Az elszámoltathatóság alapelve és az adatkezelői kötelezettségek

Árvay Viktor György – Bíró János – Horuczi Szilvia – Majsa Ágnes – Szabó Endre Győző

A kiadvány a KÖFOP-2.1.1-VEKOP -15-2016-00001 „A közszolgáltatás komplex kompetencia, életpályaprogram és oktatás technológiai fejlesztése” című projekt keretében készült el és jelent meg.

Szerzők:

Dr. Árvay Viktor György
Dr. Bíró János
Dr. Horuczi Szilvia
Dr. Majsa Ágnes
Dr. Szabó Endre Győző

Szakmai lektor:

Dr. Péterfalvi Attila

Olvasószerkesztő:

Kiss Eszter

A kézirat lezárásának dátuma:

2018. szeptember 5.

Kiadja:

Felelős kiadó:

Prof. Dr. Kis Norbert
Dékán

TARTALOM

1. AZ ELSZÁMOLTATHATÓSÁG

1.1. Az elszámoltathatóság alapelve

A GDPR egyik fontos újdonsága, hogy az adatvédelmi szabályozásban központi helyre, alapelvi rangra emelte az elszámoltathatóság elvét. A GDPR 5. cikk (2) bekezdése értelmében az adatkezelő felelős az adatvédelmi alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság"). A Rendelet 24. cikke tovább részletezi az elszámoltathatóság kötelezettségét az adatkezelő feladatainál. Ennek megfelelően az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi. Ha az az adatkezelési tevékenység vonatkozásában arányos, ennek részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.

Az elszámoltathatóság elve egy általános szemléletmód váltást jelent az adatvédelmi szabályozásban. Bár az elszámoltathatóság maga nem új intézmény az adatvédelmi szabályozásban, hiszen eddig is az adatkezelő volt felelős az adatkezelés jogszerűségéért, de nem volt általános jelleggel arra kötelezve, hogy ezt a megfelelőségét bármikor felhívásra bizonyítani tudja. Korábban csak reaktív módon, a bírósági eljárás során terhelte az adatkezelés jogszerűségének bizonyítási terhe. Azzal azonban, hogy az elszámoltathatóság általános alapelvvé vált az adatkezelőnek proaktív módon, bármikor képesnek kell lennie arra, hogy az adatkezelése jogszerűségét bizonyítania tudja, illetve bármikor képesnek kell lennie arra, hogy a GDPR-ban nevesített adatkezelői kötelezettségek megvalósítását bizonyítsa.

Tehát az adatkezelőnek az adatkezelés megtervezésétől kezdve az adatkezelés megkezdésén át egészen a kezelt személyes adatok törléséig valamennyi adatkezelési műveletet úgy kell megvalósítani, hogy az adatkezelő bármelyik pillanatban bizonyítani tudja hogyan felelt meg az adatvédelmi előírásoknak.

Az elszámoltathatóság elve lényegében azt jelenti, hogy az adatkezelőknek mind a szervezeti kultúrájukat, mind valamennyi tevékenységüket az adatvédelemi megfontolásokra tekintettel kell kialakítaniuk, végezniük. Az adatkezelőknek minden egyes lépésüknél el kell gondolkodniuk, hogy az adatvédelmi előírásokat miként vették figyelembe.

A GDPR-ral, hiszen az az egész Európai Unióban közös adatvédelmi szabályokat alkot, az adatvédelem az adatkezelők számára olyan általános területté vált, mint az adómenedzsment, a számvitel vagy a humán erőforrás kezelése. Tekintettel az adatkezelés tág fogalmára, szinte elkerülhetetlen egy vállalkozás vagy egy szervezet számára, hogy személyes adatokat kezeljen, ezért az adatvédelem valamennyi cég vagy szervezet számára kiemelt jelentőségűvé vált.

Összefoglalva ez azt jelenti, hogy az adatkezelőnek az általános gyakorlata részévé kell tennie az adatvédelmi szabályok betartását és minden tevékenysége során figyelembe kell lennie arra, hogy az adott tevékenység mennyire felel meg az adatvédelmi előírásoknak, valamint ezt dokumentálnia kell, hogy szükség esetén a felügyeleti hatóság vagy az érintett kérésére bizonyíthassa, hogy az adatkezelés kialakítása és elvégzése során minden, a kockázatok alapján elvárható intézkedést megtett az adatvédelmi előírások megtartására, az érintetti jogok biztosítására. Az elszámoltathatóság követelménye valamennyi adatkezelői kötelezettség eredője.

Természetesen ezen az általános attitűdön túl a GDPR számos elvi és gyakorlati eszközzel is megpróbálja segíteni az elszámoltathatóság elvének érvényesülését. Ennek megfelelően az elszámoltathatóság követelményének teljesítését segíti elő többek között a beépített és alapértelmezett adatvédelem (25. cikk); az adatkezelési tevékenységek nyilvántartása (30. cikk); az adatvédelmi hatásvizsgálat (35. cikk); az adatvédelmi tisztviselő (37-39. cikk); a magatartási kódexek (40-41. cikk) és tanúsítás (42-43. cikk); illetve a kötelező erejű vállalati szabályok (47. cikk); stb.

Fontos emellett kiemelni, hogy az elszámoltathatóságnak nem csak a GDPR-ban szereplő eszközökkel lehet megfelelni. Számos olyan adatvédelmet elősegítő technika (Privacy Enhancing Tecnologies) létezik, amely nincs nevesítve a GDPR-ban, de segít az adatkezelőknek az adatvédelmi megfelelés kialakításában és igazolásában.

A fentiekből látszik, hogy az elszámoltathatóság alapelve az adatvédelemben mindent átható szabállyá vált. Valamennyi adatvédelmi szabályozás felfűzhető erre az alapelve, illetve máshonnan megközelítve valamennyi a GDPR-ba foglalt adatkezelői kötelezettséget az elszámoltathatóság szemszögéből kell megközelíteni.

Az előbb említettekből következően ez alapvetően három kötelezettséget ró az adatkezelőkre. Egyrészt folyamatosan figyelemmel kell kísérni a tevékenységeiket, hogy azok érintenek-e személyes adatokat. Másrészről, ha személyes adatokat kezelnek, akkor megfelelő intézkedéseket kell arra rendszeresíteniük, hogy az adatvédelmi megfelelést ellenőrizzék és naprakészen tartsák. Harmadrészről, dokumentálniuk kell az előbbieket.

Az elszámoltathatóság elvének egyik legfontosabb eleme a megfelelő dokumentáció fenntartása. Az adatkezelői kötelezettségek gyakorlati megvalósításában lehetnek eltérő megoldások és értelmezések, az viszont egyértelmű, hogy a saját megvalósítást vagy értelmezést megfelelően dokumentálni szükséges. Ezt egyrészről segítik a GDPR-ban nevesített nyilvántartási és egyéb dokumentálási kötelezettségek, mint például az adatkezelési műveletek nyilvántartása, az adatvédelmi incidensek nyilvántartása vagy az adatvédelmi hatásvizsgálat dokumentálása. Emellett azonban fontos az adatkezelőnek dokumentálnia, hogy miként felel meg az átláthatóság alapelvének, milyen adatkezelési tájékoztatókat készít, hogyan tájékoztatja például a honlapján az érintetteket az adatkezelésről, milyen belső adatkezelési szabályzatban hívja fel a munkavállalói figyelmét az adatvédelmi követelmények, különösen az átláthatóság és a megfelelő tájékoztatás követelményének a betartására. Dokumentálni szükséges az adatfeldolgozói szerződésnek az adatvédelmi kitételeit, mint ahogyan az adatátadásokkal, adattovábbításokkal kapcsolatos adatvédelmi garanciák szerződéses kikötéseit. Ugyancsak dokumentálni szükséges az érdekmérlegelési tesztek eredményeit. Ugyancsak a dokumentálási követelményekhez tartoznak a megfelelő belső szabályzatok elkészítése, amely a fent említetteken túl szólhatnak a megőrzési szabályokról, az informatikai biztonságról. Ugyancsak érdemes nyilvántartást vezetni az adatkezelőhöz érkezett érintetti megkeresések és az arra adott válaszok. Dokumentálni érdemes továbbá az adatkezelő belső adatvédelmi tréningjeit.

Ez a dokumentációs halmazt az adatkezelő egy belső irányítási rendszerbe szervezheti, amelyben áttekintheti és naprakészen nyomon követheti adatkezeléseit.

1.2. Az elszámoltathatóság alapelvének való megfelelést segítő, GDPR-ban nevesített és GDPR-on kívüli eszközei

A 3/2010. számú vélemény az elszámoltathatóság elvéről megfogalmazza az elv bevezetésének a célját: „az általános adatvédelmi elveket konkrét, az adatkezelő szintjén meghatározott politikákra és eljárásokra fordítaná le”. Ezzel az elv szintjéről az adatvédelem egy gyakorlatiasabb, életszerűbb irányba mozdulna el.

A Rendelet általánosságban rögzíti, hogy az „adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi”(24. cikk (1) bekezdés).

Ez a rendelkezés az adatkezelőtől egy folyamatos, naprakész tevékenységet követel, az elszámoltathatóság elve az adatkezelő szervezetét teljes egészében áthatja.

Az elszámoltathatóság elve kétirányú kötelezettség az adatkezelő részére: egyrészt az adatkezelő azon kötelezettségét jelenti, hogy megfelelő és hatékony intézkedéseket tegyen az adatvédelmi elvek végrehajtására, másrészt bizonyítani kell tudnia például a Hatóság kérésére, hogy megtette a megfelelő és hatékony intézkedéseket.

1.2.1. Az elszámoltathatóság alapelvének való megfelelést segítő GDPR-ban nevesített eszközök

Az alábbiakban 3 nagy csoportban kerültek összefoglalásra a Rendelet azon rendelkezései, amelyek az elszámoltathatóság elvének való megfelelést biztosítják:

1.1.1.1 Általános eszközök

5. cikkben található alapelvek:

- a jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Az átláthatóság az előzetes tájékoztatásról szóló ajánlásban szereplő formai követelmények érvényre juttatását jelenti.
- célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethető adatkezelésnek a közérdekű archiválás, a tudományos és történelmi kutatás és a statisztika készítése.
- adattakarékosság elve: a személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.
- pontosság elve: a személyes adatok(nak) pontosnak és ahol szükséges, naprakésznek kell lenniük.
- korlátozott tárolhatóság elve: személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. Hosszabb tárolás lehetséges a közérdekű archiválás, tudományos és történelmi kutatás, vagy statisztika készítés esetén.
- integritás és bizalmas jelleg elve (adatbiztonság): a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezeti intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Az elszámoltathatóság elve azon túl, hogy „szuper-elv”-ként említett, még „híd-elv”-ként is működik, a Rendelet alapelveit vezeti át a mindennapi gyakorlatba.

A Rendelet 24. cikkében meghatározott adatkezelői feladatok: megfelelő technikai és szervezési intézkedések végrehajtása

Ennél az adatkezelői kötelezettségnél meg kell említeni az adatvédelmi szabályzatok megalkotását és elfogadását is. Az adatvédelmi szabályzatnak tartalmaznia kell az összes adatkezelési folyamatot, az adatkezeléssel kapcsolatos szervezeten belüli feladatokat, pontosan meghatározva a kapcsolódó felelősségi köröket, az adatbiztonság érdekében tett intézkedéseket, az érintettek jogait és adatkezeléssel tett panaszok kezelését és annak módját.

Az adatkezelési tájékoztatók elkészítését is itt kell megemlíteni, amelyben az adatkezelő az adatkezeléssel kapcsolatos minden lényeges információt az érintett rendelkezésére bocsát, elősegítve ezzel az érintett adatkezeléssel kapcsolatos jogai gyakorlásának érvényesülését.

Az adatfeldolgozói szerződések megkötése is ennél a pontnál kerül részletezésre, tekintettel arra, hogy az adatkezelő érdeke is, hogy az adatfeldolgozói szerződés egyértelműen leszabályozza a felek közötti felelősségmegosztást az adatkezelés kapcsán. Az adatfeldolgozói szerződést köti az alakiság, írásban kell megkötni.

- A beépített és alapértelmezett adatvédelem (25. cikk)[1]

A beépített adatvédelem (Privacy by design) elve értelmében az adatvédelmet és az adatbiztonságot a tervezéskor kell beépíteni – például álnevesítés, titkosítás révén – az üzleti folyamatokba, műszaki termékekbe. Az adatkezelőnek figyelembe kell vennie a tudomány és a technológia állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira jelentett kockázatokat kell azonosítania és elemeznie. Ezek alapján tudja az adott szervezeten belül eldönteni, hogy adott adatkezelést miként lehet a beépített adatvédelem elvárásának kialakítani. Példaként említhető az álnevesítés (személyazonosításra alkalmas adatok mesterséges azonosítókkal való helyettesítése), valamint a titkosítás használata.

Az alapértelmezett adatvédelem (Privacy by default) elve arra ad biztosítékot, hogy csak olyan személyes adatok kezelésére kerüljön sor, amelyek az elérni kívánt cél szempontjából szükségesek. Ez az alapelv jelent mennyiségi korlátot, valamint garanciát arra, hogy az adatok kezelésének mértékére, tárolásuk időtartamára és a hozzáférhetőségre nézve is megfelelő intézkedéseket alkalmaz az adatkezelő. Példaként szolgálhat a közösségi oldalak felhasználói profilbeállítása, a magánszféra szempontjából leginkább kedvezőbb beállításnak kellene az alapértelmezett beállításnak lennie.

1.1.1.2 Speciális

Belső eljárások kialakítása az adatvédelmi incidens hatékony kezelése és jelentése céljából:

- Az adatkezelési tevékenységek nyilvántartása (30. cikk)[2]

Mind az adatkezelő, mind az adatfeldolgozó nyilvántartást kell, hogy vezessen az adatkezelési tevékenységéről, amely az adott adatkezelési tevékenység alapadatait tartalmazza. Az adatkezelői és adatfeldolgozói nyilvántartás természetesen eltérő tartalmú.

- Az adatvédelmi incidensek megfelelő kezelése (33-34. cikk)

A fejezetben írt incidensbejelentési kötelezettségen túl fontos megemlíteni az adatkezelő incidensnyilvántartását, ebben feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. Ennek segítségével lehetővé válik a felügyeleti hatóság számára, hogy ellenőrizze a Rendeletben előírt követelmények megtartását. Az adatkezelő részéről az adatvédelmi incidens hatékony kezelése és jelentése céljából belső eljárások kialakítása szükséges.

- Adatvédelmi hatásvizsgálat elvégzése (35. cikk)

Előzetes hatásvizsgálat szükséges az új adatkezelések megkezdését megelőzően, illetve a speciális körülményekre vonatkozóan is szükséges az adatvédelmi hatásvizsgálat elvégzése.

---

1 A beépített és alapértelmezett adatvédelemről a szakanyag 2. fejezetében olvashatnak részletesebben

2 Az adatkezelési tevékenységek nyilvántartásáról a szakanyag 4. fejezetében olvashatnak részletesebben

- Az adatvédelmi tisztviselő kijelölése (37. cikk)[3]

Az adatvédelmi tisztviselő az a személy az adatkezelő vagy adatfeldolgozó oldalán, aki ismeri az adatvédelemmel kapcsolatos szabályozásokat és gyakorlatot, és segíti az adatkezelő/adatfeldolgozó működését – a szervezeti működés függetlenségének garantálása mellett. Legfontosabb feladata, hogy ellenőrizze a Rendeletben foglaltak teljesülését egy szervezetnél. Fontosabb feladatkörei:

- tájékoztat és szakmai tanácsot ad,
- ellenőrzi az adatvédelmi rendelkezéseknek, illetve az adatkezelő vagy adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyek (munkavállalók) tudatosság-növelését és képzését, és az ehhez kapcsolatos belső auditokat is,
- kérésre szakmai tanácsot ad adatvédelmi hatásvizsgálatra vonatkozóan, nyomon követi annak elvégzését,
- együttműködik a felügyeleti hatósággal, valamint
- az adatkezeléssel összefüggő ügyekben kapcsolattartóként szerepel a felügyeleti hatóság felé, előzetes konzultációt, illetve bármilyen egyéb esetben az adott ügyben konzultációt folytat vele.

