Adatkezelés, adatbiztonság, adatvédelem

Adatvédelem és információszabadság a korrupció-megelőzés aspektusából

Vannak a világnak olyan országai, ahol a korrupció a mindennapi élet része, látható és érzékelhető a polgárok számára, máshol ugyan a hétköznapokban láthatatlan marad az állampolgárok előtt, de ettől még létezik és az anyagi mellett erkölcsi károkat okoz.

A személyes adatok védelmét és a közszféra kezelésében lévő vagy annak működéséhez, gazdálkodásához köthető tényadatok nyilvánosságát csak ritkán hozzuk közvetlen összefüggésbe a korrupcióval, pedig az információs jogok gyakorolhatóságának előmozdítása sokat segíthet a közpénzekkel való visszaélések megelőzésében.

A közérdekű adatok nyilvánosságának biztosítása és a korrupció elleni intézkedések közötti kapcsolat egyértelmű. A korrupcióval szembeni fellépés sikeréhez hozzátartozik az elszámoltathatóság a jogalkotásban, a végrehajtásban és az igazságszolgáltatásban. Ehhez szükséges a közinformációkhoz való nyilvános hozzáférés biztosítása.

A közigazgatásban dolgozók személyes adatainak védelme, a személyükkel kapcsolatos adatokról való tudatos gondoskodás nemcsak azért fontos, hogy magánszférájukat tiszteletben tartsák, magánéletüket háborítatlanul élhessék, mint más polgár, hanem azért is, hogy ne váljanak kiszolgáltatottá, esetlegesen jogosulatlan információgyűjtések és visszaélések eszközévé.

A jogtörténeti jelentőségű 15/1991. (IV.13.) AB határozat megalkotásakor a taláros testület tagjait még az töltötte el aggodalommal, hogy az egyes állami nyilvántartások összekapcsolásával az állam túl sokat tudhat meg polgárairól, akik ily módon kiszolgáltatottá válhatnak az állami „túlhatalommal” szemben. A félelem a pártdiktatúra évei után érthető volt, azzal viszont a bírák még nem számolhattak reálisan, hogy az információs technológiák robbanásszerű fejlődése azt is magával hozza, hogy a személyes adatairól nem kellő elővigyázatossággal gondoskodó polgárról (felhasználóról) némi informatikai tudással felvértezve bárki „személyiségprofilt” alkothat.

Fogalmak

A fejezet megértéséhez és könnyebb elsajátításához elengedhetetlen néhány, a témával szorosan összefüggő fogalom értelmezése.

- **Infotv**.: a hatályos magyar adatvédelmi törvény (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény)

- **Érintett**: bármely meghatározott, személyes adat alapján azonosított vagy azonosítható természetes személy;

- **Személyes adat**: Minden azonosított vagy azonosítható természetes személlyel kapcsolatba hozható adat vagy abból levonható következtetés;

A személyes adatjelleg meghatározásakor a tény, adat, információ konkrét személyhez társíthatósága a döntő. Az adatvédelmi hatóságok vezetői részvételével működő nemzetközi munkacsoport (WP 29) álláspontja szerint annak meghatározására, hogy egy személy azonosítható-e, minden olyan módszert figyelembe kell venni, amit az adatkezelő vagy más személy valószínűleg felhasználna a személy azonosítására. Az egyén kiválasztásának hipotetikus lehetősége nem elég ahhoz, hogy a személyt azonosíthatónak tekintsük. Ha figyelembe véve minden ilyen módszert e lehetőség nem létezik, vagy elhanyagolható, a személyt nem lehet azonosíthatónak tekinteni és az információ nem számít személyes adatnak.

- **Különleges adat**: a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;

- **Bűnügyi személyes adat**: a büntetőeljárás során, a bírósági ítélettel összefüggésben valamint a büntetés végrehajtása során keletkezett, az érintettel kapcsolatba hozható adatok köre;

- **adatkezelés**: az adatokon végzett valamely művelet, amely érdemi hatással van az adatok sorsára pl. személyes adatok gyűjtése, rendszerezése, tárolása, továbbítása, nyilvánosságra hozatala, törlése;

- **adatkezelő**: az a természetes vagy jogi személy, aki érdemi döntési kompetenciával rendelkezik az adatok tekintetében és az adatokon a műveletet végrehajtja vagy megbízást ad e tevékenység elvégzésére;

- **adatfeldolgozó**: a megbízott, aki vagy amely az adatkezelővel kötött szerződése alapján az adatok feldolgozását, azaz az érdemi döntést nem igénylő technikai műveleteket elvégzi;

- **adattovábbítás**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

- **nyilvánosságra hozatal**: az adat szélesebb körben, bárki számára történő megismerhetővé tétele;

- **adatzárolás**: az adat azonosító jelzéssel ellátása annak érdekében, hogy az adatok felhasználását véglegesen vagy meghatározott időre felfüggesszék;

- **adattörlés**: az adatok felismerhetetlenné tétele oly módon, hogy az érintett és az adat közötti kapcsolat helyreállítása többé már nem lehetséges;

- **adatmegsemmisítés**: az adatokat tartalmazó adathordozó teljes és végleges megsemmisítése;

- **közérdekű adat**: a személyes adatokon kívül minden olyan információ, amely bármely állami, önkormányzati vagy egyéb közfeladatot ellátó szerv működésével, gazdálkodásával, vagy feladata ellátásával összefüggésben az adott szerv kezelésében van;

- **közérdekből nyilvános adat**: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

- **Üzleti titok:** a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása a jogosult jogszerű pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.

Az Eu adatvédelmi irányelve, uniós jogharmonizáció és a magyar szabályozás

A személyes adatok védelmére vonatkozó szabályozás összehangolására az OECD (a Gazdasági Együttműködés és Fejlesztés Szervezete) törekedett először abból a megfontolásból, hogy a tagállamok eltérő természetű szabályozása a gépi adatfeldolgozás vonatkozásában ne hátráltassa a gazdasági kapcsolatok fejlődését. Az OECD célja olyan szabályozás megalkotása volt, amely a személyes adatok magas szintű védelme mellett a gazdasági kapcsolatok zavartalanságát biztosítja. Az 1980-ban megfogalmazott alapelvek nagy hatást gyakoroltak az Európai Unió adatvédelmi jogi szabályozására is.

Az Európai Parlament és a Tanács 95/46/EK irányelve (a továbbiakban: Adatvédelmi Irányelv) a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról címmel 1995-ben született meg. Az irányelv úgy valósítja meg a személyes adatok magas szintű védelmét, hogy közben biztosítja a tagállamok közötti szabad adatforgalmat és nem nehezíti meg a belső piac hatékony működését. Az irányelv az adatkezelésnek már nem csak gépi, hanem mindennemű formáját szabályozni kívánta.

Az Adatvédelmi Irányelv, elfogadásának idejére tekintettel, még nem igazodik egészen az új technológiák adatvédelmi elvárásához.

A gazdasági szempontok, a kereskedelmi és gazdasági együttműködéshez kapcsolódó személyes adatok szabad áramlását segítő szemléletmód a kezdetektől fogva jellemzi az uniós megközelítést, olyannyira, hogy sokáig a közös piac szabályozásával foglalkozó főigazgatósághoz tartozott az adatvédelmi feladatok koordinálása. Sajnos a magyar adatvédelmi jog harmonizációja az utóbbi szempontot kevésbé tartotta szem előtt, és inkább a védelem minél magasabb szintjére összpontosított.

Az Adatvédelmi Irányelv célja a személyes adatok magas szintű védelme. A harmonizáció keretében a tagállamoknak minden olyan szabályt, amely az irányelvben a személyes adatok védelmét erősíti, és azt még a nemzeti szabályozás nem tartalmazta, a jogharmonizációs kötelezettségből fakadóan át kellett ültetni a hazai szabályozásokba. A harmonizációs kötelezettség a következő főbb témákat ölelte fel: az adatvédelmi jog alapvető definícióinak tisztázása; a nemzetközileg kimunkált adatvédelmi alapelvek (például a célhoz kötött adatkezelés elve, vagy az adatok minőségének követelménye) érvényesítése; harmadik országokba irányuló adattovábbítás követelményeinek meghatározása; a különleges adatok védelmére vonatkozó speciális szabályok megalkotása; az érintettek (adatalanyok) jogainak biztosítása, amely magában foglalja a jogellenes adatkezelés elleni tiltakozás jogát is. Lényeges még a bárki által hozzáférhető adatvédelmi nyilvántartás vezetése, adatvédelmi hatóság felállítása, e hatóság arra való jogosultsága, hogy bizonyos adatkezelési műveletek előtt előzetes ellenőrzést végezhessen és a jogellenes adatkezelés esetére megfelelő szankciók foganatosíthasson.

Az adatvédelmi irányelv helyes értelmezése alapján a tagállamoknak lehetőségük volt arra, hogy az irányelvben megfogalmazott szabályoknál szigorúbb védelmet írjanak elő. Mivel a magyar szabályozás – a szocializmus keserű tapasztalatainak okán – igen szigorú lett, Magyarország adatvédelmi szabályozását az Európai Unió még csatlakozásunk előtt megfelelő védelmi szintűnek minősítette. Az első magyar adatvédelmi törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi

LXIII. törvény (Avtv.) a védelem szintjét illetően megfelelt az uniós elvárásoknak, csak néhány részletszabály vonatkozásában kellett csatlakozásunk alkalmával módosítani.

A hatályos adatvédelmi törvény „az információs önrendelkezési jogról és az információszabadságról" címmel 2011. évi CXII. számon 2012. január 1-jén lépett hatályba (a továbbiakban : Infotv.) és kifejezetten a magánszféra védelmének kontextusában értelmezi a személyes adatok védelméhez fűződő jogot mikor kinyilatkoztatja: „a törvény célja az adatok kezelésére vonatkozó alapvető szabályok meghatározása annak érdekében, hogy a természetes személyek magánszféráját az adatkezelők tiszteletben tartsák".

Az Európai Bizottság döntése nyomán az Irányelvet az új technológiákhoz igazodva felülvizsgálják, de közben továbbra is rendszer-semleges szabályozás kialakítására törekednek. Az Irányelvet így néhány éven belül a tagálamokban közvetlenül hatályos rendelet váltja fel, ami a nemzeti törvényeket, így az Infotv-t is felülírja, illetve kiváltja majd.

A személyes adatok jogszerű kezelésének feltételei

Kötelező és önkéntes adatkezelés

Az adatkezeléseket jogalapjuk különbözősége szerint két nagy csoportba sorolhatjuk. Megkülönböztetünk

- **kötelező adatkezeléseket**, mikor a jogalkotó valamely „közérdeken alapuló célból" törvényben szabályozza az adatkezelést és az érintett rendelkezési joga adatai felett korlátozott
- **önkéntes adatkezeléseket**, mikor az érintett önkéntes hozzájárulásán alapszik az adatok kezelése.

Formázott: Felsorolás és számozás

Kötelező adatkezelésként említhetjük a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (KEKKH) kezelésében lévő állami nyilvántartásokat, így a személyi-adat és lakcímnyilvántartást, bűnügyi nyilvántartást és a gépjármű-nyilvántartás. Szintén kötelező adatkezelés valósul meg, mikor a törvény azért írja elő a személyes adatok kezelését, átadását, mert az valamely ügylet létrejöttéhez feltétlenül szükséges (pénzügyi konstrukciók, polgári jogi engedményezés).

