősége:*

Nyilatkozom, hogy a bejelentést jóhiszeműen teszem, olyan körülményekről, amelyekről tudomásom van, és feltételezem, hogy azok valósak.

Tájékoztató: A bejelentést vizsgáló szerv a bejelentő által megadott személyes adatokat a vizsgálat szakaszában az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi. CXII. törvény alapján kezeli. A bejelentési jegyzőkönyvben foglaltakat kizárólag a vizsgálattal összefüggésben az erre hatáskörrel rendelkező személyek ismerhetik. meg. A bejelentés kivizsgálására az államigazgatási szervek integritásirányítási rendszeréről és az érdekérvényesítők fogadásának rendjéről szóló 50/2013. (II. 25.) Kormányrendelet szabályai az irányadóak.

Jegyzőkönyv lezárva:

…….. *……..*

bejelentő *szerv részéről*

2. számú melléklet
Meghallgatási-jegyzőkönyv
integritási
ügyekben

Meghallgatást végző szerv elnevezése::

Meghallgatás helye:

Meghallgatás kezdete:

A meghallgatott neve:

Lakcíme:

Elérhetőségei (telefon, e-mail):

Munkahelyének és beosztásának a megnevezése:

Nyilatkozom arról, hogy előzetes tájékoztatást kaptam arról, hogy személyes adataimat az integritási eljárás során az ezzel összefüggő vizsgálat eredményes lefolytatása érdekében ……..szerv 5 évig kezelheti. Az adatkezelés önkéntes adatkezelési hozzájárulásomon alapul. A bejelentést vizsgáló szerv az általam megadott személyes adatokat a vizsgálat szakaszában az Információs önrendelkezési jogról és az információszabadságról szóló 2011. évi. CXII. törvény alapján kezeli. A meghallgatási jegyzőkönyvben foglaltakat kizárólag a vizsgálattal összefüggésben az erre hatáskörrel rendelkező személyek ismerhetik. meg. A bejelentés kivizsgálására az államigazgatási szervek integritásirányítási rendszeréről és az érdekérvényesítők fogadásának rendjéről szóló 50/2013. (II. 25.) Kormányrendelet szabályai az irányadóak.

……..

meghallgatott

Kéri-e adatai zártan kezelését:

igen *nem*

Az esemény rövid, tényszerű leírása:

A rendelkezésre álló bizonyítékok, dokumentumok felsorolása, annak megjelölésével, hogy azok kinek a birtokában találhatóak:

Az esetleges tanúk neve és elérhetősége:*

Nyilatkozom, hogy a bejelentést jóhiszeműen teszem, olyan körülményekről, amelyekről tudomásom van, és feltételezem, hogy azok valósak.

Jegyzőkönyv lezárva:

…….. ……..

meghallgatott *szerv részéről*

3. számú melléklet

Űrlap adatvédelmi nyilvántartásba vételhez

1. Adatkezelő

1.1. Az adatkezelő megnevezése: .....
1.2. Címe: .....
1.3. Telefonszáma: .....
1.4. Belső adatvédelmi felelős neve, elérhetőségei: .....

Adatkezelés

1.5. Előző adatkezelés
1.5.1. Az adatkezelő megváltozásának jogcíme:
.....
1.5.2. Előző nyilvántartási azonosító:
.....
1.6. Az adatkezelés megnevezése:
.....
1.7. Az adatkezelés célja, időtartama:
.....

1.8. Az adatkezelés jogalapja
1.8.1. Jogszabályhely vagy más jogalap:
.....
1.8.2. Jogszabály címe:
.....
1.9. A tényleges adatkezelés helye:
.....
1.10. Az adatkezelés automatizáltsága:
.....

2. Az adatfeldolgozás

2.1. Az adatfeldolgozó megnevezése: .....
2.2. Címe: .....
2.3. Telefonszáma: .....
2.4. Belső adatvédelmi felelős neve, elérhetőségei: .....

3. Az adatok forrása

3.1. Adatfajta megnevezése:
.....
3.2. Adatforrás megnevezése:
.....
3.3. Adatfelvétel (átvétel) jogalapja

3.3.1. Jogszabályhely vagy más jogalap:

.....

3.3.2. Jogszabály címe:

.....

3.4. Adatfelvétel (átvétel) módja:

.....

3.5. Az adat törlési határideje:

.....

4. Adattovábbítás(ok)

4.1. Adatfajta megnevezése:

.....

4.2. Címzett neve:

.....

4.3. Az adattovábbítás jogalapja

.....

4.3.1. Jogszabályhely vagy más jogalap:

.....

4.3.2. Jogszabály címe:

.....

4.4. Az adattovábbítás módja:

.....

4.5. Az adattovábbítás időpontja:

.....

5. Érintettek

5.1. Az érintettekre vonatkozó adatok leírása:

.....