A Rendelet lehetőséget ad arra, hogy az adatkezelő vagy az adatfeldolgozó megbízza a tisztviselőt az adatvédelmi nyilvántartás vezetésével is.

A Rendelet 37. cikk (1) bekezdésében határozza meg azon esetköröket, amikor kötelező adatvédelmi tisztviselő kijelölése.

- Magatartási kódexhez való csatlakozás (40. cikk)

A Rendelet 40. cikke értelmében az adatkezelők (adatfeldolgozók) kategóriáit képviselő egyesületek és egyéb szervezetek magatartási kódexet dolgozhatnak ki annak érdekében, hogy a Rendelet alkalmazásában a különböző adatkezelők egyedi ágazati jellemzői, valamint a mikro-, kis- és középvállalkozások sajátos igényei, az adott iparági szempontok érvényesülni tudjanak. A Rendelet 40. cikk (2) bekezdésének a)-k) pontjai tartalmazzák a példálózó felsorolást arra vonatkozóan, hogy mely kérdések vonatkozásában pontosíthatja egy magatartási kódex a Rendelet alkalmazását. A felügyeleti hatóságok e folyamatban ösztönzőként vesznek részt, és ha a magatartási kódex megfelel a rendelet szabályainak, a magatartási kódexet jóváhagyják és nyilvántartásba veszik. A magatartási kódexnek olyan mechanizmusokat kell meghatározni, amelyek lehetővé teszik, hogy az erre akkreditált szervezet ellenőrizze, hogy a kódex alkalmazását vállaló adatkezelők vagy adatfeldolgozók megfelelnek-e a kódex rendelkezéseinek. A magatartási kódexnek való megfelelés ellenőrzését olyan szervezet végezheti, amely a kódex tárgya tekintetében megfelelő szakértelemmel rendelkezik, és amelyet az illetékes felügyeleti hatóság erre akkreditál.

- Jóváhagyott tanúsítási mechanizmusokhoz való csatlakozás (42. cikk)

A tanúsítás egy olyan eszköz, amelyet a Rendelet azért vezetett be, hogy segítséget nyújtson az adatkezelőknek abban, hogy a Rendeletnek való megfelelést biztosítsák és igazolják. A tanúsítás egy önkéntes eszköz, amelynek segítségével az adatkezelő igazolni tudja a felügyeleti hatóságok felé az adatkezelési gyakorlatának az adatvédelmi szabályoknak való megfelelését. A Rendelet alapján az átláthatóság és az elszámoltathatóság érdekében a felügyeleti hatóságoknak ösztönözniük kell olyan tanúsítási mechanizmusok, adatvédelmi bélyegzők, illetve jelölések létrehozását, amelyek bizonyítják, hogy az adatkezelő vagy adatfeldolgozó által végrehajtott adatkezelési műveletek megfelelnek a Rendelet előírásainak. A tanúsítás önmagában nem bizonyítja a megfelelést, azonban felhasználható a megfelelés bizonyításának részeként. A tanúsítás lehetővé teszi az érintettek számára is, hogy gyorsan értékelni tudják az adott termék vagy szolgáltatás adatvédelmi szintjét.

- A kötelező erejű vállalati szabályok alkalmazása adattovábbítás esetén (47. cikk)

A kötelező erejű vállalati szabályok (a továbbiakban: BCR) használata azt a célt szolgálja, hogy

[3] Az adatvédelmi tisztviselőről a szakanyag 6. fejezetében olvashatnak részletesebben.

a személyes adatoknak egy adott vállalatcsoport Európai Unióban letelepedett tagjai által, ugyanazon vállalatcsoport harmadik országban található tagjai részére történő továbbítása esetén megfelelő garanciákat nyújtson. A BCR tehát egy vállalatcsoport által létrehozott, kötelező szabályozásoknak olyan összessége, amelyet annak érdekében alkotnak meg, hogy a csoport tagjai közötti adattovábbítás során semmilyen esetben ne csökkenjen a védelmi szint – akkor sem, ha a fogadó szervezet harmadik országban találhatók –, illetve az így létrehozott garanciák kikényszeríthetőek legyenek mind a csoport tagjaitól, mind az érintettek részéről. A BCR-ok kidolgozásánál annak érdekében, hogy megfelelő garanciát nyújtson a személyes adatoknak vagy azok bizonyos kategóriáinak a továbbítására vonatkozóan, minden alapvető elvet és érvényesíthető jogot magába kell foglalnia.

1.1.1.3 Gyakorlati lépések/ GDPR-on kívüli eszközök:

- Belső, megfelelő adatvédelmi képzés és oktatás megszervezése a személyes adatokat kezelő munkavállalók számára, illetve feletteseik és a döntéshozók számára. Továbbá ki kell terjednie a személyes adatokat feldolgozókra, az IT menedzserekre, a fejlesztőkre és az üzleti egységek igazgatóira is.
- Privátszférát erősítő technológiák
- Audit
- ISO tanúsítványok
- Érintetti joggyakorlásra vonatkozó eljárások kidolgozása, amelyeknek átláthatónak kell lenniük az érintettek számára.

2. A BŰNÜLDÖZÉSI CÉLÚ ADATKEZELÉS ÁLTALÁNOS FELTÉTELEI

Az Infotv. néhány olyan általános előírást tartalmaz, amely a személyes adatok bűnügyi célú kezelésével kapcsolatban határoz meg adatvédelmi szabályokat. Ezek többsége a bűnügyi adatvédelmi irányelv átültetéséből származik és olyan specifikus követelményeket tartalmaz, amelyek vagy csak a bűnügyi célú adatkezelésre értelmezhetők, vagy csak a bűnügyi célú adatkezelések esetében alkalmazandók:

1. Bűnügyi személyes adatok kezelése esetén a különleges adatok kezelésének feltételeire vonatkozó szabályokat kell alkalmazni, ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusa ettől eltérően nem rendelkezik. (Infotv. 5. § (7) bekezdés) – E szabály nem a bűnügyi adatvédelmi irányelv átültetéséből származik, hanem a következők indokolják:
   - A GDPR 10. cikkéből következő követelmény, hogy a tagállami jognak a bűnügyi személyes adatok kezelésével összefüggésben az érintett jogai és szabadságai tekintetében megfelelő garanciákat kell biztosítania. A GDPR az elvárt garanciák mibenlétét nem határozza meg, ezért ezek a tagállami jogalkotó döntési kompetenciájába tartoznak. A magyar törvényhozó úgy döntött, hogy a különleges adatokra vonatkozó szigorúbb adatkezelési feltételrendszer vonatkozzék a bűnügyi személyes adatok kezelésére is.
   - A magyar jog már a GDPR alkalmazandóvá válása előtt felismerte, hogy a bűnügyi személyes adatok kezelése az általánosnál erősebb adatvédelmi garanciákat kíván meg, ezért már régóta a különleges adatokhoz sorolta a bűnügyi személyes adatot. A hatályos szabályozás arra irányul, hogy a bűnügyi személyes adatok korábbi védelmi szintje fennmaradjon.
   - Az Európa Tanács keretei között létrehozott adatvédelmi egyezmény 6. cikke is a különleges adatok körébe sorolja a bűnügyi személyes adatokat.

2. Az Infotv. 5. § (4) bekezdése szerint kizárólag állami vagy önkormányzati szerv kezelheti az állam bűncselekmények megelőzésére, felderítésére és üldözésére irányuló, valamint közigazgatási és igazságszolgáltatási feladatainak ellátása céljából kezelt bűnügyi személyes adatokat, valamint a szabálysértési, a polgári peres és nemperes ügyekre, valamint a közigazgatási peres és nemperes ügyekre vonatkozó adatokat tartalmazó nyilvántartásokat. A szabály a GDPR 10. cikkének való megfelelést szolgálja, amely szerint „a büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatoknak a 6. cikk (1) bekezdése alapján történő kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi. A büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak közhatalmi szerv által végzett adatkezelés keretében történhet".

3. Az Infotv. 7. § (1) bekezdése bűnüldözési célú adatkezelés esetén előírja a személyes adatok érintetti kategóriák szerinti rendszerezését (ha az aránytalan nehézséggel vagy költséggel nem jár) a következők szerint:

„a) akik tekintetében alapos okkal feltételezhető, hogy bűncselekményt vagy szabálysértést követtek el vagy bűncselekményt készülnek elkövetni,

b) akik büntetőjogi vagy szabálysértési felelősségét jogerősen megállapították,

c) akik bűncselekmény vagy szabálysértés sértettjei voltak, vagy akikről megalapozottan feltételezhető, hogy bűncselekmény vagy szabálysértés sértettjei lehetnek, vagy
d) akik az a)-c) pontban meghatározottakon túl bűncselekménnyel vagy szabálysértéssel, vagy azok elkövetőivel kapcsolatba hozhatóak, így különösen, akik a büntetőeljárás során tanúként meghallgathatóak, a bűncselekményről vagy a szabálysértésről információval szolgálhatnak, vagy az a) és b) pontban meghatározott érintettekkel kapcsolatban állnak vagy velük összefüggésbe hozhatóak."

Az Infotv. idézett szabályai a bűnügyi adatvédelmi irányelv 6. cikkét ültetik át, amely az érintettek különböző kategóriái közötti különbségtételről szól. Ennek fényében az Infotv. alkalmazása során nem az az elsődleges szempont, hogy a bűnügyi célból kezelt adatok a fent nevezett érintetti kategóriák szerint rendszerezve (például tehát sorba rakva vagy névmutatóval ellátva vagy adatbázisba szervezve stb.) legyenek, hanem az a minimális követelmény, hogy az iratokból kiderüljön az, hogy az egyes érintettek adatait milyen minőségükben (sértett, tanú, terhelt stb.) rögzítették.

4. Az Infotv. 7. § (2) bekezdése szerint bűnüldözési célú adatkezelés esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó – ha az aránytalan nehézséggel vagy költséggel nem jár – egyértelműen megkülönbözteti az érintettel kapcsolatba hozható tényeket és az érintettel kapcsolatba hozható szubjektív értékeléseket. – E szabály a bűnügyi adatvédelmi irányelv 7. cikk (1) bekezdését ülteti át. Érdemben nem hoz újdonságot, ugyanis némely, az Infotv. hatálya alá tartozó adatkezelést szabályozó szektorális törvények már eddig is tartalmaztak hasonló előírásokat:

- A Rendőrségről szóló 1994. évi XXXIV. törvény 91. §-a szerint a bűnüldözési adatkezelés során a tényeken alapuló adatokat meg kell különböztetni a következtetésen, véleményen, elemzésen vagy becslésen alapuló adatoktól. A bűnüldözési adatok különböző fajtáit helyes és megbízható voltuk mértékére utaló jelzéssel kell ellátni.
- A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 49. § (2) bekezdése szerint a nemzetbiztonsági szolgálatok kötelesek rendszeresen ellenőrizni az általuk kezelt személyes adatok helyességét. A valóságnak meg nem felelő adatokat helyesbíteni kell, az adatkezelés során a tényeken alapuló adatokat meg kell különböztetni a következtetésen, véleményen vagy becslésen alapuló adatoktól.

3. A BEÉPÍTETT ÉS ALAPÉRTELMEZETT ADATVÉDELEM

A GDPR 25. cikkében szereplő beépített és alapértelmezett adatvédelem alapján az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. Az adatkezelő továbbá megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

A (78) preambulum bekezdés tovább részletezi ezt az általános kötelezettséget, amikor kimondja, hogy a természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli az e rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az adatkezelő igazolni tudja az e rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit. Az említett intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat. Az olyan alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, amelyek személyes adatok kezelésén alapulnak vagy rendeltetésük teljesítéséhez személyes adatokat kezelnek, a termékek, szolgáltatások és alkalmazások előállítóit arra kell ösztönözni, hogy e termékek, szolgáltatások és alkalmazások kifejlesztésekor és tervezésekor szem előtt tartsák a személyes adatok védeleméhez való jogot, és a tudomány és technológia állását kellően figyelembe véve gondoskodjanak arról, hogy az adatkezelők és az adatfeldolgozók adatvédelmi kötelezettségeiknek eleget tegyenek. A beépített és az alapértelmezett adatvédelem elveit a közbeszerzések során is figyelembe kell venni.

Az adatkezelőnek tehát a beépített és alapértelmezett adatvédelem alapján egyrészről már az adatkezelés tervezésekor kötelezettsége figyelembe venni az adatvédelmi megfontolásokat, tehát ha egy adatkezelés során az adatkezelés folyamatába egy adatkezelési műveletet segítő vagy végrehajtó alkalmazást, szolgáltatást vagy terméket kiválasztanak, felhasználnak, kifejlesztenek, akkor figyelemmel kell lenniük arra, hogy az adott alkalmazás, szolgáltatás vagy termék mennyire felel meg az adatvédelmi előírásoknak. Másrészről az adatkezelés folyamatába olyan intézkedéseket, garanciákat kell beleépítenie, amely az adatvédelmi alapelveknek való megfelelést, illetve az érintetti

jogok gyakorlását elősegítik. Ezek az elvek nem újdonságok az adatvédelem területén, de a GDPR általános adatkezelői kötelezettség rangjára emeli, az adatkezelők általános kötelezettségévé teszi, hogy személyes adatok kezelése esetén az adatvédelem ne egy utólagosan alkalmazott elvárás, hanem inkább a tervezés és a megvalósítás központi eleme legyen.

A beépített és az alapértelmezett adatvédelem elvei tehát azt a kötelezettséget hárítják az adatkezelőre, hogy a tervezési fázistól kezdve az adatkezelés teljes életútján át az adatkezelési műveleteibe, illetve az üzleti gyakorlatába integrálja az adatvédelmi megfontolásokat.

A beépített és alapértelmezett adatvédelem alapján egy adatkezelő minden tevékenységét áthatja az adatvédelem, így ez a megközelítés tökéletesen illeszkedik az elszámoltathatóság alapelvéhez. Emellett a beépített és alapértelmezett adatvédelem elvét az adatvédelmi kockázatokra tekintettel kell alkalmazni, így az kapcsolódik a kockázat alapú megközelítéshez is.

Ha egy adatkezelő ezeket az elveket alkalmazza, akkor ellenőrzi alkalmazások, szolgáltatások és termékek kifejlesztésekor, tervezésekor, kiválasztásakor és felhasználásakor, illetve az üzleti gyakorlatában az adatvédelmi megfontolásokat figyelembe vette-e. Az adatvédelem az adatkezelő által alkalmazott rendszerek és szolgáltatások alapvető komponensét képezi-e. Az adatkezelő az adatvédelmi kockázatokat előzetesen feltérképezte-e és tervet készített-e azok megelőzésére, hatásainak a csökkentésére. Az adatkezelő az adatkezelési rendszereit úgy állította be, hogy csak az elengedhetetlenül szükséges adatokat kezelje és csak az előre meghatározott céloknak megfelelően. Az adatkezelési folyamatait kiszolgáló infrastruktúrában megtette azokat a lépéseket, hogy azok automatikusan védjék a feldolgozott személyes adatokat. Az ügyfélkapcsolat kialakítása során figyelembe vették az a szempontot, hogy az érintettek minél hamarabb elérhessék az adatkezelőt, illetve minél könnyebben gyakorolhassák érintetti jogaikat. Az ügyféltájékoztatásban a közérdekűségre törekszik az adatkezelő. Az érintetteknek biztosít a termékeiben, alkalmazásaiban, szolgáltatásaiban olyan eszközöket, amelyekkel jelezhetik, beállíthatják adatvédelmi preferenciáikat, gyakorolhatják adatvédelmi jogaikat. Továbbá ezekben az alapbeállítások a legadatvédelembarátabbak. Az adatkezelő csak olyan adatfeldolgozót vesz igénybe, amely megfelelő garanciát vállal az adatvédelmi előírások betartására, illetve maga is betartja a fent felsorolt elveket.

A beépített adatvédelem lényegében azt a megközelítést jelenti, hogy az adatkezelő bármely rendszer, szolgáltatás vagy termék kifejlesztése esetén a tervezés fázisától figyelembe veszi az adatvédelmi követelményeket és ezeket az előírásokat a rendszer, szolgáltatás és termék teljes életútján keresztül érvényesíti. Összegezve ez azt jelenti, hogy az adatvédelem bele van égetve az adott rendszerbe, szolgáltatásba, termékbe.