Önkéntes adatkezelésekként tekintünk a piaci résztvevők üzleti, kereskedelmi célú adatbázisaira, hiszen döntően az érintettek hozzájárulása alapján kerülnek felvételre a személyes adatok.

Kötelező adatkezeléseknél az adatkezelés célját és feltételeit, a kezelendő adatok fajtáit és megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét a törvényben és a törvényi keretek között önkormányzati rendeletben kell meghatározni. Bizonyos adatállományok esetében az állami adatkezelőknek kizárólagos jogosultságai vannak, lényegében csak állami vagy önkormányzati szerv kezelhet bűnmegelőzési, bűnüldözési, közigazgatási és igazságszolgáltatási feladatok ellátásához szükséges bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat.

Általában kötelező, ágazati törvények felhatalmazása alapján, szigorú szabályok mellett kerül sor a különleges adatok körén belül az egészségügyi adatok kezelésére.

A hozzájárulás

Az Infotv értelmező rendelkezéseiben foglaltak szerint **a hozzájárulás** az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez.

Megfelelőnek tekinthető a tájékoztatás, ha még az adat felvételét megelőzően történik, tartalma egyértelmű és részletes, kiterjed az adatkezelő személynek megnevezésére, az adatkezelés céljára, jogalapjára, időtartamára, az adatszolgáltatás önkéntes vagy kötelező jellegére és informálja az érintettet arról is, hogy információs önrendelkezési jogait a tevékenység kapcsán miként érvényesítheti.

Az adatkezelők a részletes tájékoztatás megadására törekedve gyakran abba a hibába esnek, hogy a terjedelmesre sikerült tájékoztatás tartalmában kevéssé érthető és az adott adatkezelés sajátosságait nem veszi kellően figyelembe. Az adatkezelő által adandó tájékoztatással szemben alapvető elvárás az is, hogy az egyértelmű és közérthető legyen.

A hozzájárulás akkor minősíthető jogszerűnek, ha az adatszolgáltatás az érintettek részéről **önkéntesen** történt. Az önkéntesség megállapításának feltétele viszont az, hogy az adatkezelő az adatkezelés célját, és a szolgáltatandó adatok körét pontosan meghatározva oly módon tájékoztassa az érintetteket, hogy azok szabadon mérlegelhessék, rendelkezésre bocsátják-e a kért adatokat vagy sem. Megkérdőjelezhető az önkéntesség akkor is, ha az adatszolgáltatás megtagadása esetén az érintettet hátrányok érhetik, vagy a jogviszony megkötése kapcsán méltán feltételezheti, hogy diszkriminálják.

Számos jogviszonyban pl munkaviszonyban kétséges, hogy a munkavállaló valóban önkéntesen adja-e beleegyezését egyes, a munkáltató által bevezetni kívánt intézkedéshez kapcsolódó adatkezeléshez, hiszen egzisztenciális hátrányoktól vagy munkajogi következményektől tarthat, és inkább eltűri a munkáltató túlzott mértékű adatgyűjtését.

Különleges adatok jogszerű kezelése

A különleges adatok kezeléséhez a nemzetközi kötelezettség teljesítéséből vagy a közérdeken alapuló célból fakadó törvényi szintű szabályozás mellett jogalapul szolgálhat **az érintett írásbeli hozzájárulása** is. Írásbeli hozzájárulásként kell elfogadni, minden olyan elektronikusan rögzített nyilatkozatot is, amelyből kétséget kizáróan bizonyítható, hogy a hozzájárulás megadása kétséget kizáróan az érintettől származik. A többszörös elektronikus megerősítő nyilatkozatok együtt nagy valószínűséggel garantálják azt, hogy az adatokat valóban az érintett felhasználó tette meg.

„Vélelmezett" adatkezelések

Vélelmezzük az érintettek hozzájárulását **szükséghelyzetben** és az **érintett kérelmére indult eljárásokban valamint közszereplés** kapcsán is. Jogilag egyértelműen megalapozott az érdek és vélelmezhető az érintett hozzájárulása olyankor, mikor fizikai okból vagy cselekvőképtelensége folytán nem képes hozzájárulását adni adatai

kezeléséhez, holott ez életének, testi épségének megóvásához, megmentéséhez szükséges. Méltányolható és a törvény szerint megengedett a személyes és különleges adatok mielőbbi felvétele akkor is, ha az adatkezelés az érintett saját vagy más személy létfontosságú érdekeinek védelméhez, valamint katasztrófa- vagy szükséghelyzet elhárításához vagy megelőzéséhez szükséges.

Megadottnak tekinthető a hozzájárulás akkor is, ha az érintett a bíróságnál vagy valamely hatóságnál kezdeményezi eljárás megindítását. Ilyenkor ugyanis az érintett tudatában kell, hogy legyen, az ő érdekében történik személyes adatainak kezelése, e nélkül ugyanis az eljárás lefolytatása lehetetlen lenne, vagy eredményes lefolytatása kerülne veszélybe. A tisztességes adatkezelés követelményének megfelelően a hatóságnak arra kell törekednie, hogy elsődlegesen az érintettől történjen az adatfelvétel, de ennek hiányában lehetősége van arra, hogy az eljárás lefolytatásához szükséges mértékben az érintettől felvett adatokon kívül is beszerezzen és jogszerűen kezeljen információkat a kérelmezőről.

Abban az esetben, ha az érintett valamely más, hatósági vagy bírósági eljárás tárgyi hatálya alá nem tartozó ügyben kezdeményezi ügye (pl. valamely szolgáltató cégnél) intézését, úgy kizárólag az általa megadott adatkörben lehet vélelmezni hozzájárulását, további adatokat csak akkor szerezhet be az adatkezelő, ha ehhez az érintett hozzájárult.

A közszereplést vállaló érintett által közölt adatok további felhasználásakor szintén vélelmezni kell az érintett hozzájárulását, hiszen az elmondottak a nyilvánosság előtt egyszer már ismertté váltak és a közszereplő magánszférához való joga szűkebb, mint más magánemberé. Amennyiben az adatok ismételt nyilvánosságra hozatala az eredeti közzétételtől eltérő célból becsületsértő módon történik, úgy nem az adatvédelem, hanem a személyiségvédelmét szolgáló eszközök ~~vehetők~~ igénybevétele a célravezető.~~.~~

Új jogalapok az Infotv-ben

Az új szabályozás alapján azokban a helyzetekben is jogszerűnek tekinthető az adatkezelés, ha az érintett hozzájárulásának beszerzése lehetetlen vagy aránytalan költséggel járna, és a személyes adat kezelése

a) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy

b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges. Ebben az esetben azonban további feltételként szabja meg Infotv., hogy az adatkezelést megalapozó jogos érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásához képest arányos legyen.

A hozzájárulás beszerzésének lehetetlensége, annak nyelvtani értelmezése folytán valóban azt kell, hogy jelentse, az érintettől „fizikailag” is kivitelezhetetlen belegyezésének rögzítése például azért, mert nagyszámú és előre nem is meghatározható érintettről van szó (pl. a Google street view szolgáltatása esetén). E megengedő felhatalmazás semmiképpen sem eredményezheti azt, hogy az érintettet megkerülve, szándékával ellentétesen kerüljön sor az adatkezelésre. Az aránytalan költség a konkrét jogeset tükrében értelmezhető, de nyilvánvalóan azt kell, hogy jelentse, hogy a hozzájárulások beszerzésére fordított erőforrások oly nagyok lennének, hogy az adatkezelés „rentabilitását” veszélyeztetnék. A jogi kötelezettségre hivatkozás csak jóhiszeműen értelmezhető s nem vezethet az együttműködési kötelezettség kijátszásához. Az új jogalap alkalmazására mindenekelőtt az üzleti életben kerülhet sor.

Az arányos korlátozás elvére tekintettel szintén lehetőség kínálkozik arra is, hogy az érintett hozzájárulásának visszavonása esetén se kelljen törölni a személyes adatokat amennyiben az adatkezelő jogi kötelezettségének teljesítése vagy jogos érdekének érvényesítése érdekében erre szükség van. Ennek a felhatalmazásnak az Infotv.-be történő beépítésére azért volt szükség, hogy az érintett, az adatvédelmet kihasználva rosszhiszeműen ne akadályozhassa meg a másik fél jogszerű érdekérvényesítését.

Az adatkezelés elveinek való megfelelőség

Az adatkezelésnek mindvégig összhangban kell lennie annak eredetileg rögzített céljával, **az adatok felvételének** pedig **tisztességesnek és törvényesnek kell lennie.** Az elv érvényesülésére már az adatok felvételénél is figyelemmel kell lenni. Amennyiben az adatforrások jogszerűsége megkérdőjelezhető, úgy az adatok további felhasználása sem törvényes.

Az adatkezelés szempontjából sarkalatos elv: **a célhoz kötöttség elve.** E követelmény lényege, hogy az adatokat pontosan meghatározott célból kezeljék és ezzel az egyén valamely jogának gyakorlását vagy kötelezettsége teljesítését segítsék elő. A célhoz kötött adatkezelés elve magában foglalja az **adatminimalizálás elvét is**, mely szerint csak a cél teljesüléséhez feltétlenül szükséges mértékben és ideig kezeljenek személyes adatokat.

Az Alkotmánybíróság 15/1991. (IV. 13.) AB határozatában leszögezte, hogy személyes adatot feldolgozni csak pontosan meghatározott és jogszerű célra szabad. Az adatfeldolgozásnak minden szakaszában meg kell felelnie az adatalanyokkal előzetesen közölt célnak. Az adatfeldolgozás célját úgy kell az érintettel közölni, hogy az megítélhesse az adatfeldolgozás hatását jogaira, és megalapozottan dönthessen az adat kiadásáról; továbbá, hogy a céltól eltérő felhasználás esetén élhessen jogaival. Ugyanezért az adatfeldolgozás céljának megváltozásáról is értesíteni kell az érintettet. Az érintett beleegyezése nélkül az adatok új célú feldolgozása csak akkor jogszerű, ha azt meghatározott adatra és feldolgozóra nézve törvény kifejezetten megengedi. A célhoz kötött adatkezelés elvéből következik, hogy a meghatározott cél nélküli, "készletre", előre nem meghatározott jövőbeni felhasználásra való adatgyűjtés és tárolás alkotmányellenes.

Az adatkezelő hitelét is erősíti **a személyes adatok minősége elvének** való megfelelőség. E kritérium szerint az adatkezelés során biztosítani kell az **adatok pontosságát, teljességé**t és – ha az adatkezelés céljára tekintettel szükséges – **naprakészségét**. Az adatkezelőnek törekednie kell arra is, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

A személyes adatok felvételénél, a pontos adatrögzítésre kell kiemelt figyelmet fordítani. Az elvárás különösen fontos a személyazonosító és kapcsolat-felvételi adatokat tartalmazó nyilvántartások esetén. Az elírás és adatbeviteli hiba sokszor az adminisztrátor gondatlanságára vezethető vissza, hátrányos következménye mégis jelentős lehet, az adatkezelésen végiggyűrűzve az érintett jogérvényesítését is negatívan befolyásolhatja.

A naprakészség az időtényező jelentőségére utal, hogy a tárolt személyes adatoknak **időszerűnek** kell lenniük, elavult adatok nem képezhetik felelős döntések alapját, az adatbázis aktualizálása az üzleti szereplőknek is elemi érdeke. A kezelt személyes

adatokkal szemben támasztott minőségi elvárásnak való megfelelőség az adatkezelő és az érintett együttműködését feltételezi.