5.2. Érintettek száma:

.....

6. Egyéb:

Dátum: ……

Aláírás: ……

4. számú melléklet
ÁLTALÁNOS KÖZZÉTÉTELI LISTA
I. Szervezeti, személyzeti adatok

	Adat	Frissítés	Megőrzés
1.	A közfeladatot ellátó szerv hivatalos neve, székhelye, postai címe, telefon- és telefaxszáma, elektronikus levélcíme, honlapja, ügyfélszolgálatának elérhetőségei	A változásokat követően azonnal	Az előző állapot törlendő
2.	A közfeladatot ellátó szerv szervezeti felépítése szervezeti egységek megjelölésével, az egyes szervezeti egységek feladatai	A változásokat követően azonnal	Az előző állapot törlendő
3.	A közfeladatot ellátó szerv vezetőinek és az egyes szervezeti egységek vezetőinek neve, beosztása, elérhetősége (telefon- és telefaxszáma, elektronikus levélcíme)	A változásokat követően azonnal	Az előző állapot törlendő
4.	A szervezeten belül illetékes ügyfélkapcsolati vezető neve, elérhetősége (telefon- és telefaxszáma, elektronikus levélcíme) és az ügyfélfogadási rend	A változásokat követően azonnal	Az előző állapot törlendő
5.	Testületi szerv esetén a testület létszáma, összetétele, tagjainak neve, beosztása, elérhetősége	A változásokat követően azonnal	Az előző állapot törlendő
6.	A közfeladatot ellátó szerv irányítása, felügyelete vagy ellenőrzése alatt álló, vagy alárendeltségében működő más közfeladatot ellátó szervek megnevezése, és 1. pontban meghatározott adatai	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
7.	A közfeladatot ellátó szerv többségi tulajdonában álló, illetve részvételével működő gazdálkodó szervezet neve, székhelye, elérhetősége (postai címe, telefon- és telefaxszáma, elektronikus levélcíme), tevékenységi köre, képviselőjének neve, a közfeladatot ellátó szerv részesedésének mértéke	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
8.	A közfeladatot ellátó szerv által alapított közalapítványok neve, székhelye, elérhetősége (postai címe, telefon- és telefaxszáma, elektronikus levélcíme), alapító okirata, kezelő szervének tagjai	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
9.	A közfeladatot ellátó szerv által alapított költségvetési szerv neve, székhelye, a költségvetési szervet alapító jogszabály megjelölése, illetve az azt alapító határozat, a költségvetési szerv alapító okirata, vezetője, honlapjának	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával

	elérhetősége, működési engedélye		
10.	A közfeladatot ellátó szerv által alapított lapok neve, a szerkesztőség és kiadó neve és címe, valamint a főszerkesztő neve	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
11.	A közfeladatot ellátó szerv felettes, illetve felügyeleti szervének, hatósági döntései tekintetében a fellebbezés elbírálására jogosult szervnek, ennek hiányában a közfeladatot ellátó szerv felett törvényességi ellenőrzést gyakorló szervnek az 1. pontban meghatározott adatai	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával

II. Tevékenységre, működésre vonatkozó adatok

	Adat	Frissítés	Megőrzés
1.	A közfeladatot ellátó szerv feladatát, hatáskörét és alaptevékenységét meghatározó, a szervre vonatkozó alapvető jogszabályok, közjogi szervezetszabályozó eszközök, valamint a szervezeti és működési szabályzat vagy ügyrend, az adatvédelmi és adatbiztonsági szabályzat hatályos és teljes szövege	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
2.[77]	Az országos illetékességű szervek, valamint a fővárosi és megyei kormányhivatal esetében a közfeladatot ellátó szerv feladatáról, tevékenységéről szóló tájékoztató magyar és angol nyelven	A változásokat követően azonnal	Az előző állapot törlendő
3.	A helyi önkormányzat önként vállalt feladatai	Negyedévente	Az előző állapot 1 évig archívumban tartásával
4.	Államigazgatási, önkormányzati, és egyéb hatósági ügyekben ügyfajtánként és eljárástípusonként a hatáskörrel rendelkező szerv megnevezése, hatáskör gyakorlásának átruházása esetén a ténylegesen eljáró szerv megnevezése, illetékességi területe, az ügyintézéshez szükséges dokumentumok, okmányok, eljárási illetékek (igazgatási szolgáltatási díjak) meghatározása, alapvető eljárási szabályok, az eljárást megindító irat benyújtásának módja (helye, ideje), ügyfélfogadás ideje, az ügyintézés határideje (elintézési, fellebbezési határidő), az ügyek intézését segítő útmutatók, az ügymenetre vonatkozó tájékoztatás és az ügyintézéshez használt letölthető formanyomtatványok, az igénybe vehető elektronikus programok elérése, időpontfoglalás, az ügytípusokhoz kapcsolódó jogszabályok jegyzéke, tájékoztatás az ügyfelet megillető jogokról és	A változásokat követően azonnal	Az előző állapot törlendő