Az alapértelmezett adatvédelem az adatkezelés gyakorlati megvalósításánál az adatvédelmi követelmények tudatos kialakítását jelentik, elsősorban az adattakarékosság és célhoz kötött adatvédelem elvére tekintettel.

Ez olyan proaktív lépéseket jelenthet, mint például:

- az adatkezelő magánszférabarát alapértelmezett beállításokat alkalmaz;
- az adatkezelő a felhasználók számára az érintetti jogok gyakorlására megfelelő eszközöket biztosít;
- az adatkezelő átlátható felületen szemlélteti az érintett számára kivel osztja meg, kik férhetnek hozzá személyes adataihoz.

A beépített és alapértelmezett adatvédelem elveinek való megfelelésért, mint a legtöbb adatvédelmi előírás betartásáért, az adatkezelő felelős. Ugyanakkor szervezeten belül több terület is érintett lehet ezeknek az elveknek történő megfelelésért. A felső vezetésnek az adatvédelmi tudatosságot és kulturát kell növelniük, a szoftverfejlesztőknek a szoftver architektúra és a funkció specifikációk tervezése során kell az adatvédelmi megfontolásokra figyelemmel lenni. Az ügyfélkapcsolatokért felelős szervezeti egységnek olyan gyakorlatokat kell kialakítani, amelyek segíti az érintetti jogok gyakorlását, stb.

Ugyan a GDPR-ban nevesített beépített és alapértelmezett adatvédelem más jelentéstartalmat hordoz, mint a privacy by design, ugyanakkor az adatkezelőknek a GDPR szerint értelmezett beépített

adatvédelem során is érdemes kiindulni a Kanadában az 1990-es években kidolgozott a privacy by design hét alapelvéből.

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 magánszféra 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 magánszféra 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 profi 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
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.

4. A GDPR IV. FEJEZETÉNEK BEMUTATÁSA

A GDPR IV. fejezete, ahogy arra a címe is utal, az adatkezelő és az adatfeldolgozó egyes feladatairól, kötelezettségeiről szól, vagyis a célja, hogy meghatározza, hogy az adatkezelésben résztvevő szereplőknek milyen kötelezettségeknek kell eleget tennie, illetve milyen módon oszlik meg közöttük a felelősség. Emellett meghatároz néhány olyan eszközt is, amelyeknek alkalmazása nem kötelező, hanem csupán lehetőség az adatkezelő vagy adatfeldolgozó számára.

A fejezetben található kötelezettségeket, feladatokat tehát csoportosítani lehet aszerint, hogy azok:

- általános jelleggel, minden esetben kötelezőek (például a beépített és alapértelmezett adatvédelem elve; a kockázathoz mérten megfelelő technikai és szervezési intézkedések végrehajtása; az adatfeldolgozó igénybevételére vonatkozó kötelezettségek);
- meghatározott feltételek fennállása esetén kötelezőek (például adatvédelmi incidens bejelentése a felügyeleti hatóságnak; adatvédelmi hatásvizsgálat végzése; adatvédelmi tisztviselő kijelölése);
- önkéntesen alkalmazható eszközök, melyek felhasználhatók annak igazolása részeként, hogy az adatkezelés megfelel a GDPR előírásainak (ilyen eszköz a jóváhagyott magatartási kódex és a tanúsítási mechanizmus).

A második és a harmadik kategóriába tartozó kötelezettségekkel, feladatokkal, valamint eszközökkel kapcsolatban az ezeknek szentelt külön tananyagrészek tartalmaznak további részletes információkat.

5. AZ ADATKEZELŐ KÖTELEZETTSÉGEI

A GDPR IV. fejezetében arról rendelkezik, hogy egy adatkezelés vonatkozásában mi a szerepe az adatkezelőnek és az adatfeldolgozónak. Az adatkezelő elsődleges és általános kötelezettsége a GDPR által bevezetett, és a jogszabály egészét átható elszámoltathatóság elvének való megfelelés, vagyis az, hogy megfelelő és hatékony intézkedéseket hajtson végre, és képes legyen annak igazolására, hogy mind az adatkezelés, mind az alkalmazott intézkedések megfelelnek a GDPR-ban előírtaknak. Ez a fő kötelezettség tulajdonképpen magyarázza, pontosítja az elszámoltathatóság alapelvének tartalmát. Az adatkezelőnek minden adatkezelési tevékenység során szem előtt kell tartania az adatvédelmi szabályok betartását, és az ezeknek való megfelelést folyamatosan dokumentálnia kell, annak érdekében, hogy szükség esetén igazolni tudja azt, hogy az adatkezelést úgy alakította ki, és úgy is végezte a gyakorlatban, hogy a fennálló kockázatoknak megfelelő intézkedéseket hajtott végre az adatvédelmi szabályok betartása, és az érintetti jogok biztosítása érdekében.

5.1. Az adatkezelő meghatározása

Az érintettek jogainak és szabadságainak védelme, valamint az adatkezelők és az adatfeldolgozók hatásköre és felelőssége – a felügyeleti hatóságok általi ellenőrzéssel és azok intézkedéseivel összefüggésben is – megköveteli, hogy a GDPR szerinti kötelezettségek egyértelműen legyenek felosztva, ideértve azt az esetet is, amikor az adatkezelő más adatkezelőkkel közösen határozza meg az adatkezelés céljait és eszközeit, vagy amikor egy adatkezelő nevében végeznek adatkezelési műveletet.

Az adatkezelés fő szereplője az adatkezelő, aki az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Amennyiben az adatkezelés céljait és eszközeit uniós vagy tagállami jog határozza meg, az adatkezelő vagy az adatkezelő kijelölésére vonatkozó szempontokat ez a jogszabály is meghatározhatja.

Az adatkezelő ilyen módon történő meghatározásának célja, hogy a felelősséget ahhoz a szervhez telepítse, amelynél a tényleges befolyás, érdemi döntési kompetencia található, ezért annak meghatározása, hogy egy adott adatkezelés vonatkozásában ki minősül adatkezelőnek, inkább ténybeli és nem formális elemzésen alapul. Az adatkezelő fogalma arra szolgál, hogy meghatározható legyen, hogy ki felelős az adatvédelmi szabályok betartásáért, és hogy az érintettek milyen módon tudják a gyakorlatban jogaikat érvényesíteni. Ebből az is következik, hogy annak megállapítása, hogy egy adatkezelés vonatkozásában ki minősül adatkezelőnek, a körülmények alapos és hosszas vizsgálatát igényelheti.

Az adatkezelő fogalmának első alkotóeleme („természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv”) meghatározza a személyi kört, amely adatkezelő lehet. A definíció második alkotóeleme („személyes adatok kezelésének céljait és eszközeit meghatározza”) utal arra, hogy az tekinthető adatkezelőnek, aki ténylegesen eldöntötte, hogy adatkezelésre fog sor kerülni, és meghatározta annak a körülményeit, céljait és eszközeit. Az adatkezelői minőség tehát

általánosságban azon a ténybeli körülményen alapul, hogy egy természetes személy vagy szerv úgy döntött, hogy meghatározott célból személyes adatokat kezel. Ebből a szempontból az sem releváns, hogy az adott döntése jogszerű volt-e, vagyis hogy például rendelkezik-e az adatkezeléshez megfelelő jogalappal.

A GPDR megkülönböztet adatkezelőt és adatfeldolgozót, melynek célja, hogy az adatkezelésben résztvevő szereplők feladatai és felelőssége differenciált legyen. Amennyiben egy adatkezelés vonatkozásában minden szereplő megfelelően és jogszerűen jár el, akkor az adatkezelő és adatfeldolgozó szerepének elhatárolása feleslegesnek tűnhet. Azonban ennek az elhatárolásnak bizonyos esetekben kiemelt gyakorlati jelentősége is van: például egy adatvédelmi incidens bekövetkezése esetén nélkülözhetetlen az, hogy az adatkezelésben részt vevő szereplők meg tudják határozni azt, hogy melyikük minősül adatkezelőnek, és melyikük adatfeldolgozónak, mivel ez meghatározza az incidens vonatkozásában fennálló kötelezettségeiket is.

A gyakorlatban sok esetben azonban nem egyértelmű, hogy ki minősül adatkezelőnek és adatfeldolgozónak, ezért gyakran okozhat nehézséget a szerepek – és ezáltal a feladatok és a felelősség – meghatározása. Éppen ezért elengedhetetlen, hogy az adatkezelésben érintett szereplők, szervek már az adatkezelés megkezdése előtt meghatározzák a betöltött szerepüket, feladataikat, kötelezettségeiket és felelősségüket.

Ahogy már korábban is kifejtésre került, az adatkezelő határozza meg az adatkezelés céljait és eszközeit, vagyis teljes irányítással rendelkezik arra vonatkozóan, hogy miért és hogyan zajlik az adatkezelés.

Az adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel. Az adatkezelő léte tehát az adatkezelő döntésétől függ, amely dönthet úgy, hogy az adatokat a saját szervezetén belül dolgozza fel, vagy úgy, hogy az adatkezelési tevékenységek egy részét vagy egészét egy külső szervezetre ruházza át. Az adatfeldolgozói minőség alapvető feltétele tehát egyrészt az, hogy az adatfeldolgozó az adatkezelőtől elkülönülő jogi személyiséggel rendelkezzen, másrészt pedig az, hogy az adatkezelő nevében kezeljen személyes adatokat. Az adatfeldolgozó tevékenysége korlátozódhat egy pontosan meghatározott feladatra, műveletre, de lehet általánosabb, kiterjedtebb jellegű is. Fontos megjegyezni azt is, hogy ugyanaz a jogalany lehet egyidejűleg adatkezelő bizonyos adatkezelés vonatkozásában, illetve adatfeldolgozó más adatkezelésre vonatkozóan, az adatfeldolgozó szerepe ugyanis egy meghatározott esetben folytatott konkrét tevékenységéből fakad. Egy tárhelyszolgáltatást nyújtó internetszolgáltató elvileg adatfeldolgozó az ügyfelei által online közzétett személyes adatok vonatkozásában. Ha azonban az internetszolgáltató a saját céljaira tovább kezeli a weboldalon található adatokat, akkor erre a konkrét adatkezelésre vonatkozóan ő adatkezelő.

Az adatfeldolgozó meghatározásából eredő legfontosabb elem az, hogy az adatfeldolgozó az adatkezelő nevében jár el, kezel személyes adatokat, vagyis a tevékenysége az adatkezelő érdekeit szolgálja, amely a „hatáskörét" átruházza másik jogalanyra. Az adatfeldolgozó feladata tehát az, hogy végrehajtsa az adatkezelő utasításait. Így tehát az adatfeldolgozó tevékenységének jogszerűségét az adatkezelőtől kapott utasítás, „megbízás" határozza meg. Az adatkezelő bizonyos mérlegelési jogkört biztosíthat az adatfeldolgozó számára például azt illetően, hogy milyen módon szolgálja legjobban az adatkezelő által meghatározott célokat, és annak érdekében milyen technikai és szervezeti intézkedéseket hoz meg. Az adatfeldolgozó szerepét legegyszerűbben úgy lehet megfogalmazni, mint egy szakértelemmel bíró technikai partnere az adatkezelőnek, amelyet az adatkezelő egy konkrét, az adatkezelő által meghatározott célt szolgáló feladat elvégzésére bíz meg. Például egy vállalkozás arra bíz meg egy másik, szakértelemmel rendelkező vállalkozást, hogy direkt marketing kampányait lebonyolítsa, melynek során egyértelmű utasításokat ad arra vonatkozóan, hogy milyen marketing anyagokat küldjenek ki és kinek. Bár a vállalkozás rendelkezik bizonyos mérlegelési jogkörrel, például arra vonatkozóan, hogy milyen szoftvert használ, a feladatai egyértelműen meg vannak határozva.

Napjainkban egyre összetettebb a környezet, amelyben ezeket a fogalmakat használják, így például mind a magán-, mind a közszférában egyre jellemzőbb a szervezeti differenciálódás, amelynek módjai

– az információs és kommunikációs technológiák fejlődésével – új és nehezen megítélhető, komplex helyzeteket hozhatnak létre. Az adatkezelő és adatfeldolgozó fogalmának gyakorlati alkalmazása, elhatárolása ezért egyre bonyolultabbá válik.

Annak megítélése során, hogy egy adott szervezet, jogalany adatkezelőnek minősül-e figyelembe kell venni, hogy ki dönt az alábbiakról:

- az adatkezelés szükségességéről, jogalapjáról;
- arról, hogy milyen személyes adatok kezelésére kerül sor;
- az adatkezelés céljáról;
- arról, hogy mely érintettek vonatkozásában kerül sor az adatkezelésre;
- arról, hogy az adatokat közlik-e további személyekkel, szervezetekkel, és ha igen, melyekkel;
- az érintetti jogok gyakorlásának módjáról, és az érintetti joggyakorlás alóli kivételek esetleges alkalmazhatóságáról;
- az adatok megőrzési idejéről.

A fenti döntések mindegyike olyan, amelyeket csak az adatkezelő tud meghozni, mivel ő gyakorolja a tényleges irányítást, döntési kompetenciát az adatkezelés egésze felett.

A gyakorlatban a szervezetek adatkezeléssel kapcsolatos együttműködése során a szerepek inkább fokozatokra oszthatók. A legfontosabb annak meghatározása, hogy az egyes résztvevők milyen fokú önállósággal rendelkeznek az adatkezelés egyes körülményeire vonatkozóan, illetve, hogy a kezelt személyes adatok felett milyen fokú ellenőrzést gyakorolnak. Vannak olyan egyértelmű helyzetek, amikor az egyik fél meghatározza, hogy milyen személyes adatok kezelésére, milyen célból kerül sor, és részletes, pontos utasításokkal látja el a másik felet, amelyet az köteles követni, és amely meghatározza, hogy milyen műveleteket hajthat végre. Például az adatkezelő pontosan utasításokat ad arra vonatkozóan, hogy az adatokat milyen módon tárolja az adatfeldolgozó, így azt is meghatározza, hogy milyen szervert, milyen titkosítást és fizikai védelmet alkalmazzon. Az ilyen forgatókönyv esetén egyértelmű, hogy az utasításokat adó fél minősül adatkezelőnek, míg a másik adatfeldolgozónak. A gyakorlatban az ennyire egyértelmű helyzetek nagyon ritkán fordulnak elő. Ezzel szemben sokkal gyakoribb az, hogy az adatkezelő mérlegelési jogkört enged az adatfeldolgozó számára, hogy a rá bízott adatkezelési műveleteket a szakértelme alapján milyen módon hajtja végre. A leggyakoribb példa, amikor egy vállalkozás megbíz egy IT szakértelemmel rendelkező másik vállalkozást mint adatfeldolgozót, hogy például az általa kezelt adatok tárolását biztosítsa. Az ilyen esetekben – bár bizonyos mérlegelési jogköre van az adatfeldolgozónak például a technikai és szervezési intézkedések mibenlétére vonatkozóan –, annak figyelembe vételével kell a szerepeket meghatározni, hogy ki gyakorolja a tényleges ellenőrzést a személyes adatok felett (például ki jogosult arra, hogy az érintett törlésre irányuló kérelméről döntsön).

5.2. Közös adatkezelők

Ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőnek minősülnek.

Az ilyen közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban rögzítik a GDPR által előírt kötelezettségekre vonatkozóan – mint például az előzetes tájékoztatással és az érintetti jogok gyakorlásával kapcsolatos feladataikkal összefüggően – fennálló felelősségük megoszlását. Nincs szükség ilyen megállapodást kötni, ha az adatkezelésre vonatkozó felelősség megoszlását az alkalmazandó uniós vagy tagállami jog határozza meg. Az adatkezelőnek tehát már az adatkezelés megkezdését megelőzően fennálló kötelezettsége, hogy, amennyiben közös adatkezelésre kerül sor, vagyis az adatkezelés céljait és eszközeit több adatkezelő határozza meg, akkor egy megállapodásban

átlátható módon legyenek rögzítve az egyes adatkezelők hatáskörei és feladatai. Előfordulhat, hogy a közös adatkezelők között egyenlően oszlik meg a felelősség, mivel egyenlő módon vesznek részt az adatkezelés céljainak és eszközeinek meghatározásában. A megállapodásban azonban rögzíthetik azt is, hogy a felelősséget nem egyenlően osztják el, hanem minden adatkezelő meghatározott részben felel az adatkezelésért. A megállapodásnak tükröznie kell azt is, hogy az adatkezelők között milyen kapcsolat van: vannak olyan esetek, amikor nagyon szoros kapcsolat áll fenn (például az adatkezelés minden célját és eszközét közösen határozzák meg), de van olyan is, amikor lazább a kapcsolat közöttük (a célok és eszközök csak egy részét határozzák meg közösen).