Az érintett jogai

Az információs önrendelkezési jog lényegi tartalma, hogy az érintett személyes adatai kezelése tárgyában érdemi döntést hozhat, nyomon követheti adatai kezelését. Jogait a kötelező adatkezeléseknél csak korlátozottan, míg az üzleti adatkezeléseknél szabadabban érvényesítheti. Ilyenkor csak az esetleges szerződéses kötelmekre kell tekintettel lennie. Az érintettet, aktivitásától is függően az alábbi jogok illetik meg:

- *Tájékoztatáshoz való jog*

Az adatkezelő által adott előzetes tájékoztatástól függetlenül az érintett bármikor informálódhat arról, hogy pontosan mely személyes adatait és milyen feltételekkel kezelik. Kérelmére legfeljebb 30 napon belül érdemi tájékoztatást kell kapnia az adatkezelőtől. A **tájékoztatás** az ugyanazon adatkérés vonatkozásában évente egy alkalommal ingyenes.

Az érintett arról is érdemben informálódhat, hogy személyéről a nyilvántartásokból mely szervek mikor igényeltek információkat. A nyilvántartást vezető adatkezelő ugyanis az alapnyilvántartáshoz tartozó un. adattovábbítási regiszterben köteles rögzíteni, hogy a gépi adatlekérdezésekre (priorálásokra) mikor, milyen okból került sor. Az adat-megismerésről adandó tájékoztatás nemzetbiztonsági vagy nyomozati érdekből korlátozható.

- *Helyesbítéshez való jog*

Az érintett adatelírás, hibás adatbevitel észlelése esetén kezdeményezheti személyes adatai helyesbítését. Megalapozott kérelem esetén az adatkezelőnek gondoskodnia kell a hiba korrigálásáról és emellett arról is, hogy az általa korábban helytelen tartalommal továbbított adatokat szintén javítsák, a pontosítás átvezetése megtörténjen más „kapcsolódó" nyilvántartásokban is. E jog gyakorlásához az érintettnek anyagi érdeke is fűződik, hiszen más jogügyletek vonatkozásában kár érheti a hibás nyilvántartás adattartalma miatt. E jog érvényesítése az adatkezelésekkel szemben elvárt „minőségi" elvárásokat is szolgálja, vagyis hogy az adatok pontosak, teljesek és naprakészek legyenek.

A helyesbítéshez való jogból a gyakorlatban az állampolgároknak kötelezettsége is származik, így ~~pl.~~ az „állami alapnyilvántartásokban"_~~, így~~ pl. a személyi adat és lakcímnyilvántartást vezető szervnél be kell jelenteniük az adataiban bekövetkezett változást. E bejelentést az állampolgárok gyakran elmulasztják és a hibák az állami alapnyilvántartásokban komplikációkat okoznak és százalékos arányban is kimutatható és észlelhető hiányosságokhoz, pontatlanságokhoz vezetnek. Nem érvényesített szankciók hiányában a hibák állandósulnak és mivel a kötelező nyilvántartások a hiteles

okmánykiállítás alapjául szolgálnak, a pontatlan, elévült adatok a közokiratban (pl. hatósági erkölcsi bizonyítvány, hiteles tulajdoni lap) is megjelenhetnek.

A változás-bejelentés önkéntes adatkezeléseknél általában szerződésben vállalt kötelezettség (pl. hitel-szerződésben), ami lényegében a polgári jog együttműködési elvének érvényesítésén alapszik.

- *Törléshez való jog, az adatok zárolása*

Az érintett az önkéntes alapú adatkezeléseknél nemcsak előzetesen, hanem a későbbiekben is dönthet úgy, hogy nem kívánja adatai szerepeltetését valamely adatbázisban. Jogszabályban előírt, kötelező adatkezelések esetében erre nincsen lehetőség.

Szintén korlátozottan érvényesítheti az érintett törléshez való jogát, ha a felek között korábban létrejött megállapodás teljesítéséhez, mintegy járulékosan szükséges a személyes adatok kezelése.

Az adatok zárolásának van helye, ha vitatott az adatkezelés jogszerűsége vagy az adatok helyessége. Ilyenkor a tényállás tisztázásáig, illetve az eljárás lefolytatásáig az adatok kezelése lényegében felfüggesztésre kerül.

Amennyiben az adatkezelő az érintett helyesbítés, zárolás vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 30 napon belül írásban kell az érintettel közölnie az elutasítás indokait.

- *Tiltakozáshoz való jog*

Az adatvédelmi szabályozás külön nevesíti az érintett azon jogát, hogy az általa jogellenesnek vélt adatkezelés ellen az adatkezelőnél felszólaljon. Erre kötelező adatkezelések esetén kívül akkor nyílik lehetősége, ha az adatkezelés kifejezetten nem az érintett, hanem csak az adatkezelő vagy harmadik személy érdekében áll. Az Infotv. néhány tipikus adatkezelést ki is emel: a közvetlen üzletszerzés, közvélemény-kutatás és tudományos kutatás eseteit említve, mely adatkezelések vonatkozásában e jog kifejezetten érvényesíthető. A közvetlen üzletszerzéssel (direkt-marketinggel), közvélemény-kutatással foglalkozó cégek ugyanis az érintett kifejezett tiltakozásáig jogszerűen kezelhetnek a személyes adatok, az adatok csak az érintett kifejezett kérésére kerülnek tiltó, un. Robinson listára.

Adatbiztonsági ismeretek

Az adatok védelméről valamennyi adatkezelőnek gondoskodnia kell függetlenül attól, hogy az üzleti vagy az állami szektorban tevékenykedik. E törvényi kötelezettség nem bürokratikus jogalkotói szándékon alapszik, mögötte az adatkezelők érdeke áll. Míg a magán-adatkezelőnek üzleti érdeke fűződik a megfelelő óvintézkedések megtételéhez, addig az állami adatkezelő az állami adatvagyon „gazdájaként" tartozik fokozott felelősséggel polgárai személyes adatainak védelméért. Egy esetleges adatvesztés jelentős veszteséggel járhat, a közfeladatot ellátó szervek működését akadályozhatja, a piaci részvevők üzletmenetét pedig ellehetetlenítheti, az üzleti partnerek, ügyfelek

bizalma pedig meginoghat a cég iránt. Az adatbiztonsági előírások betartásának és betartatásának fontos szerepe lehet a korrupció megelőzésében is. Egy döntési kompetenciával rendelkező vagy a döntésre érdemi befolyással rendelkező kormányzati tisztviselő korrupciós célból történő megkörnyékezését hosszas és alapos információ-gyűjtés előzheti meg, hiszen a célszemély személyes adatainak birtokában, ismerve családi és vagyoni helyzetét, érdeklődési körét, munkavégzési és egyéb szokásait, ~~„beszervezése" vagy az Ö és sérelmére tervezett~~ a bűncselekmény sikerének esélye is nagyobb.

Az adatbiztonság jegyében a rendelkezésre álló adatokat minden lehetséges fenyegetéstől (threatness) védeni kell. Problematikus, hogy a nagyfokú védelem biztosításával egyidejűleg biztosítani kell, hogy közben az adatok rendelkezésre álljanak (availability), de csak kizárólag azok számára, akiket erre feljogosítottak (confidentiality).

Az információbiztonság valamennyi információ védelmét feltételezi, jóval szélesebb adatkörre vonatkozik, mint az Infotv. által szabályozott „adatbiztonság", ami a személyes adatokra szorítkozva írja elő az adatkezelővel szemben a biztonsági elvárásokat.

7. § (1) 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.

(2) Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

A törvény az érintettek magánszférája védelmének jegyében általános tartalmú adatbiztonsági elvárásokat fogalmaz meg, a részletes szabályokat a tevékenység specialitásaihoz igazodva az ágazati jogszabályok és az egyedileg kialakított adatbiztonsági szabályzatok tartalmazzák.

Az adatkezelőnek, adatfeldolgozónak számos és különféle veszélyforrással kell számolnia, az elemi károk (tűz-, vízkár, villámcsapás) mellett a szándékos külső emberi beavatkozások (hacker-, vírustámadás) és a munkavállaló hanyagsága, gondatlansága is komoly kockázati tényezők.

A törvények alapján a technika mindenkori fejlettségét figyelembe véve, a magasabb szintű védelmet biztosító megoldást kell választani, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen védve az adatokat. Az eltérő célú adatbázisokat elkülönítetten kell kezelni, a jogosulatlan adatbevitel, lekérdezés és változtatás megakadályozása érdekében a hozzáférési jogosultságokat differenciáltan kell kiosztani. Az adatlekérdezéseket és adattovábbításokat naplózni kell, az esetleges típushibákra vészforgatókönyvvel kell készülni. Az esetleges rendszerhibák regisztrálását jelentésben kell rögzíteni (belső incidens-nyilvántartás) így a történések rekonstruálhatók.

A központi nyilvántartásokból való lekérdezéshez a jogosultságot az okmányirodák működésének személyi és technikai feltételeiről szóló 58/1999. (XII.30.) BM rendeletben

foglalt feltételeknek megfelelő köztisztviselő részére adják ki. A jogosult hozzáférési kártyát kap, ezt másnak nem adhatja oda, a kártya és a nyilvántartási rendszerek használatát biztosító azonosítót (jelszó, PIN-kód, felhasználói azonosító) más személynek nem hozhatja tudomására. A rendeletben előírtakon kívül fontos, hogy az adatbiztonság érdekében a priorálási jogosultak a lekérdezési műveletek befejezése után a rendszerből kijelentkezzenek, a számítógépet adatlekérdezésre aktív állapotban felügyelet nélkül ne hagyják.

Az adatbiztonságnak jól tervezhető területe az eszközvédelem. Kevésbé lehet azonban felkészülni a foglalkoztatottak gondatlanságából fakadó következményekre. Különös figyelmet kell ezért fordítani a megelőzésre, ami a munkavállalók/köztisztviselők rendszeres képzését, felkészítését igényli.

Az Adatvédelmi Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport 5/2009. számú véleményében a közösségi oldalak adatvédelmi beállításainak jelentőségére hívja fel a figyelmet és a hozzáférés gondos kialakítására koncentrál. Kiemeli az üzemeltető/szolgáltató felelősségét annak apropóján, hogy mivel az alapértelmezett beállításokon a regisztrált felhasználók csak kisebb hányada változtat és differenciálja a hozzáférést adataihoz, ezért a szolgáltatónak kellene az alapbeállítást a személyes adatok védelmével összhangban kialakítania. A Munkacsoport elvárásként fogalmazza meg, hogy a szolgáltatóknak olyan alapértelmezett beállítást kellene nyújtaniuk, amely a külső látogató számára redukált hozzáférést tesz csak lehetővé, és az adat-megismeréshez a felhasználó kifejezett hozzájárulása szükséges minden olyan esetben, mikor az ismertségi körön kívüli személy kíván a profilt alkotó információhoz hozzáférni. A Munkacsoport ideálisnak tartaná, ha a korlátozott hozzáférésű profilokat elzárnák a belső keresőmotorok elől, az életkor, lakhely, vagy más hasonló paraméterek szerinti keresési lehetőségeket is beleértve. A hozzáférés kiterjesztésére vonatkozó döntések pedig nem lehetnének hallgatólagos jellegűek, pl. oly módon, hogy az ismertségi hálózat kezelője „elutasítási" lehetőséget biztosít.