	az ügyfelet terhelő kötelezettségekről		
5.	A közfeladatot ellátó szerv által nyújtott vagy költségvetéséből finanszírozott közszolgáltatások megnevezése, tartalma, a közszolgáltatások igénybevételének rendje, a közszolgáltatásért fizetendő díj mértéke, az abból adott kedvezmények	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
6.	A közfeladatot ellátó szerv által fenntartott adatbázisok, illetve nyilvántartások leíró adatai (név, formátum, az adatkezelés célja, jogalapja, időtartama, az érintettek köre, az adatok forrása, kérdőíves adatfelvétel esetén a kitöltendő kérdőív), az adatvédelmi nyilvántartásba bejelentendő nyilvántartásoknak az e törvény szerinti azonosító adatai; a közfeladatot ellátó szerv által - alaptevékenysége keretében - gyűjtött és feldolgozott adatok fajtái, a hozzáférés módja, a másolatkészítés költségei	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
7.	A közfeladatot ellátó szerv nyilvános kiadványainak címe, témája, a hozzáférés módja, a kiadvány ingyenessége, illetve a költségtérítés mértéke	Negyedévente	Az előző állapot 1 évig archívumban tartásával
8.	A testületi szerv döntései előkészítésének rendje, az állampolgári közreműködés (véleményezés) módja, eljárási szabályai, a testületi szerv üléseinek helye, ideje, továbbá nyilvánossága, döntései, ülésének jegyzőkönyvei, illetve összefoglalói; a testületi szerv szavazásának adatai, ha ezt jogszabály nem korlátozza	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
9.	A törvény alapján közzéteendő jogszabálytervezetek és kapcsolódó dokumentumok; a helyi önkormányzat képviselő-testületének nyilvános ülésére benyújtott előterjesztések a benyújtás időpontjától	Törvény eltérő rendelkezése hiányában a benyújtás időpontját követően azonnal	Az előző állapot 1 évig archívumban tartásával
10.	A közfeladatot ellátó szerv által közzétett hirdetmények, közlemények	Folyamatosan	Legalább 1 évig archívumban tartásával
11.	A közfeladatot ellátó szerv által kiírt pályázatok szakmai leírása, azok eredményei és indokolásuk	Folyamatosan	Az előző állapot 1 évig archívumban tartásával
12.	A közfeladatot ellátó szervnél végzett alaptevékenységgel kapcsolatos vizsgálatok, ellenőrzések nyilvános megállapításai	A vizsgálatról szóló jelentés megismerését követően haladéktalanul	Az előző állapot 1 évig archívumban tartásával
13.	A közérdekű adatok megismerésére irányuló igények intézésének rendje, az illetékes szervezeti egység neve,	Negyedévente	Az előző állapot törlendő

	elérhetősége, s ahol kijelölésre kerül, az adatvédelmi felelős, vagy az információs jogokkal foglalkozó személy neve		
14.	A közfeladatot ellátó szerv tevékenységére vonatkozó, jogszabályon alapuló statisztikai adatgyűjtés eredményei, időbeli változásuk	Negyedévente	Az előző állapot 1 évig archívumban tartásával
15.	A közérdekű adatokkal kapcsolatos kötelező statisztikai adatszolgáltatás adott szervre vonatkozó adatai	Negyedévente	Az előző állapot 1 évig archívumban tartásával
16.	Azon közérdekű adatok hasznosítására irányuló szerződések listája, amelyekben a közfeladatot ellátó szerv az egyik szerződő fél	Negyedévente	Az előző állapot 1 évig archívumban tartásával
17.	A közfeladatot ellátó szerv kezelésében lévő közérdekű adatok felhasználására, hasznosítására vonatkozó általános szerződési feltételek	A változásokat követően azonnal	Az előző állapot 1 évig archívumban tartásával
18.	A közfeladatot ellátó szervre vonatkozó különös és egyedi közzétételi lista	A változásokat követően azonnal	Az előző állapot törlendő
19.[78]	A közfeladatot ellátó szerv kezelésében levő, a közadatok újrahasznosításáról szóló törvény szerint újrahasznosítás céljára elérhető közadatok listája, valamint azok rendelkezésre álló formátuma	A változásokat követő 15 napon belül	Az előző állapot 1 évig archívumban tartásával
20.[79]	a 19. sor szerinti közadatok újrahasznosítására vonatkozó általános szerződési feltételek elektronikusan szerkeszthető változata	A változásokat követő 15 napon belül	Az előző állapot törlendő
21.[80]	A 19. sor szerinti közadatok újrahasznosítás céljából történő rendelkezésre bocsátásért fizetendő díjak általános jegyzéke	A változásokat követő 15 napon belül	Az előző állapot törlendő
22.[81]	A közadatok újrahasznosításáról szóló törvény szerinti jogorvoslati tájékoztatás	A változásokat követő 15 napon belül	Az előző állapot törlendő
23.[82]	A közfeladatot ellátó szerv által megkötött, a közadatok újrahasznosításáról szóló törvény szerint kötött kizárólagos jogot biztosító megállapodások szerződő feleinek megjelölése, a kizárólagosság időtartamának, tárgyának, valamint a megállapodás egyéb lényeges elemeinek megjelölése	A változásokat követő 15 napon belül	Az előző állapot törlendő