Az érintettek védelme nem csökkenhet amiatt, hogy több adatkezelő közösen végzi az adott adatkezelést. A közös adatkezelők közötti megállapodásnak tükröznie kell az adatkezelők szerepét, vagyis egyértelműen tartalmaznia kell azt, hogy az érintettek felé melyik adatkezelőnek milyen szerepe van, illetve velük milyen kapcsolatban állnak. Ennek részeként a felek a megállapodásban kijelölhetnek kapcsolattartót az érintettek számára, így könnyítve meg jogaik gyakorlását. A megállapodás lényegét – összhangban az átláthatóság alapelvével – az érintettek rendelkezésére kell bocsátani, vagyis az adatkezelésről szóló tájékoztatásnak ki kell terjednie arra is, hogy amennyiben többes adatkezelés valósul meg, akkor melyik adatkezelőnek milyen feladatai, kötelezettségei vannak, és milyen módon oszlik meg a felek között a felelősség.

A GDPR emellett egyértelműsíti azt, hogy a közös adatkezelők közötti megállapodás tartalmától függetlenül, az érintett mindegyik adatkezelővel szemben gyakorolhatja a rendeletben foglalt jogait, ezáltal szintén biztosítva, hogy az érintetti jogok gyakorlását ne akadályozza az, hogy közös adatkezelés mellett döntöttek az adatkezelők.

5.3. Adatfeldolgozó megbízása

Egy ideális helyzetben az adatkezelő és az adatfeldolgozó kiléte is egyértelműen meghatározható, és a közöttük fennálló kommunikáció is zökkenőmentes. A valóságban azonban nem mindig ilyen egyértelmű helyzet áll fenn, melynek kezelésére, valamint az érintettek jogainak biztosítására, a GDPR igyekszik bizonyos megoldásokat adni azáltal, hogy az adatkezelő számára meghatározott kötelezettségeket ír elő arra az esetre, ha adatfeldolgozót kíván igénybe venni egy adatkezeléshez.

5.3.1. Az adatfeldolgozó kiválasztása

Annak biztosítása érdekében, hogy az adatfeldolgozó által az adatkezelő nevében elvégzendő adatkezelésre vonatkozóan teljesüljenek a GDPR-ban előírtak, az adatkezelőnek elsődleges kötelezettsége, hogy olyan adatfeldolgozót vegyen igénybe, amely megfelelő garanciákat nyújt – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy a GDPR követelményeinek teljesülését, és az érintettek jogainak védelmét biztosító technikai és szervezési intézkedéseket hajt végre. Az adatkezelő tehát köteles meggyőződni arról, hogy olyan adatfeldolgozót vesz igénybe, amely ezen követelményeknek megfelel.

Annak igazolására, hogy az adatfeldolgozó ilyen garanciákat biztosít, felhasználhatja azt, hogy jóváhagyott magatartási kódexhez vagy tanúsítási mechanizmushoz csatlakozott.

5.3.2. Az adatfeldolgozói szerződés

Az adatkezelő további kötelezettsége, ha adatfeldolgozót kíván megbízni, hogy az adatkezelés adatfeldolgozó általi elvégzését uniós vagy tagállami jog alapján létrejött szerződésben vagy egyéb jogi aktusban szabályozzák, amely köti az adatfeldolgozót az adatkezelővel szemben.

Az adatfeldolgozói szerződésnek meg kell határoznia az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait. Az ilyen szerződésnek legalább az alábbiakat kell előírnia:

- az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja. Ezt, a szerződésben is előírandó kötelezettséget egyébként a GDPR jogszabályi szinten is megerősíti.
- az adatfeldolgozó biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- az adatfeldolgozó meghozza az adatkezelés biztonsága érdekében előírt intézkedéseket;
- tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozó feltételeket:
  - » az adatfeldolgozó az adatkezelő előzetes írásbeli eseti vagy általános felhatalmazása nélkül nem vehet igénybe további adatfeldolgozót;
  - » általános felhatalmazás esetén tájékoztatja az adatkezelőt minden tervezett változásról, amely további adatfeldolgozók igénybevételét, vagy a meglévők cseréjét érinti, így biztosítva az adatkezelőnek, hogy kifogást emeljen a változásokkal szemben;
  - » további adatfeldolgozó igénybevétele esetén uniós vagy tagállami jog alapján létrejött szerződés vagy egyéb jogi aktus megkötésével kell biztosítania, hogy erre az adatfeldolgozóra is ugyanazok a kötelezettségek vonatkoznak, mint amelyek az adatkezelő és az adatfeldolgozó közötti szerződésben kikötésre kerültek;
  - » ha a további adatfeldolgozó nem teljesíti kötelezettségeit, akkor az őt megbízó adatfeldolgozó felel az adatkezelő felé.
- az adatfeldolgozó az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- az adatfeldolgozó segíti az adatkezelőt az adatvédelmi incidenssel, illetve az adatvédelmi hatásvizsgálattal kapcsolatos kötelezettségei teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő;
- az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely az adatfeldolgozó megbízásával kapcsolatban meghatározott kötelezettségek teljesítésének igazolásához szükséges, és amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott személy által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Bár az utasítások jogszerűségéért az adatkezelő felel, a GDPR előírja, hogy amennyiben úgy véli, hogy az adatkezelő valamely utasítása sérti a GDPR-t, vagy tagállami vagy uniós rendelkezéseket, akkor az adatfeldolgozónak haladéktalanul tájékoztatnia kell az adatkezelőt.

A GDPR alapján tehát adatfeldolgozói szerződést kell kötni, amennyiben egy adatkezelő adatfeldolgozót bíz meg, illetve, ha adatfeldolgozó további adatfeldolgozót vesz igénybe. A szerződés tartalmára vonatkozóan van számos a GDPR által előírt kötelező elem, a felsorolás azonban nem taxatív jellegű, az kiegészíthető további elemekkel. Az adatkezelő és az adatfeldolgozó eldöntheti, hogy egyedi szerződés vagy általános szerződési feltételek alkalmazása útján teljesíti a GDPR-ban előírtakat. A jogszabály ugyanis megteremti annak lehetőségét, hogy a Bizottság vagy a felügyeleti hatóságok (egységességi mechanizmus útján) meghatározzanak olyan általános szerződési feltételeket, amelyek tartalmazzák a GDPR-ban előírt elemeket, és melynek megkötése útján az adatkezelők és adatfeldolgozók eleget tehetnek azon kötelezettségüknek, hogy az adatkezelést szerződésben szabályozzák.

Az adatfeldolgozói szerződésre vonatkozó ilyen részletes szabályok újdonságot jelentenek az Infotv.-hez képest, amely csak arra vonatkozóan tartalmazott rendelkezést, hogy az adatfeldolgozásra irányuló szerződést írásba kell foglalni. A tartalmára vonatkozóan azonban nem írt elő további feltételeket, ezeket a NAIH gyakorlata alakította ki. Az adatfeldolgozói szerződés megkötésének kötelezettsége nagy jelentőséggel bír, mivel az biztosítja, hogy mind az adatkezelő, mind az adatfeldolgozó tisztában legyen a kötelezettségeivel és felelősségével. A szerződés emellett segíti is az adatkezelőket és adatfeldolgozókat a GDPR-nak való megfelelés biztosításában, és az érintettekben is növelheti a bizalmat.

5.4. Általános jellegű kötelezettségek

5.4.1. Megfelelő intézkedések megtétele

Ahogy az már korábban is kifejtésre került, az adatkezelő legalapvetőbb kötelezettsége az, hogy az elszámoltathatóság elvével összhangban, megfelelő és hatékony intézkedéseket hajtson végre, és képes legyen annak igazolására, hogy mind az adatkezelés, mind az alkalmazott intézkedések megfelelnek a GDPR-ban előírtaknak. Az adatkezelőnek tehát minden adatkezelési tevékenység során szem előtt kell tartania az adatvédelmi szabályok betartását, és dokumentálnia is kell az ezeknek való megfelelést.

A szükséges intézkedéseket az adatkezelőnek az adatkezelés jellege, hatóköre, körülményei és céljai, illetve a természetes személyek jogait és szabadságait érintő kockázatok figyelembevételével kell meghatároznia és végrehajtania. A GDPR tehát alkalmazza a kockázatközpontú megközelítést, amikor előírja, hogy az intézkedéseket az adatkezelőnek úgy kell meghoznia, hogy ahhoz figyelembe veszi az adatkezelés kockázatait. Tekintettel arra, hogy az adatkezelés kockázata kihatással van arra, hogy az adatkezelőnek milyen kötelezettségeknek kell eleget tenni (például az, hogy kell-e adatvédelmi hatásvizsgálatot végezni), illetve milyen intézkedéseket kell hoznia, ezért kiemelten fontos, hogy az adatkezelő már az adatkezelés tervezése során elemezze és meghatározza, hogy az milyen kockázatokkal jár a természetes személyek jogaira és szabadságaira nézve. A kockázatokat az adatkezelőnek objektív értékelés alapján kell felmérnie, melynek eredményeképpen megállapíthatja, hogy az adott adatkezelés kockázattal, illetve magas kockázattal jár-e.

Az alábbiak utalhatnak arra, hogy egy adatkezelés kockázatos:

- az adatkezelésből fizikai, vagyoni vagy nem vagyoni kár származhat, például, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, jó hírnév sérelme, szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, álnevesítés engedély nélküli feloldása, vagy bármilyen más jelentős gazdasági vagy szociális hátrány fakadhat;

- az érintettek nem gyakorolhatják az adatkezeléssel kapcsolatos jogaikat, vagy nem tudnak személyes adataik felett rendelkezni;
- az adatkezelés olyan személyes adatra vonatkozik, amely faji vagy etnikai származásra, politikai véleményre, vallási, világnézeti meggyőződésre, szakszervezeti tagságra utalhat, illetve sor kerül genetikai adatok, egészségügyi adatok, szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó intézkedésekre vonatkozó személyes adatok kezelésére;
- az adatkezelés személyes jellemzők értékelésére, például munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére, előrejelzésére irányul, profil létrehozása vagy felhasználása céljából;
- az adatkezelés kiszolgáltatott személyek, különösen gyermekek személyes adataira vonatkozik;
- az adatkezelés nagy mennyiségű személyes adatra, nagyszámú érintettre terjed ki.

A GDPR egészéről elmondható, hogy kockázatközpontú megközelítést alkalmaz, amely arra ösztönzi, kényszeríti az adatkezelőket és adatfeldolgozókat, hogy az adatkezelés megkezdését megelőzően végezzenek el egy kockázatelemzést, és ehhez mérten állapítsák meg, hogy mely intézkedések a megfelelőek. A kockázat fogalma számos adatkezelői és adatfeldolgozói kötelezettséggel összefüggésben is megjelenik, azok konkrét tartalmára is kihatással van, ezért kiemelkedő jelentőséggel bír.

5.4.2. A beépített és alapértelmezett adatvédelem elve

Ezt az alapelvi jellegűnek is tekinthető kötelezettséget a GDPR IV. fejezete tartalmazza, ezáltal az adatkezelő egyik alapvető kötelezettségévé teszi. Az elv lényege, hogy az adatkezelőnek alapvető kötelezettsége az, hogy már az adatkezelés tervezése során figyelembe kell vennie az adatvédelmi megfontolásokat, előírásokat, és az adatkezelés folyamatába eredendően be kell építenie olyan garanciákat, amelyek elősegítik az adatvédelmi szabályoknak való megfelelést, illetve az érintettek jogainak biztosítását.

5.4.3. Az unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó képviselője

Amennyiben az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett adatkezelésre, a területi hatályra vonatkozó rendelkezések értelmében alkalmazni kell a GDPR-t, akkor az adatkezelőnek vagy adatfeldolgozónak írásban ki kell jelölnie egy uniós képviselőt.

Ha tehát az Unióban tartózkodó érintettek személyes adatait az Unióban tevékenységi hellyel nem rendelkező olyan adatkezelő vagy adatfeldolgozó kezeli, amelynek az adatkezelési tevékenysége termékeknek vagy szolgáltatásoknak az ilyen érintettek számára történő Unión belüli kínálásához, vagy az ilyen érintettek Unión belüli magatartásának a megfigyeléséhez kapcsolódik, akkor annak érdekében, hogy mind a felügyeleti hatóság, mind az érintettek számára legyen az ilyen harmadik országban letelepedett adatkezelőnek vagy adatfeldolgozónak egy Unióban található kapcsolattartója, ki kell jelölni egy képviselőt.

A képviselő az az Unióban tevékenységi hellyel vagy lakóhellyel rendelkező természetes vagy jogi személy, akit, vagy amelyet az adatkezelő vagy adatfeldolgozó jelölt meg írásban, és aki, vagy amely az adatkezelőt képviseli a GDPR alapján rá háruló kötelezettségek vonatkozásában.

A képviselőnek tevékenységi hellyel kell rendelkeznie az egyik olyan tagállamban, ahol azon érintettek tartózkodnak, akiknek személyes adatait kezelik. A képviselő az adatkezelő vagy az adatfeldolgozó nevében jár el, és e minőségében bármelyik felügyeleti hatóság megkeresheti. Az adatkezelő vagy az adatfeldolgozó írásbeli megbízás útján jelöli ki a képviselőt, amelyben rendezni kell a képviselő és az adatkezelő vagy adatfeldolgozó kötelezettségeit, egymáshoz való viszonyát. A képviselő a feladatait az adatkezelőtől vagy az adatfeldolgozótól kapott megbízással összhangban látja el. Az írásbeli megbízásban a harmadik országban letelepedett adatkezelő vagy adatfeldolgozó kifejezetten kijelöli a képviselőt arra, hogy nevében a GDPR értelmében fennálló kötelezettségei tekintetében eljárjon. A képviselő kijelölése nem érinti az adatkezelőre, illetve adatfeldolgozóra háruló kötelezettségeket és felelősséget. Az adatkezelő vagy adatfeldolgozó meg nem felelése esetén, a kijelölt képviselővel szemben az adatkezelő vagy a felügyeleti hatóság kikényszerítési eljárásokat indíthat.

Nem minden esetben kötelező ilyen képviselő kijelölése, a GDPR meghatároz kivételeket, amikor a főszabálytól megengedett az eltérés. Nem kell tehát képviselőt kijelölni, ha:

- az adatkezelés alkalmi jellegű, amely nem terjed ki sem a személyes adatok különleges kategóriáira, sem a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelésére, és amely valószínűsíthetően nem jelent kockázatot a természetes személyek jogaira és szabadságaira nézve; vagy
- az adatkezelést közhatalmi vagy egyéb, közfeladatot ellátó szerv végzi.

Az első kivétel esetén a három feltételnek egyszerre kell teljesülnie, vagyis az adatkezelés alkalmi jellegű, ami nem terjed ki különleges adatokra vagy bűnügyi személyes adatokra, és az adatkezelés nem jelent kockázatot a természetes személyek jogaira és szabadságaira nézve. A kockázatok elemzése során itt is irányadóak a korábban kifejtettek (2.4.1. pontban), annak során figyelembe kell venni az adatkezelés jellegét, körülményeit, hatókörét és céljait.

5.4.4. Együttműködés a felügyeleti hatósággal

A GDPR szintén általános kötelezettségként írja elő, hogy az adatkezelő és az adatfeldolgozó, illetve – ha van ilyen – képviselőjük, feladataik végrehajtása során együttműködnek a felügyeleti hatósággal, annak megkeresése alapján. Ez az általános kötelezettség több helyen megjelenik a GDPR-ban speciális kötelezettségként is, például amikor előírja, hogy az adatkezelési tevékenységekről vezetett nyilvántartást az adatkezelő vagy adatfeldolgozó megkeresés alapján köteles a felügyeleti hatóság rendelkezésére bocsátani.