A nyilvántartások automatikus összekapcsolása és az adatok érintetthez rendelése a biztonsági kockázatot is növeli, ezért a törvény feltételeket ír elő ennek megvalósulása esetére. A törvények alapján a technika mindenkori fejlettségét figyelembe véve, a magasabb szintű védelmet biztosító megoldást kell választani, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen védve az adatokat. Az eltérő célú adatbázisokat elkülönítetten kell kezelni, a jogosulatlan adatbevitel, lekérdezés és változtatás megakadályozása érdekében a hozzáférési jogosultságokat differenciáltan kell kiosztani. A hozzáférési jogosultságokat célszerű rendszeres időközönként az aktuális munkakörhöz és feladatokhoz mérten felülvizsgálni, illetve rendelkezni arról, hogy a munkaviszony megszűnése esetén a hozzáférési jogot haladéktalanul visszavonják a távozó munkavállalótól.

Az adatvesztés ellen hatékony titkosítási és erős hozzáférés-ellenőrzési megoldásokat célszerű használni, mivel a mobileszközök és internet-alkalmazás elterjedése sebezhetőbbé tette az adattárolási rendszereket. Az online szolgáltatások és távoli hozzáférések bővülésével „biztonsági rések" keletkeztek. E biztonsági rések rosszindulatú kihasználásának esélyét növeli a munkavállaló, felhasználó tapasztalatlansága, hanyagsága, ezért is fontos a munkatársak oktatása és az adatbiztonsági előírások betartatása.

Az adatvédelmet felügyelő szervek az Eu-ban

Európai Adatvédelmi Biztos (European Data Protection Supervisor)

A Biztos feladatai közé tartozik az EU szervek adatkezeléseinek ellenőrzése, a velük kapcsolatos egyéni panaszok kivizsgálása. A biztoshoz bárki fordulhat, akinek megítélése szerint személyes adatainak védelméhez fűződő jogát valamely uniós szerv vagy intézmény adatkezelése megsértette. A Biztos hatásköre tehát csak az uniós szervek adatkezelésének ellenőrzésére korlátozódik, a tagállami intézmények és magántársaságok tevékenységét a Biztos nem vizsgálhatja. Tanácsadói, véleményezési jogkörében tanácsokat ad az uniós szervek számára, a 29. cikk szerinti munkacsoportban pedig a tagállami hatóságok közötti együttműködés koordinálásával segíti az egységes európai adatvédelmi joggyakorlat kialakítását.

Az Adatvédelmi Irányelv 29. cikk szerint létrejött Adatvédelmi Munkacsoport

Az Adatvédelmi Irányelv 29. cikke rendelkezik arról, hogy a tagállamok adatvédelmi hatóságaiból álló munkacsoport végzi munkáját. A szervezet célja az adatvédelmi irányelv hatálya alá eső adatvédelmi kérdések megvitatása, állásfoglalások és vélemények kibocsátása, tekintettel az adatvédelmet érintő technológiai újításokra is. A munkacsoportban való részvétel a csatlakozás előtt még nem volt kötelező, de a magyar adatvédelmi biztos megfigyelői státusszal részt vehetett az üléseken. Jelenleg az ülések állandó résztvevője a Nemzeti Adatvédelmi és Információszabadság elnöke vagy helyettese.

Az Európai Unió Bírósága

A luxembourgi székhelyű Bíróság dönt az uniós jog értelmezésének ügyeiben. Jogértelmezési kérdésekben a nemzeti bíróságoknak is iránymutatást ad, álláspontja kötelező a tagállamok bíróságaira nézve.

Az Emberi Jogok Európai Bírósága

A nemzetközi szerződések és belső törvények mellett az adatvédelmi jog forrásai a bírósági jogfejlesztés eredményei is. A strasbourgi székhelyű Emberi Jogok Európai Bírósága „Az emberi jogok és az alapvető szabadságok védelméről" szóló egyezmény alapján hozza meg döntéseit. Az 1950-ben Rómában kelt Egyezmény szövege, sem annak kiegészítő jegyzőkönyvei nem nevesítik a személyes adatok védelméhez fűződő jogot. A bíróság adatvédelmi tárgyú ítéleteit elsősorban az egyezmény magán- és családi élet tiszteletben tartásáról szóló 8. cikke alapján hozza meg. E cikk deklarálja, hogy „mindenkinek joga van arra, hogy magán- és családi életét, lakását és levelezését tiszteletben tartsák."

A hazai adatvédő szerv: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)

A NAIH 2012. január 1-jétől, az Infotv. hatályba lépésétől látja el feladatait a hazai adatvédelem területén. A független autonóm államigazgatási szerv, kizárólag a törvényeknek alárendelve segíti a személyes adatok védelméhez, valamint a közérdekű és a közérdekből nyilvános adatok megismeréséhez való jog érvényesülését. Míg a korábbi felügyeleti szerv, az Adatvédelmi Biztos Irodája csak korlátozott hatósági jogkörrel rendelkezett a jogellenes adatkezelés szankcionálására, addig a NAIH alapjogvédelmi funkciói megtartása mellett akár 10 millió Ft. bírsággal is sújthatja a jogsértő adatkezelőt.

A Hatóság kettős funkcióját követi a Hatóság eljárási rendje is.~~,~~ M~~m~~íg a vizsgálati eljárás alapvetően a régi biztosi gyakorlat szerint a kötetlenebb eljárási rend szerint alakul, addig hatósági eljárás lefolytatásánál a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) rendelkezéseire is tekintettel kell lennie az intézkedéseket foganatosító hatósági munkatársak.

A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet és bejelentése miatt nem érheti hátrány. Amint a biztosi években, úgy – a bírói függetlenségre tekintettel - most is kizárt a Hatóság érdemi vizsgálata, ha az adott ügyben bírósági eljárást folytatnak vagy az ügyben már jogerős döntés született.

Belső adatvédelmi felelős

A nagyobb adatkezelők szervezeten belül is gondoskodnak adatkezeléseik ellenőrzéséről. Belső adatvédelmi felelős kinevezése kötelező az országos hatáskörű adatállományok tekintetében (hatósági, munkaügyi, bűnügyi), emellett a magánszférában a pénzügyi szervezetnél valamint az elektronikus hírközlési és közüzemi szolgáltatónál is. Tevékenysége a szervezeten belüli adatbiztonsági feltételek teljesülését és az érintettek jogérvényesítését szolgálja. A jogi, közigazgatási, informatikai vagy e végzettségeknek megfelelő szakképesítéssel rendelkező adatvédelmi felelős akkor tudja hatékonyan végezni a teljes szervezetre irányuló ellenőrzési feladatait, ha kizárólag a szerv első számú vezetőjének felel, munkájában mások által nem utasítható. Tekintettel arra, hogy az érintettek jogérvényesítését is szolgálnia kell, célszerű elérhetőségeinek szerepeltetése az adatkezelő honlapján. Feladatai közé tartozik a jogszabályok és belső szabályzatoknak való megfelelőség rendszeres ellenőrzése, az egyedi bejelentések kivizsgálása, a NAIH-tól érkező megkeresések határidőn belüli, adekvát megválaszolása és az adatvédelmi ismeretek oktatása is a szervezeten belül.

Adatvédelmi nyilvántartás

A Hatóság az Irányelv rendelkezéseivel összhangban a személyes adatokra vonatkozó adatkezelések meghatározott köréről nyilvántartást vezet. A nyilvántartás adatkezelési célonként tartja nyilván az adatkezelők által bejelentett adatkezeléseket. A nyilvántartás, amely elsősorban az érintettek tájékozódását szolgálja, tartalmazza a konkrét adatkezelés céját, jogalapját, a kezelt személyes adatok körét, az adatkezelő és az esetleges adatfeldolgozó(k) megnevezését.

Formázott: Betűtípus: Verdana, 10 pt

Formázott: Sorkizárt

Formázott: Betűtípus: Verdana, 10 pt

Formázott: Sorkizárt

Formázott: Sorkizárt

Nyilvános adatok az átláthatóság szolgálatában

A transzparenciát két, az Infotv-ben nevesített „adatcsoport" nyilvánosságán keresztül érvényesíti az Infotv.: a személyes adatoknak nem tekinthető, közszféra kezelésében lévő és annak működésére vonatkozó **közérdekű adatok** megismerhetőségén, valamint a valamely közérdek megalapozta okból nyilvánosságra hozott vagy hozható egyéb, akár személyes adatok (**közérdekből nyilvános adatok**) megismerhetősége által.

A **közérdekű adat** jellemzői:

- nem személyes adatok körébe tartozó tényadatok

- közfeladatot ellátó szerv (pl. minisztérium, önkormányzat, autonóm államigazgatási szerv, közszolgáltatást végző társaság) birtokában vannak és annak tevékenységével kapcsolatosak (pl. a szerv feladatellátása, gazdálkodása).

Közfeladatot ellátó szervként tekintünk:

- minden államigazgatási és önkormányzati szervre

- e szervek tulajdonában álló cégekre, amennyiben tevékenységük a szervek feladatellátásához köthető

- egyéb olyan szervezetre, társaságra, amelyek kötelezően ellátandó feladatait jogszabály határozza meg.

A **közérdekből nyilvános adat**ok jellemzői:

- személyes adatok is lehetnek

- valamely nevesíthető közérdek alapozza meg a nyilvánosságukat

- törvény pontosan meghatározza a nyilvánosságra szánt adatkört.

Közérdekből nyilvános adatok egyebek mellett a következő adatok:

- a hitelezői érdekek védelme és a piaci forgalom biztonsága érdekében a cégjegyzék adatai (Ctv. alapján)

- az ingatlan-nyilvántartás tulajdoni lapjának adattartalma (Inytv. alapján)
- a Gt. alapján közzéteendő a szabályozott piacra bevezetett, nyilvánosan működő részvénytársaságok felügyelőbizottsági tagjainak neve és juttatásaik
- az átláthatóság szolgálatában a köztulajdonban álló gazdasági társaságok vezető tisztségviselőinek, fb. tagjainak neve, tisztsége, juttatásai (Kgtv. alapján)
- a közszolgálatban dolgozó közfeladatot ellátó személyek feladatköréhez kapcsolódó személyes adatok az Infotv. 26. § (2) bekezdése alapján a jogviszonyt szabályozó törvényekben (Kttv., Hszt.,) meghatározottak szerint.

A közérdekű, közérdekből nyilvános adatok megismeréséhez fűződő alapvető jogunk érvényesítése a közszféra átláthatóságát segíti, hatékony eszköze a közpénz-felhasználás állampolgári ellenőrzésének és általa a korrupció megelőzésében és felderítésében is szerepe lehet. E jog érvényesítéséhez a közfeladatot ellátó szerveknek is hathatós segítséget kell nyújtaniuk: egyrészről a nyilvános adatokra nézve közzétételi kötelezettségük van, másrészről az egyedi adatigényléseket az Infotv-ben meghatározott eljárási rendben kell teljesíteniük.

A közérdekű adatigénylés szabályai, rendje, az igény elutasítása

A közérdekű adat megismerése iránti igényt bárki benyújthatja. Az adatigénylés teljesítésére vonatkozó szabályokat az Infotv. tartalmazza, annak részletes eljárási rendjét a közérdekű adatokat kezelő szervnek szabályzatban kell rögzíteni, a részletszabályok – a törvényi keretek között - a speciális szervezeti sajátosságaihoz igazodhatnak.