III. Gazdálkodási adatok

	Adat	Frissítés	Megőrzés
I.[83]	A közfeladatot ellátó szerv éves	A változásokat követően	A közzétételt követő 10

	költségvetése, számviteli törvény szerinti beszámolója vagy éves költségvetés beszámolója	azonnal	évig
2.	A közfeladatot ellátó szervnél foglalkoztatottak létszámára és személyi juttatásaira vonatkozó összesített adatok, illetve összesítve a vezetők és vezető tisztségviselők illetménye, munkabére, és rendszeres juttatásai, valamint költségtérítése, az egyéb alkalmazottaknak nyújtott juttatások fajtája és mértéke összesítve	Negyedévente	A külön jogszabályban meghatározott ideig, de legalább 1 évig archívumban tartásával
3.[84]	A közfeladatot ellátó szerv által nyújtott, az államháztartásról szóló törvény szerinti költségvetési támogatások kedvezményezettjeinek nevére, a támogatás céljára, összegére, továbbá a támogatási program megvalósítási helyére vonatkozó adatok, kivéve, ha a közzététel előtt a költségvetési támogatást visszavonják vagy arról a kedvezményezett lemond	A döntés meghozatalát követő hatvanadik napig	A közzétételt követő 5 évig
4.[85]	Az államháztartás pénzeszközei felhasználásával, az államháztartáshoz tartozó vagyonnal történő gazdálkodással összefüggő, ötmillió forintot elérő vagy azt meghaladó értékű árubeszerzésre, építési beruházásra, szolgáltatás megrendelésre, vagyonértékesítésre, vagyonhasznosításra, vagyon vagy vagyoni értékű jog átadására, valamint koncesszióba adásra vonatkozó szerződések megnevezése (típusa), tárgya, a szerződést kötő felek neve, a szerződés értéke, határozott időre kötött szerződés esetében annak időtartama, valamint az említett adatok változásai, a nemzetbiztonsági, illetve honvédelmi érdekkel közvetlenül összefüggő beszerzések adatai, és a minősített adatokkal kivételével A szerződés értéke alatt a szerződés tárgyáért kikötött - általános forgalmi adó nélkül számított - ellenszolgáltatást kell érteni, ingyenes ügylet esetén a vagyon piaci vagy könyv szerinti értéke közül a magasabb összeget kell figyelembe venni. Az időszakonként visszatérő - egy évnél hosszabb időtartamra kötött - szerződéseknél az érték kiszámításakor az ellenszolgáltatás egy évre számított összegét kell alapul venni. Az egy költségvetési évben ugyanazon szerződő féllel kötött azonos tárgyú szerződések értékét egybe kell számítani	A döntés meghozatalát követő hatvanadik napig	A közzétételt követő 5 évig
5.	A koncesszióról szóló törvényben	Negyedévente	A külön jogszabályban

	meghatározott nyilvános adatok (pályázati kiírások, pályázók adatai, az elbírálásról készített emlékeztetők, pályázat eredménye)		meghatározott ideig, de legalább 1 évig archívumban tartásával
6.[86]	A közfeladatot ellátó szerv által nem alapfeladatai ellátására (így különösen egyesület támogatására, foglalkoztatottai szakmai és munkavállalói érdek-képviseleti szervei számára, foglalkoztatottjai, ellátottjai oktatási, kulturális, szociális és sporttevékenységet segítő szervezet támogatására, alapítványok által ellátott feladatokkal összefüggő kifizetésre) fordított, ötmillió forintot meghaladó kifizetések	Negyedévente	A külön jogszabályban meghatározott ideig, de legalább 1 évig archívumban tartásával
7.	Az Európai Unió támogatásával megvalósuló fejlesztések leírása, az azokra vonatkozó szerződések	Negyedévente	Legalább 1 évig archívumban tartásával
8.	Közbeszerzési információk (éves terv, összegzés az ajánlatok elbírálásáról, a megkötött szerződésekről)	Negyedévente	Legalább 1 évig archívumbantartásával