Azt, hogy a felügyeleti hatóság megkeresésére milyen formában és módon, milyen eljárási szabályok mellett kerülhet sor, az adott tagállamban irányadó nemzeti jog fekteti le, vagyis a NAIH eljárására vonatkozóan az Infotv. és az Ákr. Míg a GDPR egyéb konkrét, az együttműködésre irányuló kötelezettségek elmulasztásához szankciót is párosít, ez az általános, a GDPR egészét átható kötelezettség önmagában nem kikényszeríthető a GDPR alapján.

5.5. Adatkezelési tevékenységek nyilvántartása

További általános kötelezettségként írja elő a GDPR, hogy az adatkezelőnek, felelősségébe tartozóan végzett adatkezelési tevékenységekről, az adatfeldolgozónak pedig az adatkezelő nevében végzett adatkezelési tevékenységek kategóriájáról nyilvántartást kell vezetnie. Ez is egy általános jellegű kötelezettség, amely csak a GDPR-ban meghatározott kivételek fennállása esetén nem áll fenn.

A Rendelet 30. cikke szerint mind az adatkezelő, mind az adatfeldolgozó kötelesek nyilvántartást vezetni az adatkezelési tevékenységeikről.

Az adatvédelmi tevékenységek nyilvántartása hasznos eszköz a meglévő, valamint a tervezett adatkezelési tevékenységek következményeinek elemzéséhez. Segítséget nyújt az adatkezelőnek tényszerűen megállapítani, hogy az adatkezelő vagy adatfeldolgozó adatkezelési tevékenysége kockázattal jár-e az érintett jogaira vagy szabadságaira nézve, illetve segít azonosítani és végrehajtani a személyes adatok védelmét biztosító intézkedéseket. Az előbb írtak is mutatják, hogy az adatkezelési tevékenységek nyilvántartása az átláthatóság és az elszámoltathatóság elvének egyik eleme. A 29. cikk szerinti Munkacsoport (a továbbiakban: Adatvédelmi Munkacsoport) 2016. december 13-án kiadott, és 2017. április 5-én felülvizsgált „Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban" kimondja: „Ezeket a nyilvántartásokat az egyik olyan eszköznek kell tekinteni, ami lehetővé teszi az adatvédelmi tisztviselő számára, hogy teljesítse a megfelelés ellenőrzését, a tájékoztatást és az adatkezelő vagy az adatfeldolgozó részére végzett tanácsadást", továbbá „a 30. cikk értelmében előírt nyilvántartások olyan eszközként is kell tekinteni, amely lehetővé teszi az adatkezelő és – kérésére – a felügyeleti hatóság számára, hogy áttekintést kapjon a személyes adatok kezelésével kapcsolatban a szervezet által végzett valamennyi tevékenységről. Ezért ez a megfelelés előfeltétele, és mint ilyen, hatékony elszámoltathatósági eszköz."

A 30. cikk (1) bekezdése felsorolja az adatkezelők által vezetendő nyilvántartás kötelező tartalmi elemeit:

- az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- az adatkezelés céljai (néhány jellemző cél: például munkaviszonnyal kapcsolatban kezelt munkavállalói adatok; munkahelyi kamerarendszer (CCTV) üzemeltetése; az email/laptop/Internet munkavállaló általi használatának ellenőrzése; munkáltatói visszaélés-jelentéstételi rendszer; nyereményjáték szervezése; direkt marketing; ügyféladatok kezelése; webshop működtetése; követeléskezelő társaság igénybe vétele stb.);
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;
- olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- a különböző adatkategóriák törlésére előirányzott határidő;
- az adatbiztonság fenntartása érdekében tett technikai és szervezési intézkedések általános leírása (például az adatokhoz hozzáféréssel rendelkezők megnevezése, az alkalmazott IT biztonsági szint).

A 30. cikk (2) bekezdése pedig megnevezi az adatfeldolgozók által vezetendő nyilvántartás kötelező tartalmi elemeit:

- az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
- az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;
- adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítása, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a megfelelő garanciák leírása;
- az adatbiztonság fenntartása érdekében tett technikai és szervezési intézkedések általános leírása (például az adatokhoz hozzáféréssel rendelkezők megnevezése; az alkalmazott IT biztonsági szint stb).

A nyilvántartás elektronikus formában történő elkészítése eleget tesz a követelményeknek, amely a gyakorlatban például Excel táblázatba foglalt adatkezelési tevékenységek felsorolását tartalmazza a Rendeletben felsorolt információkkal. Az adatkezelési tevékenységek nyilvántartását naprakészen kell tartani, az adatkezelési tevékenység tekintetében történő változásokat át kell vezetni az adatkezelési tevékenységek nyilvántartásán.

Az Adatvédelmi Munkacsoport állásfoglalást bocsátott ki a Rendelet 30. cikk (5) bekezdésében foglalt adatkezelési tevékenységekre vonatkozó nyilvántartási kötelezettségektől való eltérésekről. A Rendelet (13) preambulumbekezdésének értelmében „A mikro-, kis- és középvállalkozások sajátos helyzetének figyelembevétele érdekében a 250 főnél kevesebb személyt foglalkoztató szervezetek esetében a Rendelet a nyilvántartás vezetése tekintetében eltérést tartalmaz.” Az idézett (13) preambulumbekezdést a 30. cikk (5) bekezdése juttatja érvényre. E szerint „a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriának vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére”. Az Adatvédelmi Munkacsoport állásfoglalása ugyanakkor kiemeli, hogy az idézett bekezdés által biztosított eltérés nem abszolút. Nem vonatkozik a következő 3 adatkezelési típusra:

- az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal járó adatkezelés;
- nem alkalmi jellegű adatkezelés;
- a különleges kategóriákra vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatokra kiterjedő adatkezelés.

Az Adatvédelmi Munkacsoport hangsúlyozza, hogy az előbb felsorolt adatkezelési típusok, amelyek esetében az eltérés nem alkalmazható vagylagosak: ha valamelyikük egymagában fennáll, előidézi az adatkezelési tevékenységre vonatkozó nyilvántartási kötelezettséget.

Ugyanakkor az ilyen szervezeteknek csak a 30. cikk (5) bekezdésében említett adatkezelési típusokról kell nyilvántartást vezetniük.

5.6. Az adatkezelői és az adatfeldolgozói nyilvántartás és az elektronikus napló

5.6.1. Az adatkezelői és az adatfeldolgozói nyilvántartás

Az adatkezelői és az adatfeldolgozói nyilvántartás szabályait az Infotv. 25/E. §-a tartalmazza. E szabályok a nyilvántartások rendeltetését, adattartalmát, valamint vezetésük és felhasználásuk szabályait illetően hasonlítanak a GDPR adatkezelési tevékenységek nyilvántartására vonatkozó joganyagára (l. a GDPR 30. cikkét).

Az adatkezelői nyilvántartás adatkörének eltérései a következők:

1. Az Infotv. 25/E. § (1) bekezdése néhány olyan, az adatkezelésre vonatkozó paraméter adatkezelői nyilvántartásba vételét is előírja, amelyet a GDPR 30. cikk (1) bekezdés a) – g) pontjai nem. Ezek a következők:

e) pont: profilalkotás alkalmazása esetén annak ténye,

f) pont: nemzetközi adattovábbítás esetén a továbbított adatok köre,

g) az adatkezelési műveletek – ideértve az adattovábbítást is – jogalapjai.

2. A 25/E. § (1) bekezdés j) pontja szerint az adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és a kezelésükre tett intézkedéseket is az adatkezelői nyilvántartásban kell rögzíteni. (A GDPR 33. cikk (5) bekezdése külön nyilvántartásként utal ugyanerre az adatkörre.)

3. A 25/E. § (1) bekezdés k) pontja az érintett hozzáférési jogának érvényesítését korlátozó vagy megtagadó intézkedésének jogi és ténybeli indokait is rögzíteni rendeli az adatkezelői nyilvántartásban.

Az adatfeldolgozói nyilvántartás adatköre azonos az Infotv.-ben és a GDPR-ban. (L. az Infotv. 25/E. § (2) bekezdését, ill. a GDPR 30. cikk (2) bekezdését.)

Az Infotv. – a GDPR-tól eltérően – feltételesen sem ad felmentést a nevezett nyilvántartások vezetése alól a 250 főnél kevesebb személyt foglalkoztató szervezetek számára. Ezt az indokolja, hogy a bűnügyi, honvédelmi és nemzetbiztonsági célból végzett adatkezelések dokumentáltságához és elszámoltathatóságához olyan közérdek fűződik, amely az adatkezelést végző szerv személyi állományának létszámától függetlenül szükségessé teszi a nyilvántartások vezetését.

5.6.2. Elektronikus napló

Az Infotv. 25/F. § tartalmazza az elektronikus napló vezetésének kötelezettségét. Ez egy olyan nyilvántartás, amely a korábbi adatvédelmi szabályozás által előírt adattovábbítási nyilvántartáshoz hasonló, de nemcsak az adattovábbításokra, hanem az adatokkal végzett más műveletekre is kiterjed, ám célja ugyanaz: az adatkezelés jogszerűségének ellenőrizhetőségéhez szükséges adatok megőrzése. Az elektronikus napló adatai kizárólag az adatkezelés jogszerűségének ellenőrzése, az adatbiztonsági követelmények érvényesítése, továbbá büntetőeljárás lefolytatása céljából ismerhetőek meg és használhatóak fel. Az adatkezelő, illetve az adatfeldolgozó a következő adatokat rögzíti az elektronikus naplóban az egyes adatkezelési műveletekről:

a) az érintett személyes adatok köre,
b) az adatkezelési művelet célja és indoka,
c) az adatkezelési művelet elvégzésének pontos ideje,
d) az adatkezelési műveletet végrehajtó személy megjelölése,
e) adattovábbítás esetén annak címzettje.

Az Infotv. az elektronikus úton vezetett adatkezelések esetében írja elő az elektronikus napló vezetését, amelyet automatizált rendszerben kell végezni. Ha tehát az adatkezelés nem elektronikus, hanem manuális úton történik (l. például a kartoték-nyilvántartásokat, illetve az adatok ügyiratokban történő gyűjtését), akkor az elektronikus napló vezetésére vonatkozó szabályokat nem kell alkalmazni.

5.6.3. Az adatkezelői és az adatfeldolgozói nyilvántartás és az elektronikus napló vezetésének közös szabályai

Az adatkezelői és az adatfeldolgozói nyilvántartás és az elektronikus napló vezetésének módját akként célszerű kialakítani, hogy a bejegyzések tényét, idejét és tartalmát utóbb is hitelesen igazolni lehessen. Ez többféleképp megvalósítható, például az elektronikus bejegyzések legalább fokozott biztonságú elektronikus aláírással és időbélyeggel történő ellátásával, vagy zárt és szigorúan ellenőrzött adatkezelési rendszer kialakításával, továbbá rendszeres archiválással stb.

A nemzetbiztonsági célú adatkezelést végző szervek az adatkezelői nyilvántartás és az elektronikus napló vezetésére irányuló kötelezettséget a nemzetbiztonsági szolgálatokról szóló törvényben meghatározott nyilvántartási és dokumentációs kötelezettségek útján is teljesíthetik.

Az adatkezelői és az adatfeldolgozói nyilvántartásban, valamint az elektronikus naplóban rögzített adatokat a kezelt adat törlését követő tíz évig kell megőrizni.

5.7. Egyéb adatkezelői kötelezettségek általános ismertetése (adatvédelmi incidens bejelentése, adatvédelmi hatásvizsgálat)

5.7.1. Az adatvédelmi incidens bejelentése

A Rendelet 4. cikk 12. pontja értelmében adatvédelmi incidens „a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi".

A biztonság sérülése következtében az adatkezelő nem lesz képes biztosítani a személyes adatok kezelésére vonatkozó elveknek való megfelelést. Ebből eredően valamennyi adatvédelmi incidens biztonsági incidens, viszont nem minden biztonsági incidens minősül szükségszerűen adatvédelmi incidensnek.

Az Adatvédelmi Munkacsoport adatvédelmi incidens bejelentésről szóló WP 250. számú iránymutatása (a továbbiakban: WP 250. számú iránymutatás) az adatvédelmi incidenseket a következő három klasszikus biztonsági kritériumon keresztül kategorizálja:

- „Bizalmas jelleg sérülése", ami a személyes adatok jogosulatlan vagy véletlen közzétételének vagy az ezekhez való hozzáférésnek felel meg;
- „Integritás sérülése" alatt a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítását értjük;
- „Rendelkezésre állás sérülése", mely a személyes adatok véletlen vagy jogosulatlan megsemmisítésének vagy a személyes adatok elvesztésének felel meg.

Az adatvédelmi incidensek fent írt kategóriái esetében előfordulhat olyan adatvédelmi incidens bekövetkezése is, amely két- vagy akár mindhárom kategória alá is besorolható, és míg a „bizalmas jelleg sérülése" és az „integritás sérülése" viszonylag könnyen megfoghatóak, addig a „rendelkezésre állás sérülésének" azonosítása nem minden esetben olyan nyilvánvaló.

Az adatkezelőt terhelő bejelentési kötelezettség vonatkozásában a Rendelet 33. cikk § (1) bekezdése úgy rendelkezik, hogy „az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is".

Az adatvédelmi incidenshez kapcsolódó adatkezelői kötelezettségek elmulasztása esetén alkalmazható szankciók tekintetében a Rendelet (87) preambulumbekezdése úgy fogalmaz, hogy „meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. A felügyeleti hatóságnak történt bejelentést az e rendeletben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti". Abban az esetben, ha az adatkezelő elmulasztja teljesíteni bejelentési, vagy tájékoztatási kötelezettségét, a felügyeleti hatóságot megilleti a választás lehetősége a rendelkezésére álló korrekciós hatáskörei gyakorlása közül, amibe beletartozik a körülményeknek megfelelő közigazgatási bírság kivetése, továbbá a Rendelet 58. cikk (2) bekezdése szerinti korrekciós hatáskörében megtehető egyéb intézkedés alkalmazása vagy annak mellőzése. Közigazgatási bírság alkalmazása esetén a kiszabható legmagasabb bírság 10 000 000 EUR, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeg. A szankciók alkalmazása szempontjából

kiemelést érdemel az a tény, hogy amennyiben az adatkezelő elmulasztja bejelenteni az adatvédelmi incidenst, az felszínre hozhatja biztonsági intézkedések hiányosságait, vagy esetlegesen azok teljes hiányát is. Ebben az esetben a felügyeleti hatóságnak lehetősége van jogkövetkezményeket alkalmazni mind a bejelentés, illetve a tájékoztatás elmulasztásáért (Rendelet 33. cikk, 34. cikk.), mind pedig a megfelelő biztonsági intézkedések elmaradásáért (Rendelet 32. cikk), mint teljesen különálló jogsértésekért.

A tudomásszerzés időpontjával kapcsolatban az Adatvédelmi Munkacsoport WP 250. számú iránymutatásában úgy foglalt állást, hogy a tudomásszerzés időpontja az az időpont, amikor az adatkezelő ésszerű mértékben bizonyossággal bír afelől, hogy olyan biztonsági sérülés következett be, mely személyes adatok megsértéséhez vezetett. Ez függ a konkrét incidens körülményeitől, és egyes esetekben már kezdettől fogva egyértelmű, hogy adatvédelmi incidens következett be, míg más esetekben hosszabb időt vehet igénybe ennek megállapítása.

Annak érdekében, hogy az adatkezelő képes legyen adatvédelmi incidensekkel felmerülő feladatainak teljesítésére, belső eljárásrendet kell kidolgoznia az adatvédelmi incidensek feltárása és kezelése céljából.

Az adatvédelmi incidens bejelentés tartalmi elemei tekintetében a Rendelet 33. cikk (3) bekezdése értelmében adatvédelmi incidens bekövetkezése esetén az adatkezelőnek az incidensbejelentés során ismertetnie kell a Hatósággal minimálisan az adatvédelmi incidens jellegét, az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát. A fentieken túlmenően közölnie kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, az adatvédelmi incidensből eredő, valószínűsíthető következményeket, valamint az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket. Az adatkezelőnek lehetősége van a szakaszos bejelentésre is, abban az esetben, ha nem lehetséges az információkat egyidejűleg közölni.