A közérdekű adat-igénylési szabályzat kidolgozásánál az Infotv. alábbi kötelező szabályaira kell figyelemmel lenni:

- az adatigénylés szóban, írásban vagy elektronikus úton is benyújtható, a szabályzat nem korlátozhatja az igénylés módját és nem tehet kizárólagossá egyes módokat

- a tájékoztatás-adás tartalmában a közérthetőségre kell törekedni

- amennyiben korábban nyilvánosságra hozták az igényelt adatokat, úgy az igény a nyilvános forrás (link) megjelölésével is teljesíthető

- az igénylés oka, jogalapja, annak alanyi jogi jellegéből kifolyólag nem firtatható

- az igénylő adatai tartalmában és időben is csak korlátozottan kezelhetőek (csak annyiban, hogy a kapcsolatfelvétel, válaszadás teljesíthető, a költségtérítés megfizethető legyen; az adatigénylés teljesítését követően az igénylő személyes adatai törlendők);

- az adatokat tartalmazó dokumentumról az igénylő másolatot is kaphat

- a másolaton a meg nem ismerhető adatokat felismerhetetlenné kell tenni

- a másolat készítéséért csak a szerv tényleges költségei számíthatóak fel (munkaköltség, nyereségorientált elemek nem érvényesíthetők)

- a határidők a 15 illetve 8 naptári naphoz igazodnak

- a határidők tekintetében fő szabály a 15 napos teljesítési határidő

- költségtérítés megállapítása esetén a határidő a költségtérítés megfizetésekor kezdődik

- a határidő, jelentős terjedelmű adatigénylés esetén további 15 nappal meghosszabbítható

- a határidő meghosszabbításáról, illetve a megállapított költségtérítés mértékéről az adatigénylés beérkezését követő 8 napon belül kell értesíteni az igénylőt

- az igény megtagadásáról, annak egyértelmű indokáról és a jogorvoslati lehetőségekről az adatigénylés beérkezését követő 8 napon belül kell értesíteni az igénylőt

Az adatigénylés elutasítása jogszerű, ha:

- az igényelt adat nem közérdekű/közérdekből nyilvános adat
- minősített adat (a Mavtv. szerinti eljárás szerint Ld. Közigazgatási alapvizsga tananyag)
- ~~üzleti titok (Ptk. 81. §)~~
- döntés megalapozását szolgáló adat
- uniós jogi aktus folytán pénzügyi vagy gazdaságpolitikai érdek miatt kivételt képező adatkör
- az adatfajták meghatározásával azt külön törvény honvédelmi, nemzetbiztonsági, bűnüldözési vagy bűnmegelőzési; környezet- vagy természetvédelmi érdekből; központi pénzügyi vagy devizapolitikai érdekből; külügyi kapcsolatokra, nemzetközi szervezetekkel való kapcsolatokra; bírósági vagy közigazgatási hatósági eljárásra tekintettel kiveszi a megismerhető adatok köréből.

Az állami és önkormányzati vagyon kezelésével, birtoklásával, használatával, hasznosításával, az azzal való rendelkezéssel kapcsolatos adat nem minősül üzleti titoknak és fő szabályként nyilvános. Ez a kitétel egybeesik azzal, a transzparencia ügyét szolgáló követelménnyel, hogy az állam üzleti titokra az adatigénylés megtagadásaként alapvetően nem hivatkozhat.

Formázott: Betűtípus: Verdana, 10 pt

Formázott: Sorkizárt, Behúzás: Bal: 0,63 cm

Formázott: Betűtípus: Verdana, 10 pt

Formázott: Betűtípus: Verdana, 10 pt

Elektronikus információszabadság

A digitális kor vívmányai ~~amellett, hogy sajnos korlátozzák a magánéletet,~~ az információszabadság ügyét segíthetik. Számos nemzetközi példa bizonyítja, hogy az állami szervek internetes, úgynevezett *„proaktív információs politikája”* az állam átláthatóságát, nyilvánosság általi ellenőrizhetőségét is növelik.

Az állam működésének, a közpénzek felhasználásának átláthatóságát biztosítja – az egyedi adatigénylések teljesítésén túl – a közfeladatot ellátó szervek azon kötelezettsége, amely a közérdekű, illetve közérdekből nyilvános adatok elektronikus, azaz internetes honlapon történő közzétételét írja elő.

1. A közérdekű adatok elektronikus közzétételének általános kötelezettsége

Az általános elektronikus közzétételi kötelezettség jogszabályi hátterét – az elektronikus információszabadságról szóló 2005. évi XC. törvény (Eitv.) hatályon kívül helyezését követően – az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény IV. fejezete teremti meg.

Az egyedi adatigénylésekhez hasonlóan az elektronikus információszabadság esetében is a közfeladatot ellátó szerv kötelezettsége, hogy mivel ezen jog jogosultja bárki lehet, a közzétett adatokat bárki, a személyes adatok közlése, kezelése nélkül megismerhesse, letölthesse (Infotv. 33. § (1) bekezdés).

Az általános közzétételi kötelezettség két fórumon, honlapon, a saját honlapon és az egységes közadatkereső (www.kozadat.hu) oldalon való közzétételt jelent azok számára, akik az Infotv. 33. § (2) bekezdése szerint kötelesek saját honlapot működtetni: a Köztársasági Elnöki Hivatal, az Alkotmánybíróság Hivatala, az Országgyűlés Hivatala, az Állami Számvevőszék, a Magyar Művészeti Akadémia, a Magyar Tudományos Akadémia, az Országos Bírósági Hivatal és a Legfőbb Ügyészség, a fővárosi és a megyei kormányhivatalok, az országos kamarák, és a központi államigazgatási szervek (pl. Nemzeti Adó- és Vámhivatal, GYEMSZI, Nemzeti Fejlesztési Ügynökség)

Azon szervek, amelyek nem kötelesek saját honlapot működtetni választhatnak, hogy

- saját vagy

- társulásaik által közösen működtetett vagy

- a felügyeleti, szakmai irányításukat vagy működésükkel kapcsolatos koordinációt ellátó szervek által fenntartott,

- valamint az erre a célra létrehozott központi honlapon (www.kozadat.hu) való közzététellel is eleget tehetnek kötelezettségüknek (Infotv. 33. § (3) bekezdés).

A kisebb települések önkormányzatai tehát nem kötelesek saját honlapot létrehozni, külön informatikust alkalmazni a közzétételi kötelezettségek teljesítésére, hanem a közigazgatási informatika infrastrukturális megvalósíthatóságának biztosításáért felelős miniszter (jelenleg a nemzeti fejlesztési miniszter) megbízásából a Nemzeti Infokommunikációs Szolgáltató Zrt. keretein belül működő Közadat programhoz való csatlakozással, és az általános közzétételi lista adattartalmának feltöltésével is teljesíthetik ezen kötelezettségüket.

Az általános közzétételi kötelezettség teljesítéséhez az Infotv. 1. számú mellékletében meghatározott adatokat kell közzétenni.

Ezen adatok három csoportra oszthatók:

1. szervezeti, személyzeti adatok

2. tevékenységre működésre vonatkozó adatok

3. gazdálkodási adatok

A gazdálkodási adatokkal összefüggésben kiemelendő, hogy az államháztartásról szóló 2011. évi CXCV. törvény és annak végrehajtásáról szóló 368/2011. (XII. 31.) Korm.

rendelet további gazdálkodási adatok közzétételéről rendelkezik, amely azonban már túlmutat az általános közzétételi kötelezettségen.

Az Infotv. rendelkezéseit az alábbi rendeletek egészítik ki részletszabályokkal:

- 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,
- a közzétételi listákon szereplő adatok közzétételi mintáiról szóló 18/2005. (XII. 27.) IHM rendelet.

2. Egyedi közzétételi listák (Infotv. 33. § (3) bekezdés)

A közfeladatot ellátó szerv vezetője – a NAIH véleményének kikérésével – további kötelezően közzéteendő adatkört határozhat meg. Mivel az Infotv. 1. számú mellékletének III/4. pontja az ötmillió forintot elérő szerződésekről kell adatokat közzétenni, jellemzően az önkormányzatok a közérdeklődésre való tekintettel az ennél alacsonyabb értékű szerződésekről is publikálnak adatokat a honlapjukon, illetve a közadat.hu-n.

3. Különös közzétételi listák (Infotv. 37. § (2) bekezdés)

Egyes ágazati jogszabály a közfeladatot ellátó szervtípusra vonatkozóan meghatározhat egyéb közzéteendő adatokat.

3.1. A bírósági határozatok nyilvánossága

A bírósági határozatok meghatározott körének nyilvánosságát a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény (a továbbiakban: Bszi.) XII. fejezet szabályozza.

Alapvetően a bírósági jogalkalmazást meghatározó bírósági ítéleteket kell a Bírósági Határozatok Gyűjteményében közzétenni, a kisebb jelentőségű, bagatell ügyekben született ítéleteket nem kell nyilvánosságra hozni, hiszen azok nem gyakorolnának jelentős hatást a polgárok jogkövető magatartására.

Közzé kell tenni a jogegységi határozatokat, az elvi bírósági ítéleteket, valamint a Kúria is és az ítélőtáblák is kötelesek az általuk az ügy érdemében hozott határozatokat digitalizálva közzétenni.

Nem kell azonban közzétenni a fizetési meghagyásos ügyeket, a cégbírósági, csőd- és felszámolási eljárásokban, valamint a házassági bontóperben, az apaság és származás megállapítása iránti perben született ítéletet.

Természetesen a közzététel nem sértheti az eljárásban érintettek információs önrendelkezési jogát, így a Bszi. 166. §-ában külön rendelkezik a személyes adatok, minősített adatok felismerhetetlenné tételéről, amely azonban nem járhat azzal, hogy a határozat érdemi része érthetetlen tartalommal jelenjen meg. Fontos kiemelni, hogy a határozatokból nem lehet felismerhetetlenné tenni a közérdekű, a közérdekből nyilvános adatokat, valamint az alperesként pervesztes természetes személy nevét, továbbá jogi személy vagy jogi személyiséggel nem rendelkező szervezet nevét és székhelyét, ha a határozatot olyan ügyben hozták, amelyben jogszabály alapján közérdekű igényérvényesítésnek helye van. (www.birosag.hu)

3.2. A jogalkotás nyilvánossága

Az Alaptörvény B) cikkének (2) bekezdésében deklarált, az Alkotmánybíróság által számos határozatban értelmezett jogállamiság elvéből, annak integráns részeként értelmezett jogbiztonság elvéből, valamint az Alaptörvény VI. cikkének (2) bekezdésében foglalt, és az Infotv.-ben részletezett közérdekű adatok megismeréséhez való jogból is levezethető a jogszabályok közzétételének – így bárki által megismerhetővé tételének – kötelezettsége. Mind a jogszabályalkotás során, mind a kihirdetést követően biztosítani kell az egyének számára, hogy megismerhessék a rájuk kötelező jogszabályokat.

Ennek megfelelően – a korábban az Eitv.-ben szabályozott – *„A jogalkotás nyilvánossága"* cím alatt található rendelkezések átkerültek a jogalkotásról szóló 2010. évi CXXX. törvény (a továbbiakban: Jat.) 25/A. §-ába, valamint a Jat. 28/B-29/A. §-aiba.

A jogszabály-alkotás nyilvánosságát a jogszabályok előkészítésében való társadalmi részvételről szóló 2010. évi CXXXI. törvény szabályozza. Ezen törvény előírja, hogy a jogszabályt az azt előkészítő minisztérium a kormányzati szervekkel való egyeztetésre bocsátással egyidejűleg az egyeztetés állapotának megjelölésével a honlapján tegye közzé. A törvény azonban nem vonatkozik a nem minisztériumban előkészített jogszabályok tervezeteire, például az egyéni képviselői indítványként benyújtott törvényjavaslatokra.