Habár a Rendelet bevezeti az adatvédelmi incidens bejelentési kötelezettséget, azonban ez nem minden esetben követelmény, az adatkezelőnek abban az esetben kell bejelentenie a felügyeleti hatóság irányában az adatvédelmi incidenst, amennyiben az valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

A NAIH a Rendelet 33. cikkének (3) bekezdésében található, az adatvédelmi incidens bejelentésének minimális tartalmi elemeire tekintettel, elkészített egy egységes online felületet, a NAIH Incidensbejelentő Rendszert, a bejelentési kötelezettség elektronikus úton történő teljesítése céljából. Azon adatkezelők számára, akik papír alapon kívánják adatvédelmi incidens bejelentésüket megtenni, a NAIH bejelentésre szolgáló formanyomtatványt biztosít.

5.7.1.1. Adatvédelmi incidensek bejelentése az Infotv-ben

Az Infotv.-ben a 25/J. § és a 25/K. § tartalmazza az adatvédelmi incidensekhez kapcsolódó szabályokat, valamint a 3. § 26. pontja az adatvédelmi incidensre vonatkozó értelmező rendelkezést . Az adatvédelmi incidensek Infotv. szerinti joganyaga a jogintézmény célját, az adatkezelő és az adatfeldolgozó feladatait, valamint az adatvédelmi incidens bejelentésének eljárásrendjét illetően nagyrészt párhuzamos szabályokat tartalmaz a GDPR 33-34. cikkeiben, valamint a vonatkozó preambulumbekezdéseiben foglaltakkal. Az ezekről leírtakat nem szükséges itt megismételni. Ezen túl az Infotv. olyan kiegészítéseket és kivételeket tartalmaz, amelyek az adatkezelés kiemelten közérdekű céljaira (bűnüldözés, honvédelem, nemzetbiztonság), valamint titokvédelmi szempontokra tekintettel a szükséges mértékben módosítják az adatvédelmi incidensekkel kapcsolatos teendők ellátásának eljárásrendjét:

1. Törvény előírhatja, hogy az adatkezelő az érintett adatvédelmi incidensről történő tájékoztatását az elérni kívánt céllal arányosan késleltethesse, korlátozhassa vagy mellőzhesse, ha ez elengedhetetlenül szükséges

a) az általa vagy részvételével végzett vizsgálatok vagy eljárások – így különösen a büntetőeljárás – hatékony és eredményes lefolytatásának,
b) a bűncselekmények hatékony és eredményes megelőzésének és felderítésének,
c) a bűncselekmények elkövetőivel szemben alkalmazott büntetések és intézkedések végrehajtásának,
d) a közbiztonság hatékony és eredményes védelmének,
e) az állam külső és belső biztonsága hatékony és eredményes védelmének, így különösen a honvédelem és a nemzetbiztonság vagy
f) harmadik személyek alapvető jogai védelmének biztosításához.

2. Nemzetbiztonsági célú adatkezelést érintő magas kockázatú adatvédelmi incidens esetén az adatkezelő nem köteles az érintett tájékoztatására.

3. Nemzetbiztonsági célú adatkezelés esetén az adatkezelő az adatvédelmi incidens Hatóságnak történő bejelentését, valamint a 25/J. § (7) bekezdésében előrt közlések megtételét elhalaszthatja, ha ezek teljesítése nemzetbiztonsági érdekbe ütközne. Ilyen esetben a bejelentési kötelezettséget, valamint a közlési kötelezettséget a nemzetbiztonsági érdek megszűnését követően kell teljesítenie.

4. Ha az adatvédelmi incidensről a Hatóságnak teljesítendő bejelentés minősített adatot tartalmaz, úgy a bejelentést nem elektronikus, hanem hagyományos úton (papír alapú adathordozón, az Állami Futárszolgálat vagy minősített adat továbbítására jogosult kézbesítő útján) kell a Hatóságnak továbbítani. Ennek az az oka, hogy még nem áll rendelkezésre olyan országos lefedettségű elektronikus adatkapcsolati rendszer, amely alkalmas lenne minősített adatot tartalmazó elektronikus dokumentumok továbbítására.

5.7.2. Adatvédelmi hatásvizsgálat

Az adatkezelést megelőzően adatvédelmi hatásvizsgálatot akkor kell elvégezni a Rendelet 35. cikk (1) bekezdése alapján, amikor az adatkezelés „valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve". A hatásvizsgálat szorosan kapcsolódik a Rendeletben található és újonnan nevesített elszámoltathatóság alapelvéhez.

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával. A gyakorlatban ez azt jelenti, hogy az adatkezelő a tervezett adatkezelési műveletet/vagy műveleteket áttekinti, megvizsgálja az adott adatkezelés érintettekre gyakorolt esetleges hatását, felméri és értékeli annak kockázatait, megtervezi a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja.

A Rendelet 35. cikk (3) bekezdése néhány példával szolgál azokra az esetekre, amikor az adatkezelési művelet valószínűsíthetően magas kockázattal jár, és amikor az adatvédelmi hatásvizsgálatot el kell végezni:

- a természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriái (9. cikk (1) bek.), vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok (10. cikk) nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

Ezen túlmenően is hatásvizsgálatot kell végezni azon adatkezelések vonatkozásában, amelyek valószínűsíthetően magas kockázattal járnak az érintettekre nézve. Az eredendően magas kockázatuk

miatt kötelező adatvédelmi hatásvizsgálat hatálya alá tartozó adatkezelési műveletek körének pontosabb meghatározása érdekében – a Rendelet 35. cikkében írtakra, valamint a kapcsolódó preambulum bekezdés értelmében tagállami szinten elfogadandó jegyzékre, továbbá a Rendeletben a „valószínűsíthetően magas kockázattal járó" adatkezelési műveletekre tett egyéb utalásokra figyelemmel– az Iránymutatás részletezi a kilenc fő szempontot, amit mérlegelni kell.

Az adatkezelőknek további segítséget nyújt a Rendelet 35. cikkének (4) bekezdése szerinti adatkezelési műveletek típusainak a jegyzéke, amelyet a felügyeleti hatóságnak kell összeállítania és nyilvánosságra hoznia.

Az adatvédelmi hatásvizsgálatot több fajta, különböző módszertan segítségével el lehet végezni, de a hatásvizsgálatnál figyelembe veendő szempontok azonosak, hiszen a Rendelet meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit.

Az adatvédelmi hatásvizsgálat eredményéről előzetesen konzultálni kell a felügyeleti hatósággal, ha az érintettek jogait és szabadságait érintő kockázatok adatkezelő által történt értékelését követően az adatkezelő nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére (tehát a fennmaradó kockázatok továbbra is jelentősek), akkor kötelező konzultálni a felügyeleti hatósággal. Az elfogadhatatlanul magas fennmaradó kockázatra példa, ha az érintettek olyan jelentős vagy akár visszafordíthatatlan következményekkel szembesülnek, amelyeket nem tudnak leküzdeni (például adatokhoz való jogosulatlan hozzáférés, amely az érintettek életét fenyegető veszélyt, elbocsátást vagy pénzügyi nehézséget eredményez).

Az adatkezelő kötelezettsége és felelőssége az adatvédelmi hatásvizsgálat elvégzése, ugyanakkor ahol van kijelölt adatvédelmi tisztviselő, ott fontos szerepe van a hatásvizsgálat elvégzésében, az ő tanácsát is ki kell kérni.

5.7.2.1. Az adatvédelmi hatásvizsgálat és az előzetes konzultáció az Infotv. szerint

Akárcsak a GDPR, az Infotv. joganyagában is helyet kapott az adatvédelmi hatásvizsgálat jogintézménye. A hatásvizsgálat és az ahhoz kapcsolódó előzetes konzultációs eljárás azt hivatott elősegíteni, hogy lehetőleg még az adatkezelés megkezdése előtt fény derüljön az adatkezelés esetleges alapjogi kockázataira és idejekorán meg lehessen tenni a kockázatok csökkentéséhez szükséges intézkedéseket. A vonatkozó szabályokat az Infotv. 25/G. és 25/H. §§-ai tartalmazzák.

Kockázatbecslés

A törvény főszabály szerint az adatkezelő kötelezettségévé teszi, hogy a tevékenységének megkezdése előtt felmérje az adatkezelés lehetséges hatásait az érintetteket megillető alapjogok érvényesülésére. Ehhez meg kell határoznia, hogy a tervezett adatkezelés várhatóan milyen érintetti körre fog kiterjedni, hiszen e személyi körrel kapcsolatban kell elvégeznie az előzetes kockázatbecslést. A kockázatbecslés elsősorban arra vonatkozik, hogy a tervezett adatkezelés milyen hatással fog járni az adatalanyok személyes adatai védelméhez, valamint a magán- és családi életének és otthonának tiszteletben tartásához való joga érvényesülésére, de érinthet más alapvető jogokat is, mint például a véleménynyilvánítás szabadságát, a lelkiismereti- és vallásszabadságot, a hátrányos megkülönböztetés tilalmát. Az Infotv. az adatkezelés előzetesen vizsgálandó körülményei közül példálódzó jelleggel az adatkezelés célját, az érintettek körét, valamint az adatkezelési műveletek során alkalmazott technológiát emeli ki.

Az adatkezelés kockázati tényezői

A 29. cikk alapján létrehozott munkacsoport WP248. számú, az adatvédelmi hatásvizsgálat elvégzéséhez kiadott iránymutatását alapul véve különösen a következő kockázati tényezők esetében lehet szükséges a hatásvizsgálat elvégzése:

Értékelés vagy pontozás, ideértve a profilalkotást és az előrejelzést is, különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodás helyére vagy mozgására vonatkozó jellemzők alapján.

Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal

Módszeres megfigyelés: mind a nyílt forrásból, mind a titokban végzett megfigyelés az nyomon követés vagy ellenőrzés ide tartozik.

Különleges adatok vagy fokozottan személyes jellegű adatok kezelése. A fokozottan személyes jellegű adatok köre nincs jogszabályban meghatározva, hanem a közvélekedés és az adatkezelő mérlegelése sorolhat valamely adatfajtát e körbe. A közvélekedés alapján fokozottan személyes jellegűek például az érintettek jövedelmi és vagyoni viszonyainak részletei vagy az aktuális hollétüket felfedő helymeghatározási adatok.

Nagy számban kezelt adatok. A WP29 munkacsoport szerint különösen alábbi tényezőket kell figyelembe venni:

- az érintettek száma konkrét számadatként vagy a lakosság arányában;
- a kezelt adatok mennyisége vagy adatfajták köre;
- az adatkezelési tevékenység időtartama vagy állandó jellege;
- az adatkezelési tevékenység földrajzi kiterjedése.

Adatállományok összekapcsolása

Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok. Például a gyermekek, a betegek, a hajléktalanok és a menekültek személyes adatainak kezelése.

Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása, például a biometrikus azonosítás, a dolgok internete, mesterséges intelligencia alkalmazása stb.

Az érintettek jogainak korlátozásával járó adatkezelés. Ennek tipikus esete a titkos információgyűjtés.

Az Infotv. annyiban egyszerűsíti a hatásvizsgálatok során végzendő kockázatelemzést, hogy felhatalmazza a Hatóságot lista közzétételére azokról az adatkezelés típusokról, amelyek a Hatóság megállapítása szerint magas kockázatúak, valamint (egy másik listán) azokról az adatkezelés-típusokról, amelyek a Hatóság szerint nem magas kockázatúak. Az e listákon közzétett megállapítások vélelemként veendők figyelembe a hatásvizsgálatok során. Tehát ha a Hatóság azt állapította meg, hogy valamely adatkezelés-típus magas kockázatú (vagy éppen nem magas kockázatú), akkor az adatkezelőnek ugyanezt kell vélelmeznie.

Adatvédelmi hatásvizsgálat

Ha a kockázatbecslés alapján az valószínűsíthető, hogy az adatkezelés, vagy annak valamely része – például bizonyos adatkezelési művelet, vagy műveletek – magas kockázatú, úgy az adatkezelő az adatkezelés megkezdését megelőzően írásban elkészíti a hatásvizsgálatot, vagyis a tervezett adatkezelés érintettekre kiható alapjogi hatásairól szóló elemzést. Az adatvédelmi hatásvizsgálat tartalmazza legalább:

- a tervezett adatkezelési műveletek általános leírását,
- az érintettek alapvető jogainak érvényesülését fenyegető, az adatkezelő által azonosított kockázatok leírását és jellegét,
- az e kockázatok kezelése céljából tervezett, valamint a személyes adatokhoz fűződő jog érvényesülésének biztosítására irányuló, az adatkezelő által alkalmazott intézkedéseket.

Az adatvédelmi tisztviselő szakmai tanácsadással elősegíti és figyelemmel kíséri az adatvédelmi hatásvizsgálat lefolytatását.

A hatásvizsgálat rendje a kötelező adatkezelések esetében

Az Infotv. hatálya alá tartozó bűnüldözési, honvédelmi és nemzetbiztonsági célú adatkezelések esetében a törvényben elrendelt kötelező adatkezelések a tipikusak, amelyeket az adatkezelésre vonatkozó jogszabályok részletesen szabályoznak, továbbá az adatkezelésnél alkalmazott eszközöket és informatikai rendszereket általában központilag, országosan egységesen fejlesztik vagy szerzik be és rendszeresítik. Az ilyen jogi, szervezeti és technológiai viszonyok között az adatkezelést és az adatfeldolgozást végző szervek és személyek jogalkalmazó és feladatvégrehajtó szerepkörben járnak el és ebből adódóan kevés ráhatásuk van az adatkezelés kockázati tényezőire, hiszen a kockázatok felismerésének és kezelésének már korábban meg kellett történnie, mégpedig akkor, amikor:

- a kötelező adatkezeléssel járó, jogszabályban meghatározott feladatot előíró jogszabály előkészítésére sor került, illetve akkor, amikor
- az adatkezelő által kötelezően alkalmazandó információs rendszer, illetve eszköz beszerzése vagy fejlesztése központilag megtörtént.

Ezért az Infotv. úgy rendelkezik, hogy kötelező adatkezelés esetén az adatvédelmi hatásvizsgálatot az adatkezelést előíró jogszabály előkészítője folytatja le.

Kötelező adatkezelést törvény írhat elő, ezért az adatvédelmi hatásvizsgálatot a törvény előkészítőjének kell elvégeznie. A Kormány által kezdeményezett törvényjavaslat előkészítője az a miniszter, aki a törvényjavaslatot a Kormány nevében benyújtotta, ezért az ő feladata a kötelező adatkezelésre vonatkozó hatásvizsgálat elkészíttetése. A hatásvizsgálatot célszerű a törvénytervezet közigazgatási egyeztetése előtt elvégezni.

A kötelező adatkezelésre vonatkozó adatvédelmi hatásvizsgálatnak nem csak arra kell kiterjednie, hogy a kötelező adatkezelést előíró törvény szabályai összhangban vannak-e az adatvédelmi követelményekkel, hanem azokra a műszaki, technológiai és informatikai kockázati tényezőkre ki kell terjednie, amelyek a kötelező adatkezelést elrendelő törvény normaanyagán kívül esnek, de az Infotv. szerint az adatvédelmi hatásvizsgálat során elemzendők. Ezért a kötelező adatkezelésre vonatkozó adatvédelmi hatásvizsgálat tárgyához kell tartoznia a tervezett törvényi szabályozáson kívül a kapcsolódó végrehajtási rendeleti joganyag, valamint a kötelező adatkezeléshez alkalmazandó informatikai rendszer(ek) és eszközök(ök) elemzésének is. Ez csak úgy lehetséges, ha a tervezett jogszabály előkészítését végző kodifikátorok együtt dolgoznak a kötelező adatkezelés műszaki-informatikai technológiai előkészítésén dolgozó szakemberekkel.

Előzetes konzultáció

Az Infotv. előírja a kötelező adatkezelést elrendelő jogszabály előkészítője számára, hogy előzetesen konzultáljon a Hatósággal, ha az adatvédelmi hatásvizsgálat magas kockázatot tárt fel, illetve, ha az adatkezelés (vagy annak valamely adatkezelési művelete) szerepel azon a listán, amelyen a Hatóság azokat az adatkezelés-típusokat sorolja fel, amelyek magas kockázatát vélelmezni kell. A konzultáció során az adatkezelő a Hatóság rendelkezésére bocsátja az adatvédelmi hatásvizsgálat eredményét, továbbá felvilágosítást nyújt a tisztázandó körülményekről. A Hatóság az előzetes konzultáció során a feladat- és hatáskörébe tartozó intézkedések megtétele mellett konkrét javaslatokat fogalmazhat meg az adatkezelő, illetve az adatfeldolgozó részére az adatkezelés kockázatainak csökkentése érdekében.