A jogalkotás átláthatóságát, megértését hivatott szolgálni azon rendelkezés is, amely szerint – bizonyos kivételektől eltekintve – a tervezettel együtt közzé kell tenni a jogalkotásról szóló törvényben meghatározott előzetes hatásvizsgálat összefoglalóját is. A jogszabálytervezetek, a koncepciók és a hatásvizsgálatok így nem minősülhetnek korlátozott nyilvánosságú, döntés megalapozását szolgáló adatnak.

Nemzeti Jogszabálytár (www.njt.hu) elektronikus közszolgáltatásként működő, bárki számára térítésmentesen hozzáférhető, egységes szerkezetű szövegeket tartalmazó elektronikus jogszabálygyűjtemény.

Önellenőrző kérdések

1. *Milyen összefüggésekre tud rámutatni az adatvédelem, információszabadság és a korrupció megelőzése között?*
2. *Mit tud az EU Adatvédelmi irányelvéről?*
3. *Miként kezelhető szükséghelyzetben személyes adat?*
4. *Az adatbiztonság jegyében miként kell megterveznie az adatkezelőnek az adatkezelési műveleteket?*
5. *Mi az adattovábbítási nyilvántartás funkciója?*
6. *Mely szervek gondoskodnak az EU-ban az adatvédelem érvényesüléséről?*
7. *Magyarországon melyik szerv felügyeli az adatkezelési szabályok betartását?*
8. *Milyen feladatai vannak a belső adatvédelmi felelősnek?*
9. *Melyek a közérdekből nyilvános adatok jellemzői?*
10. *Miként alakul a közérdekű adatigénylés határideje jelentős terjedelmű adatigénylés esetén?*

11. Mikor jogszerű a közérdekű adatigénylés elutasítása?

Irodalomjegyzék

1. *Adatvédelem és információszabadság a mindennapokban Bp., 2012 HVG-Orac*
2. *Az információs társadalom jogi vetületei – Alkalmazott jogi informatika, PPKE JÁK Bp, 2011, Adatvédelmi jogi ismeretek Révész Balázs - Baka Péter*
3. *3. Az információs jogok kihívásai a XXI. Században - tanulmánykötet*

I. A statisztikai adatkezelés

1. A statisztikai adatkezelés jogi alapjai és keretei

A Hivatalos Statisztikai Szolgálat tagjai a különféle társadalmi és gazdasági jelenségek átfogó jellemzése céljából adatgyűjtéseket végeznek, illetve külső forrásokból adatokat vesznek át. Az adatkezelés rendszerében a statisztikai adatok kezelése kitüntetett szereppel bír. Ennek fő oka, hogy habár a statisztika mindig valamilyen sokaságot jellemez, alapvetően különféle statisztikai egységekről (pl. természetesen személyek, vállalkozások) szerez be információt. A hivatalos statisztikai adatgyűjtések és adatátvételek egyik legfontosabb tulajdonsága, hogy **az egyes egységekre vonatkozó információk gyűjtése a statisztikák előállításának eszköze, de nem célja**. A statisztika fókuszában mindig az egyedek valamilyen csoportja áll és nem célja az egyes egyedek vizsgálata. Ebből a sajátosságból eredő statisztikai adatkezelésre két alapvető fontosságú hazai jogszabály vonatkozik. Egyrészt az 1993. évi XLVI. törvény a statisztikáról, kiegészülve e törvény végrehajtásáról szóló 170/1993. (XII. 3.) kormányrendelettel (együtt továbbiakban: Statisztikai törvény), mely a Központi Statisztikai Hivatal feladatai közé sorolja az általa kezelt adatok védelmét; másrészt az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.

A statisztikai adatkezelés egyik kulcsfogalmát, az egyedi adatot, a Statisztikai törvény nevesíti. Ennek értelmében **egyedi adat**nak minősül **a természetes és a jogi személy, valamint a jogi személyiséggel nem rendelkező adatszolgáltatóval kapcsolatba hozható adat** (Statisztikai törvény 17.§. (2)).

Alapszabályként a Statisztikai törvény az egyedi adatokra vonatkozóan megfogalmazza, hogy az „csak statisztikai célra használható, mással csak akkor közölhető, és abban az esetben adható át, valamint hozható nyilvánosságra, ha ehhez az adatszolgáltató előzetesen írásban hozzájárult." (Statisztikai törvény 18.§. (1)).

A hazai jogszabályokon felül az adatok védelmére vonatkozóan az Európai Parlament és a Tanács 223/2009/EK rendelete (továbbiakban: Európai statisztikai törvény), valamint az általa hivatkozott Európai Statisztika Gyakorlati Kódexe (továbbiakban: Gyakorlati Kódex) jelentik a legfontosabb nemzetközi előírásokat. Jogilag fontos szempont, hogy a Gyakorlati Kódex önmagában nem rendelkezik jogi kötőerővel, azonban az Európai statisztikai törvény lényegében kötelezővé teszi használatát, így előírásainak a magyar Hivatalos Statisztikai Szolgálat tagjai is kötelesek megfelelni.

A Gyakorlati Kódex, mint az európai statisztikák fejlesztéséért, előállításáért és közzétételéért felelős nemzeti szervezetekre vonatkozó elv- és ismérvgyűjtemény, külön elvben rendelkezik a statisztikai adatok bizalmas kezeléséről. A Gyakorlati Kódex 5. számú elve kimondja, hogy „[az európai statisztikák fejlesztéséért, előállításáért és közzétételéért felelős intézmények] a legmesszebbmenőkig tiszteletben tartják az adatszolgáltatók (háztartások, vállalatok, közigazgatási intézmények és más válaszadók) jogait, biztosítják az általuk szolgáltatott információk bizalmas kezelését és kizárólag statisztikai célokra történő felhasználását".

2. A statisztikai adatkezelés alapfogalmai

Amikor adatvédelemről beszélünk, több megoldásra gondolhatunk: informatikai biztosítékok alkalmazására, jogosultságkezelésre, jogi garanciákra vagy módszertani, matematikai megoldásokra is. Összefoglalóan úgy mondhatjuk, hogy **az adatvédelem minden olyan jogi, módszertani, fizikai, informatikai és egyéb eljárás, módszer, tevékenység, amit annak érdekében alkalmaznak, hogy a rendelkezésre álló adatokat a jogosulatlan, céltól eltérő felhasználástól, az adatszolgáltatók magánjellegű adatainak megismerésétől megóvják**.

A statisztikai adatok védelmének két kulcsfogalma az azonosítás, illetve a felfedés. **Az azonosítás lényében azt az eseményt jelenti, amikor egy adott statisztikai egységet (pl. természetes személyt, vállalatot)** egy adatsorban **egyértelműen felismernek**. Egy adatszolgáltatót legtöbbször a hozzá tartozó adatok alapján azonosíthatnak (pl. vállalatokat törzsszám alapján), de azonosítás történhet indirekt módon, például kizárás útján is. A statisztikai adatok védelme szempontjából **a felfedés**

az egyik legfontosabb fogalom, mely **azt jelenti, hogy a közzétett adatokból egy adott statisztikai egységre vonatkozóan új, eddig nem ismert információt ismerünk meg**. **A felfedési kockázat tehát az azonosítási kockázat, valamint új információ nyilvánosságra kerülésének együttes veszélyét jelenti.** Fontos megjegyezni, hogy a felfedésnek nem szükséges feltétele az azonosítás. Előfordulhat ugyanis, hogy egy új információ egy csoport minden tagjára érvényes. Ebben az esetben nem szükséges a csoport minden tagját azonosítani ahhoz, hogy tudjuk, hogy az új információ minden, az adott csoporthoz tartozó tagra is vonatkozik. Például ha megtudnánk, hogy minden ipari eszköz gyártásával foglalkozó vállalat környezetszennyező, akkor biztosra tudhatjuk, ha egy ilyen céggel találkozunk, hogy környezetszennyező tevékenységet folytat.

Jelen fejezetrész célja, hogy a Hivatalos Statisztikai Szolgálat, kiemelten a Központi Statisztikai Hivatal által alkalmazott módszertani adatvédelmi megoldásokat röviden megismertesse. A gyakorlatban az adatvédelmi tevékenység ellátása során követett módszertani megoldásokat **felfedés elleni védelem** fogalomkör alatt fogjuk össze, amely **a statisztikai célra összeállított adatállományok módosítását célzó olyan módszerek összességét jelenti, melyek a lehető legnagyobb mértékben csökkentik a felfedési kockázatot**.

Statisztikai célra gyűjtött adatok tehát statisztikai célra, a sokaság jellemzésére használhatók, azaz nem tehetők hozzáférhetővé úgy, hogy abból az adatszolgáltatókra azonosíthatóan jusson ki információ. Az azonosítás lehetősége, kockázata jellemző módon több tényező függvénye. Ezt a kockázatot az érintett adatkör, az adatkiadási csatorna, a felhasználó személye, intézménye, a felhasználás célja és körülményei is behatárolhatják.

A felfedés elleni védelmi módszerek megismerése előtt említést kell tenni a táblázatos adat, illetve a mikroadat fogalmáról. **A táblázatos adat olyan adatot jelent, melyben az egyedekre vonatkozó információt valamely ismérvek szerint aggregáljuk és ezt az összesített információt táblázatos formában jelenítjük meg. A mikroadat** pedig **olyan rekordok sorozatából álló állomány, amely elemi megfigyelési egységek adatait tartalmazza, egy rekord–egy elemi megfigyelési egység elv alapján.** Elemi megfigyelési egység lehet például egy személy, egy háztartás, egy lakás, egy vállalat, egy üzlet terméke, egy vállalat egy tranzakciója, stb.

II. A statisztikai adatok felfedés elleni védelme

A táblázatos adat, illetve a mikroadat fogalmaknak a következőkben bemutatott módszerek ismertetésénél van kiemelt szerepe, más és más módszereket alkalmazhatunk ugyanis a táblázatos adatok és a mikroadatok védelmére.

1. A táblázatos adatok felfedés elleni védelmi módszerei

Táblázatos adatok felfedés elleni védelme során az alapprobléma, hogy egy összeállított táblázatot eredeti formájában nem közölhetünk, mert úgynevezett érzékeny cellát tartalmaz. **Érzékeny cella a táblázat olyan cellája, amelyet valamilyen adatvédelmi szabály alapján védeni kell.** Amennyiben érzékeny cella szerepel a közlendő táblázatban, úgy több megoldást is alkalmazhatunk a védettség biztosításához. Az alábbiakban a hivatalos statisztikai gyakorlatban leginkább használt módszereket mutatjuk be röviden. Az ismertetendő módszerek csupán a „klasszikus" felfedés elleni védelmi módszereket jelentik. A gyakorlatban a statisztikai adatok felfedés elleni védelme során további módszereket alkalmazhatunk, illetve az ismertetett módszerek kombinált alkalmazása is jellemző.