6. AZ ADATBIZTONSÁG

A GDPR egyik pozitívuma, hogy pontosabb adatbiztonsági szabályokat tartalmaz, amelyek mind az új definíciókban (például: álnevesítés), mind az új eljárásokban (például: az adatvédelmi incidensek bejelentése) megmutatkoznak. Ugyanakkor tekintettel arra, hogy a szabályozásnak technológia semlegesnek és rugalmasnak kell maradnia csupán csak az évtizedek óta kiforrott adatbiztonsági, információbiztonsági elvárásokat fogalmazza meg. A jogalkotó az információbiztonság területén régóta ismert szabályokat és jó gyakorlatokat illesztett bele az adatvédelmi rezsimbe és nem lép túl az általános elvárások rögzítésén.

Az adatbiztonság kérdése már alapelvi szinten megjelenik, hiszen a GDPR az 5. cikk (1) bekezdésének f) pontjában, az integritás és bizalmas jelleg alapelvével kimondja, hogy a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

Ezeket az előírásokat tovább pontosítja később a jogszabály többek között és különösen a GDPR 32. cikk (1) és (2) bekezdésével, amikor kimondja, hogy az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

A kockázatokról GDPR (75) és (85) preambulumbekezdésben nyerhetünk több információt, amelynek értelmében kockázatról többek között akkor beszélhetünk, ha az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt. A természetes személyek jogait és szabadságait érintő kockázatok jelenthetnek hátrányos megkülönböztetést, személyazonosság-lopást vagy személyazonossággal

való visszaélést, pénzügyi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrányt; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett.

Az említett fogalmi elemek jól ismert információbiztonsági megjelöléseket jelölnek, ennek megfelelően kijelenthető, hogy az adatbiztonság kialakítása és meghatározása esetén az adatkezelők nyugodtan támaszkodhatnak az információbiztonság több évtizedes fogalomrendszerére, szakirodalmára, jó gyakorlataira. A személyes adat megsemmisítése azt jelenti, hogy a személyes adat már nem létezik, legalábbis nincs meg olyan formátumban, amelyben az adatkezelő számára bármilyen módon felhasználható lenne. A személyes adatok elvesztéséről akkor beszélhetünk, ha a személyes adat továbbra is létezik, de az adatkezelő nem fér hozzá, nincs a birtokában. A személyes adatok megváltoztatásáról akkor beszélhetünk, ha a személyes adat állapotában, tartalmában, illetve megjelenésében módosulás történik. Jogosulatlan közlés akkor következik be, ha arra illetéktelen személyekkel a személyes adatot megosztják, míg jogosulatlan hozzáférésről akkor beszélhetünk, ha illetéktelen személy képes a személyes adatot megismerni. A személyes adatok károsodásáról pedig akkor beszélhetünk, ha az eredeti adatállományt megváltoztatták, az nem teljes.

A kockázatokat a GDPR természetesen az érintettek szempontjából határozta meg elsősorban, ugyanakkor a megfelelő szintű adatbiztonság elérése érdekében az adatkezelőnek saját magát is el kell helyeznie a kibertérben, és fel kell mérnie, hogy milyen kiberbűnözők látóterében kerülhet az adatkezelési tevékenysége.

Az adatvédelmi kockázat egy feltételes forgatókönyv, amely azt írja le, hogy a kockázatok forrásai (többnyire a rosszindulatú támadók) az általános fenyegetettségeket figyelembe véve milyen módon tudják a személyes adatokat kiszolgáló infrastruktúra sebezhetőségeit kihasználni, hogy olyan nem kívánt eseményt váltsanak ki, amely személyes adatok jogellenes kezeléséhez vezet és amely hatással van az adatalanyok magánszférájára. A kockázatot két alapvető szempontból érdemes vizsgálni, annak hatása, illetve valószínűsége alapján.

Az adatbiztonság megvalósítása, ahogyan azt fentebb láttuk, elsősorban technikai és szervezeti intézkedésekből áll, ugyanakkor a megfelelő szintű védelem meghatározásánál több szempontot is figyelembe kell vennie az adatkezelőnek, így a tudomány és technológia állását; a megvalósítás költségeit; az adatkezelésének összetettségét, illetve az adatkezelésnek az érintett magánszférájára jelentett kockázatát. Ezen túlmenően a szabályozás inkább csak általános, példálózó szinten emel ki adatbiztonsági jó gyakorlatokat, mint például az információbiztonság „szentháromságát” (bizalmasság, sértetlenség, rendelkezésre állását) vagy az alapvető biztonsági megfontolásokat (álnevesítés, titkosítás, biztonsági betörési teszt, incidens kezelés).

Az adatbiztonság és az érintettek magánszférájának a védelme elsősorban megfelelő szervezési és technikai intézkedésekkel érhető el. A szervezési intézkedéseket többnyire belső szabályozásban, szabályzatokban határoznak meg. Ezekben a szabályzatokban kell aprópénzre váltani az adatvédelmi alapelveket, illetve a GDPR által megkövetelt új kötelezettségeket, valamint itt lehet érvényesíteni azokat az új koncepciókat, amelyeket a GDPR megemlít. Így a belső szabályozásban megjelenik az átláthatóság alapelve az adatkezelési tájékoztatókban, ahol az adatkezelés legfontosabb körülményeit ismertetik meg az adatalanyokkal, illetve az adatvédelmi szabályzatban, ahol a munkavállalók ismerik meg, hogyan kell az adatalanyokat megfelelően tájékoztatni. A belső szabályozás az adatbiztonság szempontjából is kiemelt jelentőségű, hiszen például egy információbiztonsági szabályzatban írhatja le az adatkezelő, hogy milyen IT infrastruktúrával rendelkezik, illetve határozhatja meg, hogy ehhez mérten az adatbiztonság biztosítására milyen magatartást vár el a munkavállalóitól, illetve az ügyfeleitől. Ugyancsak ilyen szabályzatokban juttathatja érvényre a beépített és alapértelmezett adatvédelem elvárásait.

A szervezési és technikai intézkedések jelentős része természetesen függ az adatkezelés jellegétől, körülményeitől, céljaitól, a kezelt személyes adatok körétől, illetve attól, hogy ezekből a körülményekből milyen kockázatok következnek az adatalanyok magánszférájára nézve. Az

adatkezelőnek ezeket a kockázatokat kell folyamatosan értékelnie és a megfelelő adatbiztonsági jó gyakorlatok alkalmazásával csökkentenie. Természetesen az adatbiztonság szintje az erőforrások függvényében jelentősen növelhető.

A (77) preambulum bekezdés alapján a megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához – különösen ami az adatkezeléssel kapcsolatos kockázat beazonosítását, valamint a kockázat forrásának, jellegének, valószínűségének és súlyosságának a felmérését illeti –, továbbá a kockázat mérséklésével kapcsolatos bevált gyakorlatoknak az azonosításához útmutatással szolgálhatnak különösen a jóváhagyott magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Testület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások.

Az adatkezelésének összetettsége, illetve az adatkezelésnek az érintett magánszférájára jelentett kockázata a GDPR másik új koncepciójához a kockázat alapú megközelítéshez kapcsolódik. Az adatbiztonságnak tehát sohasem ugyanazon szinthez kell igazodnia, hanem a kockázatokat mérlegelve, azok hatását és valószínűségét figyelembe véve kell a megfelelő intézkedéseket megtenni. A megtehető intézkedéseknek, pedig az adatkezelés bonyolultságához kell igazodni, figyelembe véve az adatkezelést kiszolgáló eszközöket, infrastruktúrát – a hálózati, hardver és szoftver elemeket is. A leggyakoribb adatkezelési műveletek kialakításánál érdemes figyelembe venni az információbiztonsági standardokat, így biztosítva az elvárható minimális védelmet. Ezzel tudják legkönnyebben figyelembe venni az adatkezelők a tudomány és a technológia állását. A GDPR a költséghatékonyság szempontját is megemlíti, ennek megfelelően az adatbiztonsági intézkedések a fenti szempontok alapján azonosított kockázatokhoz igazodhatnak és amennyiben a kockázatbesorolás megengedi, akkor a költséghatékonyabb megoldás is választható.

6.1. Adatbiztonsági intézkedések az INFOTV. alapján

Az Infotv. 25/I. §-a foglalja össze az adatkezelőtől és az adatfeldolgozótól elvárt adatbiztonsági intézkedéseket. A szabályozása GDPR 32. cikkében foglaltakhoz képest részletesebb és kézzelfoghatóbb követelményrendszert épít fel, ezért hasznos megismerni.

Az adatbiztonsági intézkedések az adatkezelés alapelvei közül elsősorban az Infotv. 4. § (4a) bekezdéséhez kapcsolhatók. Az Infotv. az adatkezelőt és adatfeldolgozót egyaránt kötelezi az adatbiztonsági intézkedések megtételére. A szabályozás az érintettek alapvető jogainak érvényesülését jelöli meg az intézkedés céljaként. A figyelembe veendő alapvető jogok közül – figyelemmel az Infotv. céljára, valamint arra, hogy az érintettek alapvető jogairól van szó – elsősorban az érintettek személyes adatai védelméhez, valamint a magán- és családi életének és otthonának tiszteletben tartásához való joga érvényesülése emelendő ki.

Az Infotv. a kockázatok mértékéhez igazodó műszaki és szervezési intézkedések megtételét várja el. Ez feltételezi az adatkezelés alapvető jogok érvényesülésével kapcsolatos kockázatainak előzetes becslését és elemzését. Az előzetes kockázatbecslés és a kockázatelemzés az adatvédelmi hatásvizsgálat munkafolyamatához is hozzátartozik, tehát ezen a ponton az adatvédelmi intézkedések és az adatvédelmi hatásvizsgálat logikailag összekapcsolódik.

A lehetséges kockázatok Infotv. által elvárt felmérése magában foglalja az adatkezelés összes körülményét, így különösen:

- a tudomány és a technológia mindenkori állását,
- az intézkedések megvalósításának költségeit,
- az adatkezelés jellegét, hatókörét és céljait, továbbá
- az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.

Az adatbiztonsági intézkedések a következő tárgyköröket ölelik fel:

a) az adatkezelő rendszerhez való jogosulatlan hozzáférésének megtagadása,
b) az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozása,
c) jogosulatlan adatbevitel, -megismerés, -módosítás vagy törlés megakadályozása,
d) az adatkezelő rendszerekbe való betörés megakadályozása,
e) a felhasználók csak a számukra engedélyezett adatokhoz férhessenek hozzá,
f) az adattovábbítások és adathozzáférések utólagos ellenőrizhetősége,
g) az adatbevitelek körülményeinek utólagos ellenőrizhetősége,
h) az adattovábbítás közben történő jogosulatlan adatmegismerés, -másolás, – módosítás vagy törlés megakadályozása,
i) az adatkezelő rendszer üzemzavart követően helyreállítható legyen,
j) az adatkezelő rendszer működőképes legyen és a működése során fellépő hibákról jelentés készüljön, továbbá
k) az adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.

Az Infotv. 25/I. § (4) bekezdése az adatbiztonsági intézkedések körébe sorolja az olyan műszaki megoldások alkalmazását, amelyek azt biztosítják, hogy a nyilvántartásokban tárolt adatok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők (kivéve, ha azt törvény lehetővé teszi). E szabály egyúttal az Alkotmánybíróság által kidolgozott egyik adatvédelmi alkotmányossági követelmény, az osztott információs rendszerek elvének érvényesülését is elősegíti.

7. AZ ADATVÉDELMI TISZTVISELŐ[4]

7.1. Bevezetés

Az Európai Unió általános adatvédelmi rendeletének 2018. május 25-étől alkalmazandó szabályai szerint az adatvédelmi tisztviselő kinevezése számos adatkezelő esetében kötelezővé válik. A kinevezés szabályairól a források általában egy-egy kérdés vagy ágazati szempont kiemelése révén adnak tájékoztatást, ezért szükségesnek látszik egy összefoglaló jellegű írás megjelentetése.

Az adatvédelmi tisztviselőkről szóló eszmecserék során gyakran tapasztalható félreértés, amelynek lényege, hogy az adatkezelőknek az adatvédelmi tisztviselőről kialakított, számukra kézenfekvő elgondolása nem találkozik a rendeletben leírt tisztviselői szereppel. Mindez megerősíti annak szükségességét, hogy az adatvédelmi tisztviselőre vonatkozó szabályozás minél szélesebb körben ismertté váljon, és a rendeletben meghatározott szerepre mindenki felkészülhessen.

Elemzésünkben alapvetően a GDPR normaszövegére, a vonatkozó preambulum bekezdésekre, mint értelmező rendelkezésekre támaszkodunk, továbbá az egyes értelmezési kérdésekben bemutatjuk az Európai Unió adatvédelmi hatóságait tömörítő, a 29. cikk szerint működő Adatvédelmi Munkacsoport iránymutatását az adatvédelmi tisztviselőről.

7.2. Kockázatok és elszámoltathatóság

A rendelet kapcsán gyakran említjük a kockázatalapú megközelítést, mint jogalkotói koncepciót, valamint az elszámoltathatóság elvét, amely átszövi a rendelet valamennyi rendelkezését.

A kockázatokról a rendelet preambulum bekezdéseiben találunk egy részletes felsorolást. A jogalkotó a privacy-t fenyegető kockázatokat veszi számba, amelyek a rendelet tekintetében mindvégig egyfajta zsinórmértékül szolgálnak: addig, amíg a személyes adatok kezelése kapcsán ezek a jelenségek előfordulhatnak, a védelem indokolt és végső soron ez adja az adatvédelmi intézkedések legitimitását.

Az elszámoltathatóság lényege abban ragadható meg, hogy a jogalkotó szándéka szerint az adatkezelés végrehajtása során egyrészt érvényesül a rendelet szabályrendszere, másrészt pedig a szervezet képes arra, hogy ezt világosan és egyértelműen bemutassa. Az érintett helyzete és várakozásai fontosak a megfelelés szempontjából, ez a rendelet (47) preambulum bekezdésében is érvényre jut, amikor a jogalkotó a „számíthat-e észszerűen” fordulatot használja. Ez mércéje is az adatkezelés jogszerűségének, mert ha erre megnyugtató válasz adható az adatalanynak, úgy az adatkezelés feltehetően nem jogellenes, illetve az érintetti panaszoknak elejét lehet venni, amelyek tipikus esetben kiindulópontjai jogvitáknak, illetve a hatósági eljárásoknak.

Az elszámoltathatóság hangsúlyozásával az adatkezelő és adatfeldolgozó oldalán érvényesülő felelősség még világosabban kirajzolódik. Valamennyi szereplő helyzete változik valamilyen módon:

---

[4] A fejezet Szabó Endre Győző: Az adatvédelmi tisztviselőről – A GDPR szabályainak elemzése, Infokommunikáció és Jog XV. évfolyam 70. szám, a 2018 című tanulmánya.

az adatkezelők felelősségének kiemelése mellett a megfelelés eszközeinek tárháza is bővül: a jogalkotó új alapelveket fogalmazott meg (privacy by design és privacy by default), az adatvédelmi tisztviselő olyan belső ellenőrzési mechanizmus letéteményese, amelyre eddig nem volt példa. Ha egy mondatban szeretnénk összefoglalni a tisztviselő szerepét, akkor a rendeletet idézve azt mondhatjuk, hogy az adatvédelmi tisztviselő megkönnyíti a GDPR rendelkezéseinek való megfelelést. Mindezt a kockázatokra tekintettel, az elszámoltathatóság jegyében teszi.

Az adatkezelő a jogi megfelelés terén a tisztviselő igénybevételén túl más eszközökre is támaszkodhat: magatartási kódexek kidolgozása révén közös, például ágazati erőfeszítések részese lehet és meríthet a közös tudásból, amely az adott területen való megfelelést elősegítheti. A tanúsítás révén egy külső szereplő segítségét veheti igénybe belső folyamatai áttekintése és adatvédelmi jogi rendezése érdekében.