1. Cellaelnyomás alkalmazása

A cellaelnyomás a táblázatos adatvédelem egyik módszere, melynek eredményeképp **adott cellák értékét nem közöljük, hanem „letakarjuk" (kitöröljük) és egy egyezményes jelleg helyettesítjük** (például … jelet írunk a helyére). A cellaelnyomás két egymásra épülő részből áll: elsődleges és másodlagos cellaelnyomásból.

a. Elsődleges cellaelnyomás

Az elsődleges cellaelnyomás olyan, a táblázatos adatok védelmére alkalmazott eljárás, melynek lényege, hogy valamilyen táblázatos adatok védelmére alkalmazandó szabály(ok) eredményeként kijelölt érzékeny cellákat nem közlünk. Az elsődlegesen elnyomandó cellák kijelölésére több módszert hívhatunk segítségül. Az alábbiakban a 3 leggyakrabban használt módszert mutatjuk be.

– *Küszöbszabály*

Egy táblázatban a küszöbszabály szerint érzékenynek tekintendő egy cella, ha az adatszolgáltatók száma egy meghatározott küszöbértéknél alacsonyabb. Fontos megjegyezni, hogy a Statisztikai törvény 19.§-a előírja, hogy **„összesítve sem lehet nyilvánosságra hozni** *[…]* **olyan adatot, amelynél az adatszolgáltatók száma háromnál kevesebb". A küszöbszabálynak ezt a nevesített változatát nevezzük a gyakorlatban hármas szabálynak.** A jogi megkötés miatt tehát háromnál alacsonyabb küszöbszám nem választható, azonban szakmai megfontolások alapján keményebb szabályok (magasabb küszöbszám) is kijelölhető a táblázatok védelmére.

Példa: Az 1. táblázatpár bal oldalán látható egy nyilvánosságra hozatalra szánt táblázatrészlet, mely területi és tevékenység szerinti bontásban tartalmaz értékösszegeket. Az ehhez a táblázathoz tartozó gyakorisági táblázat a jobb oldalon látható, mely az egyes cellákhoz hozzájárulók számát (pl. adatszolgáltatók számát) tartalmazza.

	1. régió	***2. régió***	***3. régió***	***…***
1. tevékenység	12500	5900	5500	…

2. tevékenység	2500	600	1400	…
3. tevékenység	4500	7400	6200	…
…	…	…	…	…

	1. régió	***2. régió***	***3. régió***	***…***
1. tevékenység	2	7	8	…
2. tevékenység	12	11	9	…
3. tevékenység	9	4	7	…
…	…	…	…	…

1. táblázat – Küszöbszabály alkalmazása

A hármas szabályt alkalmazva láthatjuk, hogy az 1-es régió 1-es tevékenységének adata nem közölhető, így azt elsődlegesen elnyomandónak kell kijelölni, ezt jelzi a sötétített hátterű cella. Vegyük észre, hogy amennyiben a küszöbértéket például 5-nek választjuk, abban az esetben a második régió 3-as tevékenységének adata sem közölhető.

– *Dominancia szabály*

Egy táblázatban a dominancia szabály szerint érzékenynek tekintendő egy cella, **ha az értékét adó adatszolgáltatók közül a legnagyobb n darab hozzájárulásának összege meghaladja a cella értékének k%-át**. Az n és k értékét jellemzően az érintett szakstatisztikai terület, a felvétel koncentráltsága, valamint a lehetséges felhasználók ismeretében határozhatjuk meg.

Példa: Dominancia szabály alkalmazásához részletesebben meg kell vizsgálni az egyes cellaértékeket. Az 1. táblázat kiinduló tábláját felhasználva, például n=2 és k=90 esetén a cella érzékenyek tekintendő, ha a két legnagyobb hozzájárulással rendelkező válaszadó hozzájárulásának értéke meghaladja a cella értékének 90%-át. A 2. régió 1. tevékenységi adatát vizsgálva például, amennyiben a két legnagyobb hozzájárulási érték meghaladja az 5310-et (5900×0,9), akkor az 5900-as értéket elsődlegesen elnyomandónak kell kijelölni.

– *p% szabály*

Egy táblázat egy celláját p%-szabály szerint érzékenynek tekintjük, **ha valaki képes a cellához hozzájáruló adatszolgáltatók legalább egyikének a cellához való hozzájárulását a megismert cellaérték alapján legfeljebb p%-os hibával becsülni**. A gyakorlatban általában a második legnagyobb hozzájárulással rendelkező adatszolgáltatónak a legnagyobb hozzájárulásra vonatkozó becslése lehet a legpontosabb. Ezért egy cellát jellemzően érzékenynek tekintünk, ha a cella értékéből a két legnagyobb hozzájárulás értékét levonva a kapott eredmény kisebb, mint a legnagyobb hozzájárulás értékének p%-a.

Példa: Az 1. táblázat kiinduló tábláját felhasználva, például a 2. régió 1. tevékenységének cellája érzékenyek tekintendő, ha az 5900-as értékösszeg esetén igaz, hogy $5900-x_1-x_2 < p/100 \times x_1$, ahol x_1 a cella értékhez legnagyobb hozzájárulással rendelkező válaszadó hozzájárulásának értéke, x_2 pedig a második legnagyobb.

b. Másodlagos cellaelnyomás

A cellaelnyomás második része **a másodlagos cellaelnyomás**, mely **olyan, a táblázatos adatok védelmére alkalmazott eljárás, melynek során az elsődleges**

cellalenyomás során elnyomott cellákon felül további cellákat nyomunk el a táblázat védettségének biztosítása érdekében. Elsődleges cellaelnyomás után minden esetben meg kell vizsgálni, hogy szükséges-e alkalmazni másodlagos cellaelnyomást is, mert az elsődleges cellaelnyomás az esetek többségében önmagában nem elégséges a táblázat védettségének biztosításához.

A cellalenyomás során fontos szempont, hogy a lehető legkisebb legyen az információveszteség. Ez a gyakorlatban legtöbbször azt jelenti, hogy másodlagosan a lehető legkevesebb cellát nyomjuk el. A másodlagosan elnyomandó cellákat általában többféleképpen lehet megválasztani, az alábbi példában egy lehetséges megoldást mutatunk.

Példa: Tegyük fel, hogy a hármas szabály alapján az alábbi táblázatban a sötétített háttérrel jelölt cellát kell elsődlegesen elnyomni.

	1. régió	***2. régió***	***3. régió***	***Összesen***
1. tevékenység	12500	5900	5500	*23900*
2. tevékenység	2500	600	1400	*4500*
3. tevékenység	4500	7400	6200	*18100*
Összesen	*19500*	*13900*	*13100*	*46500*

2. táblázat – Elsődleges cellaelnyomásra kijelölt cellák

A cellaelnyomás szabályai szerint a 12500-as értékösszegű cellát nem közöljük, hanem egyezményes jelleg helyettesítjük. Elég-e ez a táblázat védettségének biztosításához?

A kérdés eldöntéséhez vizsgáljuk meg a 2. táblázatot! Láthatjuk, hogy a táblázatban sor- és oszlopösszesenek is szerepelnek. Amennyiben a 12500-as értékű cellát letakarjuk, úgy az összesenek alapján a cellaérték könnyen visszaszámolható (sor irányban: 23900-5900-5500, oszlop irányban: 19500-2500-4500). Az elnyomás megvalósításakor a legnagyobb kérdés az, hogy mikor lesz egy tábla védett, azaz melyik cellákat kell még másodlagosan elnyomni. Általában igaz, hogy az összesen sorok értékeit nem vonjuk be a másodlagosan elnyomandó cellák körébe, mert az összesen információk letakarása jellemzően jóval nagyobb információveszteséget jelent, mint a táblázat egyéb celláinak elnyomása. Az egyik lehetséges megoldás az alábbi táblázatban látható:

	1. régió	***2. régió***	***3. régió***	***Összesen***
1. tevékenység	12500	5900	5500	*23900*
2. tevékenység	2500	600	1400	*4500*
3. tevékenység	4500	7400	6200	*18100*
Összesen	*19500*	*13900*	*13100*	*46500*

3. táblázat – Elsődleges és másodlagos cellaelnyomásra kijelölt cellák

Amennyiben a sor irányban való visszaszámolhatóság megakadályozásához egy újabb cellát takarok le (pl. az 5500-as értékűt), úgy a tábla továbbra sem védett, mert az eredeti cellaérték oszlop irányban visszaszámolható. Ezért oszlop irányban újabb cella letakarásával (pl. 4500-as értékű) az elsődlegesen elnyomandó cella védettsége biztosítottnak látszik. Ez azonban nem igaz, mert a 4500-as és 5500-as cellák ismét visszaszámolhatók a saját sor-, illetve oszlop összesenjeik alapján. Ezért egy 4. cellát (a táblázatban a 6200-as értékűt) takarom le. Ezzel a tábla védettsége biztosított.

2. Oszlopok/sorok összevonása

A cellaelnyomás mellett vagy helyett „egyszerűbb" megoldásokkal is biztosíthatjuk egy táblázat védettségét. Amennyiben kiadandó táblázatunk érzékeny cellát tartalmaz, megtehetjük, hogy összevonással élünk, azaz valamely oszlopokat vagy sorokat összevonunk (összeadunk) és az így kialakított, alacsonyabb részletezettségű táblázatot adjuk ki.

3. Dimenziókorlátozás

A táblázatos adatok lekérdezésének egyik népszerű megoldása, hogy a felhasználók megadott feltételek szerint maguk készítik el táblázataikat egy vagy több, számukra nem elérhető adatbázisból gyűjtve az információkat. Komoly adatvédelmi problémák merülhetnek fel, amennyiben a felhasználók „túl mélyre tudnak fúrni" ezekben az adatbázisokban, hiszen a felhasználók a kiválasztott tulajdonságok növelésével egyúttal a felfedési kockázatot is növelik. Ilyen esetben célravezető megoldás lehet a választható dimenziók (ismérvek) számának maximalizálása (legyen ez a szám n). Ezt az értéket úgy kell megválasztani, hogy a tulajdonságokból bármely n darabot választva se juthassunk olyan információhoz, amely védendőnek tekintendő. A Központi Statisztikai Hivatal honlapján elérhető Tájékoztatási adatbázis is alkalmazza a dimenziókorlátozást.

2. A mikroadatok felfedés elleni védelmi módszerei

A hivatalos statisztikai adatok kezelése során egyes egyedekre vonatkozó mikroadat állományok állnak elő. Az állományok összeállítása és kialakítása során olyan informatikai és logikai megoldásokat kell alkalmazni, melyek ezen állományok védelmét biztosítani képesek (pl. jogosultsági rendszer, fizikai adatvédelmi megoldások, egyedekre vonatkozó közvetlen azonosítók leválasztása a mikroadat állományról, stb.). Ezeknél az adatállományoknál, jellegüknél fogva, az esetek többségében sokkal hangsúlyosabban jelenik meg az azonosítás és felfedés problematikája, mint a táblázatos adatoknál.

A Központi Statisztikai Hivatal a kutatók számára több csatornán is hozzáférést biztosít a statisztikai célra kezelt mikroadatokhoz, tudományos célból. Az egyik legjelentősebb csatorna a mikroadatok adathordozón való kiadása. Megjegyezzük, hogy jelentősen felértékelődőben van a mikroadatokhoz való biztonságos környezetben való hozzáférés, amely adatvédelmi szempontból más megoldásokat igényel, mint a mikroadatok kiadása.

A biztonságos környezetbeli hozzáférés adatvédelmi kérdéseire ez a rövid összefoglalás nem tér ki.

A mikroadatok kiadása során a mikroadatok felfedés elleni védelmére több módszer áll rendelkezésre. A módszerek rövid ismertetése előtt fontos kiemelni, hogy a mikroadatok felfedés elleni védelménél kiemelt szerepe van a közvetlen és közvetlen azonosíthatóságnak. A **közvetlen azonosítás a statisztikai egység neve és/vagy címe, vagy egy, az egységhez rendelt és nyilvánosan hozzáférhető egyedi azonosítási kód (pl. valamilyen egyedi azonosítószám) alapján való azonosítását jelenti**.

A mikroadatok védelme során fontos szabály, hogy közvetlen azonosítót nem adunk ki, a jogszabályi kötelezettségeken felül részben azért sem, mert nagyon könnyűvé teszik az azonosítást, részben pedig azért sem, mert a statisztikai cél indokolja, hogy nem is lehet szükség közvetlen azonosítókra kutatási célokra. A kiadandó állományban a statisztikai egységek technikai azonosítókkal természetesen elláthatók (a technikai azonosítók hozzárendelése során fontos a rekordok véletlenszerű megkeverése, így biztosított, hogy nagyobb azonosító sorszám például ne magasabb törzsszámot takarjon. Amennyiben indokolt, hasonló módon lehet például a háztartások tagjait „szétültetni" az állományban). **Minden, a közvetlen azonosítástól eltérő módon történő azonosítás a közvetett azonosítás kategóriájába tartozik**, melyeknél jellemzően a kulcs fogalmával dolgozunk. **A kulcs a mikroadat-állomány néhány változójának** (ismérvének) **vagy néhány változó kategóriájának kombinációját jelenti.** A gyakorlatban olyan változókat választunk kulcsváltozónak, amelyek egy vagy több statisztikai egységre általában ismertek a mikroadat-állományból, ezáltal lehetségessé válhat statisztikai egységek választott változók mentén történő azonosítása. Az alábbiakban a leggyakrabban használt mikroadatvédelmi módszereket mutatjuk be röviden.

- *Globális átkódolás*

A globális átkódolás a mikroadatok védelmére alkalmazott olyan eljárás, mely során adott kategorikus változó néhány kategóriáját egy új kategóriába vonjuk össze. A globális átkódolás módszerét olyan esetekben érdemes alkalmazni, amikor egy változó egyes kategóriái bizonyos kulcsokra nézve nagyon kevés számú kombinációban fordulnak elő.

Példa: Ha területi szinten (például település szintű bontás mellett egy adott településen) csak egy női fizikust találunk, érdemes lehet ezt a kategóriát a változó más kategóriáival összevonni (például a fizikusokat a matematikusokkal, melynek eredményeként az adatállományban minden helyen, ahol „fizikus" vagy „matematikus" szerepelt, az átkódolás után „fizikus vagy matematikus"-nak kell szerepelnie.). Hasonló megoldás lehet például az állományban az életkor adatokat korcsoportokba rendezni és csak a

korcsoportos adatokat kiadni vagy például adott területi bontást (pl. település) magasabb aggregáltsági szintre (pl. megye) emelni. A globális átkódolás nagy előnye, hogy egyszerűen alkalmazható, azonban az átkódolást az egész adatállományra kiterjedően kell elvégezni, nem csak az adatvédelmi szempontból aggályos részre (tehát minden más településre vonatkozóan is csak „fizikus vagy matematikus" kategóriát kiadni), így a módszer alkalmazása jelentős információveszteséget eredményezhet.

– *Alsó/felső kódolás*

Az alsó/felső kódolás mikroadatok védelmére alkalmazott olyan eljárás, melynek lényege, hogy **adott változó minden értékét egy definiált értékhatár alatt vagy felett egy megadott értékkel helyettesítjük**, hogy ne legyenek felismerhetőek az extrém értékekkel rendelkező rekordok. Lényegében a globális átkódolás speciális változatának tekinthető.

Példa: Egy adatállományban környezetvédelmi beruházási információk szerepelnek, vállalati telephelyenként, melyek között néhány kiugróan magas értékű található, ezért könnyebben beazonosíthatók. Szakmai és adatvédelmi megfontolások alapján (pl. küszöbszabályhoz hasonlóan) meghatározunk egy felső küszöbértéket, mely legyen most 50.000 euró. Az állományban tehát minden 50.000 euró vagy afeletti környezetvédelmi beruházással rendelkező telephely értékét 50.000-el helyettesítjük. Az alsókódolás hasonló logika alapján történhet, ott az extrém kiugró alacsony értékek kezelése a cél.

– *Kerekítés*

Olyan eljárás, melynek lényege, hogy **numerikus adatokat egy előre meghatározott értéknek megfelelően kerekítjük, vagyis az eredeti adat helyett a meghatározott érték valamely többszörösét szerepeltetjük** az állományban.

Példa: 10-et választva meghatározott értéknek, az állományban lévő minden adat helyett 10 többszörösét fogjuk szerepeltetni, így az egyedi előfordulások száma csökken.

Alapterület (m2)	***Létszám (fő)***	***Árbevétel (Euro)***
747,5	46	3212334
747,5	46	2283340

– *Mikroaggregálás*

Mikroadatok védelmére használt eljárás, melynek lényege, hogy **ha adott egy n elemű mikroadat-állomány, akkor ebből g darab csoportot képzünk úgy, hogy minden egyes csoport legalább k számú egyedet tartalmazzon. Ezután bizonyos változók értékét úgy változtatjuk meg a mikroadat-állományban, hogy azok a képzett csoportokon belül azonos értéket vegyenek fel.**

Példa: Minden egyes csoport esetén kiszámítjuk például az adott csoportba eső értékek átlagát és ezekkel az átlagokkal helyettesítjük a mikroadat-állományban lévő eredeti értékeket.

Vállalat neve	***Alapterület (m^2)***	***Létszám (fő)***	***Árbevétel (Euro)***
Alma Bt.	790	55	3212334
Körte Kft.	710	44	2283340
Barack Bt.	730	32	1989233
Szőlő Kft.	810	17	984983
Banán Kft.	950	3	194232
Kiwi Kft.	510	25	119332
Ananász Bt.	400	45	3012444
Ribizli Bt.	330	50	4233312
Áfonya Kft.	510	5	159999
Eper Kft.	760	52	5333442
Málna Kft.	50	12	645223

4. táblázat – Küszöbszabály alkalmazása[1]

747,5	46	1989233
756,67	8	984983
756,67	8	194232
322,5	33	119332
322,5	33	3012444
322,5	33	4233312
756,67	8	159999
747,5	46	5333442
322,5	33	645223

A bal oldalon látható induló tábla és a jobb oldalon látható eredménytábla összevetéséből jól látszik, hogy a közvetlen azonosító eltávolítása után az alapterületet és a létszámot figyelembe véve képződtek a csoportok, melyeknél a felfedési kockázat jelentősen csökkent.

– *Adatcsere*

Mikroadatok védelmére alkalmazott eljárás, melynek lényege, hogy **megcseréljük bizonyos változók olyan rekordokhoz tartozó értékeit, melyek egy bizonyos kulcson megegyeznek.** A csere jellemzően területi változókat érint.

Példa: Egy adatállományban kiválasztunk két rekordot (i. rekord: nő, Hatvan, fogorvos, házas / j. rekord: férfi, Pécs, állatorvos, elvált) és megcseréljük egy vagy több változó értékét. A csere után például a következő két rekordot kaphatjuk: i. rekord: nő, Pécs, állatorvos, házas; j. rekord: férfi, Hatvan, fogorvos, elvált. Fontos, hogy az adatok cseréjével előállt „fiktív" rekordok konzisztenciája ne sérüljön (pl. férfihoz ne tartozhasson abortusz esetszám).

– *Numerikus sorrendcsere*

Mikroadatok védelmére használt eljárás, melynek lényege, hogy **egy változó minden egyes rekordhoz tartozó értékét egy általunk meghatározott távolságon belül lévő másik rekordhoz tartozó értékével megcserélünk.** A módszer elvégzéséhez a numerikus változókat sorrendbe rendezzük és úgy végezzük el a cseréket, hogy a rekordok egymástól nem lehetnek nagyon „távol" a már meghatározott sorrendben.

[1] Handbook on Statistical Disclosure Control nyomán

Példa: A 4. táblázatban szereplő rekordokat alapterület szerint növekvő sorrendbe rendezzük és 30%-os intervallumon belül megcseréljük egy másik rekordértékkel.

- *Utólagos randomizálás (PRAM)*

Mikroadatok védelmére alkalmazott eljárás, melynek lényege, hogy **a mikroadat-állományban egy adott kategorikus változó által felvett minden egyes értéket előre meghatározott valószínűségnek megfelelően az adott változó egy másik értékére változtatunk.**

Példa: Egy adatállományban szereplő rekord (pl. férfi, Pécs, állatorvos, elvált) esetén 90% valószínűséggel a nem férfi marad, viszont 10% valószínűséggel nőre módosul. Az adatcseréhez hasonló módon itt is s fontos a végső rekord konzisztenciája!

- *Lokális elnyomás*

Mikroadatok védelmére alkalmazott eljárás, melynek lényege, **hogy egyes változók olyan értékeit, melyek bizonyos kulcsokra nézve nagyon kevés számú kombinációban fordulnak elő, kitöröljük**, annak érdekében, hogy az adott rekord felismerhetőségét megakadályozzuk.

Példa: Egy községben csak egy női fogorvos van, tehát a terület, nem és foglalkozás kulcs alacsony találatszámot eredményez. Megoldásnak választhatjuk, hogy a három változó értékének valamelyikét töröljük az állományból. Működését tekintve a módszer a táblázatos adatok esetében alkalmazott cellaelnyomás megoldáshoz hasonlít.

Önellenőrző kérdések

12. *Miért van kiemelt szerepe a statisztikai adatok kezelésének az adatkezelés rendszerében?*
13. *Melyek a statisztikai adatkezelés legfontosabb hazai és nemzetközi jogi keretei?*
14. *Mi a kapcsolat a statisztikai adatok védelme és az Európai Statisztika Gyakorlati Kódexe között?*
15. *Mi a különbség az azonosítás és a felfedés között?*
16. *Mit értünk táblázatos adat és mikroadat alatt?*
17. *Soroljon fel és mutasson be röviden táblázatos adatok felfedés elleni védelmére alkalmazható módszereket!*
18. *Mit értünk hármas szabály alatt? Miért fontos kiemelni, mint a küszöbszabály speciális esetét?*

19. *Mikor alkalmazunk másodlagos cellaelnyomást? Mi a másodlagos cellaelnyomás célja?*
20. *Mit értünk közvetlen azonosítás, közvetett azonosítás és kulcs alatt?*
21. *Soroljon fel és mutasson be röviden mikroadatok felfedés elleni védelmére alkalmazható módszereket!*

Irodalomjegyzék

4. *1993. évi XLVI. törvény a statisztikáról: http://www.complex.hu/kzldat/t9300046.htm/t9300046.htm*
5. *170/1993. (XII. 3.) Korm. rendelet a statisztikáról szóló 1993. évi XLVI. törvény végrehajtásáról: http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99300170.KOR*
6. *Európai Statisztika Gyakorlati Kódexe (2011-es, felülvizsgált változat): http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/10425-HU/HU/10425-HU-HU.PDF*
7. *Handepool, Anco et. al.: Handbook on Statistical Disclosure Control: http://neon.vb.cbs.nl/casc/.%5CSDC_Handbook.pdf*
8. *τ-Argus User's manual: http://neon.vb.cbs.nl/casc/Software/TauManualV3.5_rev.pdf*
9. *μ-Argus User's manual: http://neon.vb.cbs.nl/casc/Software/MuManual4.2.pdf*

Tartalomjegyzék