Az említetteken túl az adatkezelő az előzetes adatvédelmi hatásvizsgálat elvégzéséhez igénybe vehet külső, erre szakosodott intézményeket, akár például az üzleti vagy egyetemi szektorból is. A hatásvizsgálat során bizonyos esetekben kötelező lesz a konzultáció az adatvédelmi felügyeleti hatósággal, amely a jogi megfelelésről folytatandó egyeztetésre ad módot. A határon átnyúló adatkezelések ügyében az Európai Adatvédelmi Testület rendelkezik végső soron döntési lehetőséggel, amely Európai Unió szerte egységes jogértelmezést és gyakorlatot ígér.

Amennyiben a rendszer a jogalkotói elgondolás szerint hatékonyan működik majd, úgy az adatkezelők nagyobb jogbiztonság mellett végezhetik tevékenységüket, mint az irányelv alatti, széttöredezett tagállami szabályozással jellemezhető időszakban. A felügyeleti hatóságok az előzetes konzultáció, a tanúsítási mechanizmus felügyelete, valamint a tisztviselőkkel való kapcsolat révén szintén új és gyakorlatias szerepbe kerülnek.

Az érintettek régi és megerősített, valamint új jogaikkal a korábbiakhoz hasonlóan élhetnek, azonban az elsődleges jogorvoslati lehetőségek egyértelműen az adatkezelő felé tevődnek át. Nagyobb jelentősége lesz annak, hogy első körben milyen módon lehet megnyugtató megoldást találni az adatkezelő oldalán.

Ha élnek, és helyesen élnek a rendelet adta lehetőségekkel, akkor a hazai vállalatok versenyképessége is javítható, hiszen az új uniós jogi keret egy professzionálisabb menedzsmentet vár el az adatkezelőktől. Érdemes tehát a felkészülést nem csupán kötelezően adódó feladatként, hanem fejlődési lehetőségként is felfogni. Ebben is lesz feladata az adatvédelmi tisztviselőnek.

7.3. Adatvédelmi tisztviselők

Az adatvédelmi rendelet kiemelt figyelmet fordít azokra az adatkezelő szervezetén belül alkalmazott tisztviselőkre, akik már eddig is nagymértékben hozzájárultak az adatvédelmi szabályok érvényesítéséhez.

A 29-es Munkacsoportnak az adatvédelmi tisztviselőről készült iránymutatását azzal kezdi, hogy ők az új jogi keret „szívében” lesznek sok adatkezelő szervezetnél, elősegítve a rendeletnek való megfelelést. A Munkacsoport továbbmegy, és azt állítja, hogy az elszámoltathatóság egyik alapköve a tisztviselői intézmény, és foglalkoztatásuk versenyelőnyt jelenthet az üzleti szereplők számára.

A rendelet (77) preambulum bekezdése szerint „a megfelelő intézkedéseknek az adatkezelő általi végrehajtásához, valamint a megfelelés általuk való bizonyításához – különösen, ami a kockázat beazonosítását, valamint a kockázat súlyosságának a felmérését illeti –, továbbá a kockázat mérséklésével kapcsolatos útmutatással szolgálhatnak különösen a jóváhagyott magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Testület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások”.

Hozzáteszi az anyag, hogy a tisztviselők maguk személyesen nem felelősek a jogszabályoknak való

megfelelésért, az adatkezelőre vagy az adatfeldolgozóra hárul a felelősség az esetleges jogsértésekért. E szabálynak, amint látni fogjuk, munkajogi vonatkozásai is vannak.

A nemzetközi példák azt mutatják, hogy vannak országok, ahol a belső adatvédelmi felelősök intézménye még nem honosodott meg, ezért a GDPR-ra való felkészülés a tisztviselők képzésének jegyében is telik.

7.4. Az adatvédelmi tisztviselő kinevezésének kötelezettsége

A rendelet először felsorolja azokat a szervezeteket, ahol ki kell nevezni tisztviselőt:

Ilyen adatkezelő szervezetek a közhatalmi szervek, illetve közfeladatot ellátó szervek. Ennek definícióját nem uniós szinten kell megadni, hanem tagállami szinten. A közhatalmi szervek magukban foglalják a központi, regionális és helyi kormányzati szerveket, a közfeladatot ellátó szervek pedig széles skálát jelentenek.

A 29-es Munkacsoport véleménye a közfeladatot ellátó szervek között megemlíti a tömegközlekedési szolgáltatásokat, közszolgáltatásokat (víz és áram), közútfenntartás ellátóit, közszolgálati műsorszolgáltatókat, szabályozott szakmák fegyelmi testületeit. A vélemény szerint ezekben az esetekben is hasonló az érintett helyzete, mint a közhatalmi szervekénél, tehát nincs választása, illetve befolyása az adatok kezelésére, ezért is indokolt az a pótlólagos védelem, amit a tisztviselő jelenthet. Jó gyakorlatként említi a vélemény azt, hogy azok a magánszervezetek, amelyek valamilyen közfeladatot is ellátnak, kineveznek adatvédelmi tisztviselőt, és az ő tevékenységük kiterjed egyébként a nem közfeladathoz kötődő személyes adatkezelésekre is.

A rendelet megjelöli azokat a tevékenységeket, amelyek végzése kinevezési kötelezettséggel jár:

A rendelet azután felsorol tevékenységeket, amelyek indokolják a tisztviselő kinevezését: fő tevékenységük rendszeres, szisztematikus és nagymértékű megfigyelést (monitoring) foglal magába. Itt nem csupán azokat a tevékenységeket kell érteni, amelyek a szó hétköznapi értelmében jelentenek megfigyelést (például kamerás megfigyelés), hanem a felhasználói magatartást nagy részletességgel rögzítő, naplózó (például banki ügyviteli vagy bűnüldözési célból végzett) tevékenységeket is. Fontos, hogy ez a kitétel csak a magánszektorban működő adatkezelőkre vonatkozik (nem vonatkozik tehát a közszférára, mert ott egyébként általános kinevezési kötelezettség érvényesül).

A 680/2016-os számú bűnügyi irányelv, amely az adatvédelmi csomag része, szintén kötelezővé teszi az adatvédelmi tisztviselő kinevezését. Itt tehát a tevékenység jellege az a körülmény, amely a kinevezést indokolja. A kötelezés általános, a tagállam azonban felmentheti a kinevezés kötelezettsége alól az eljáró bíróságokat és egyéb független igazságügyi hatóságokat.

Kinevezési kötelezettséget eredményező adatkezelés az adatok típusára tekintettel:

Végül a rendelet felsorolja azokat az adatokat, amelyeknek a kezelése, ha a fő tevékenységi körhöz tartozik, és nagy számban kezelnek ilyen adatokat, akkor a tisztviselő kinevezése kötelező: a különleges adatok tartoznak ide, ahol a rendelet külön kategóriaként határozza meg a büntetőjogi felelősséggel kapcsolatos adatokat.

Figyelmet érdemel a jelenlegi magyar szabályozás és a rendelet szövegének az összehasonlítása, ugyanis a rendelet alkalmazásától olyan adatok is a különleges adatok körébe tartoznak majd, amelyek most még nem: ilyen a biometrikus adatok és a genetikai adatok köre.

7.4.1. Értelmezési kérdések – fő tevékenység, nagymértékű adatkezelés

7.4.1.1. Fő tevékenység

A rendelet több ponton is utal a fő tevékenységre. A (97) preambulum bekezdés szerint az adatkezelők fő tevékenységi körébe az adatkezelők elsődleges tevékenységei tartoznak, a járulékos tevékenységként végzett személyes adatok kezelése nem.

A fő tevékenység kitétel az adott kontextusban értelmezendő. Egy kórház esetében például a gyógyító-megelőző tevékenység a fő feladat, és mivel ezt személyes adatok tömege nélkül nem tudnák ellátni, ezért a kinevezés kötelezettsége itt is érvényesül. Egy magánbiztonsági cég nagy területen és sok személyre nézve végez megfigyeléseket – ebben az esetben is érvényesül, hogy fő tevékenysége együtt jár személyes adatok kezelésével. Futball klub esetében a szurkolók beléptetése megint csak a fő tevékenységi körhöz tartozik. Hasonlóképpen a követeléskezelő szervezetek esetében az ügyfelekkel való kapcsolattartás, az ahhoz tartozó adatkezelés ismét fő tevékenységnek tekintendő.

A skála másik oldalán olyan járulékos adatkezeléseket kell említeni, amelyek nem indokolják az adatvédelmi tisztviselő kinevezését, így például a munkavállalói adatok kezelése (bérszámfejtés) vagy a szokásos IT támogatási tevékenységek.

7.4.1.2. Nagymértékű adatkezelés

A rendelet nem definiálja pontosan a nagymértékű kitételt, de a (91) preambulum bekezdés nyújt némi eligazítást. E szerint nagymértékű adatkezelésnek tekintendő az, amely jelentős mennyiségű személyes adat regionális, nemzeti vagy nemzetközi szintű kezelését célozza, továbbá amelyek az érintettek jelentős számára hatással lehetnek.

Nem is lehet ezt a kritériumot teljes pontossággal meghatározni, a Munkacsoport mégis nyújt támpontokat ennek mérlegeléséhez:

- Adatalanyok száma
- Kezelt adatok mértéke
- Az adatkezelés időtartama, tartóssága
- Az adatkezelés földrajzi kiterjedtsége

Mindezek alapján a nagymértékű adatkezelés körébe tartozó adatkezelésnek tekintendő:

- Egy kórház adatkezelése
- Közlekedési rendszerek adatkezelése (például elektronikus jegyeken keresztül)
- Valós idejű helymeghatározó adatok kezelése például egy nemzetközi élelmiszerlánc szolgáltató részéről
- Egy biztosító vagy bank ügyféladat kezelése
- A keresőmotor magatartásalapú reklámozási tevékenysége
- A telefon- vagy internet szolgáltató adatkezelése (tartalom, forgalom, helymeghatározás)
- Egy nagy tömegrendezvény, például fesztivál kapcsán kezelt adatok tömeges mérete miatt, még ha az adatkezelés rövid ideig valósul is meg.

7.4.1.3. Rendszeres és szisztematikus megfigyelés

Ez a kitétel sincs definiálva a rendelet szövegében, a (24) preambulum bekezdés említi a megfigyelést, igaz, más kontextusban. E szerint annak meghatározásakor, hogy az adatkezelés az érintett magatartása megfigyelésének minősül-e, meg kell vizsgálni, hogy a természetes személyeket nyomon követik-e az interneten, illetve ezután az érintett profiljának elkészítését is magában foglaló adatkezelést alkalmaznak-e annak érdekében, hogy a természetes személyre vonatkozó döntéseket hozzanak, vagy elemezzék, illetve előre jelezzék a személy preferenciáit, magatartását vagy éppen beállítottságát.

Az internetes követés és profilozás egyértelműen ide tartozik, beleértjük a magatartás alapú reklámozást is. Az internet csak egy példa, minden más közegben megvalósuló rendszeres és szisztematikus megfigyelés kiváltja a kinevezési kötelezettséget.

A rendszeres kitételhez a munkacsoporti iránymutatás az alábbi támpontokat nyújtja:

- Folyamatos vagy rendszeres időközönként történik
- Meghatározott időnként ismétlődik

A szisztematikus kitétel tartalma a Munkacsoport szerint az alábbi:

- Rendszerszerű történések jellemzik
- Előre meghatározott, szervezett vagy módszeres tevékenységekből épül fel
- Egy általános adatgyűjtési terv részeként valósul meg
- Stratégia részeként kerül rá sor

Mindezek alapján a kinevezési kötelezettség az alábbi adatkezelések esetében érvényesül a Munkacsoport szerint:

- Telekommunikációs hálózat üzemeltetése
- Biztosítási prémiumok, csalás megelőzése érdekében alkalmazott scoring
- Helymeghatározás révén követés

7.4.2. Az adatkezelőnek vagy az adatfeldolgozónak kell kineveznie az adatvédelmi tisztviselőt?

A feltett kérdésre nincs általános válasz, de az eddigi tapasztalataink alapján az adatkezelőknél mintha természetesebben adódna a kinevezési kötelezettség, mint az adatfeldolgozónál. Az, hogy az adatkezelőnél ki kell nevezni tisztviselőt, nem jár automatikusan kinevezési kötelezettséggel az adatfeldolgozó oldalán.

Elképzelhető olyan eset, amikor az adatkezelőre nem, de az adatfeldolgozóra vonatkoznak már a tárgyalt kritériumok, ezért ott kötelező lesz a kinevezés. A Munkacsoport példája a következő: egy családi vállalkozás kiskereskedelemmel foglalkozik, amely nem jár nagymértékű adatkezeléssel. Azonban előfordulhat, hogy az adatfeldolgozó, amely számos üzleti szereplőt kiszolgál honlapok elemzése és célzott reklámozás révén, már olyan mennyiségű adatokat kezel, amely teljesíti a nagymértékű kitételt. Ebben az esetben az adatfeldolgozónak ki kell jelölni adatvédelmi felelőst, míg az adatkezelő mentesül ez alól.

7.4.3. A kinevezés mérlegelése, a mérlegelés dokumentálása

A fentiekben azt mutattuk be, hogy hol és milyen feltételek fennállása esetén kell kinevezni adatvédelmi tisztviselőt. Azokban az esetekben, amikor nem nyilvánvaló, hogy az adatvédelmi tisztviselő kinevezése nem szükséges, a Munkacsoport azt ajánlja, hogy az adatkezelő dokumentálja azt a mérlegelést, amely a kinevezés mellőzéséhez vezetett. Ez része a rendeletnek való megfelelést bemutató dokumentációnak, amely adott esetben a felügyeleti hatósággal való kapcsolatban releváns lehet. Szükség esetén ezt a dokumentumot frissíteni kell, ha például az adatkezelő új tevékenységekbe kezd, amely már a kinevezés kötelezettségével járhat.

7.4.4. Adatvédelmi tisztviselő önkéntes kinevezése

A rendelet csak a kötelező kinevezés eseteit rögzíti, az önkéntes kinevezés természetesen magától értetődő lehetőség. Ha az adatkezelő szervezet erre kötelező rendelkezés hiányában úgy dönt, hogy kinevez adatvédelmi tisztviselőt, akkor rá, az ő státuszára, munkajogi helyzetére ugyanúgy vonatkoznak a rendelet 37-39. cikkeiben, illetve az irányelv 32-34. cikkeiben foglalt rendelkezések.

Az is lehetséges, hogy önkéntes alapon nem adatvédelmi tisztviselőt, hanem egy olyan belső vagy külső munkatársat bíznak meg, aki az adatvédelmi ügyekben működik közre. Ebben az esetben világosan jelezni kell, hogy nem tisztviselőről, hanem például tanácsadóról van szó. Az is fontos ajánlása a Munkacsoportnak, hogy amennyiben a tisztviselőt a szervezeten belül kinevezték, akkor ez a szerep a szervezet által folytatott valamennyi adatkezelésre kiterjed, nem lehet a különböző tevékenységeket megszűrni, vagy más szempontból nézve a tisztviselő hatáskörét megcsonkítani.

Ami a magyar viszonyokat illeti, arra lehet számítani, hogy nem szűkül azoknak a szervezeteknek a köre, amelyeknél a tisztviselő alkalmazása kötelező. Egyébként is az prognosztizálható, hogy a rendelet alkalmazása kapcsán adódó jogalkalmazási kérdések inkább a foglalkoztatott tisztviselők vagy tanácsadók számának emelkedésével fog járni.

A tisztviselő kinevezésével kapcsolatos kritériumok egyébként jól illeszkednek az előzetes adatvédelmi hatásvizsgálatra vonatkozó szabályokhoz. Nem véletlen, hogy a jogalkotó a hatásvizsgálat elkészítése kapcsán kötelezővé teszi a tisztviselő tanácsának kikérését azokban az esetekben, amikor van kijelölt adatvédelmi tisztviselő.

7.5. Az adatvédelmi tisztviselő jogállása

Az információs önrendelkezési jogról és az információszabadságról szóló törvény (Infotv.) meghatározza a felelős lehetséges végzettségeit (jogi, közigazgatási, informatikai, vagy ezeknek megfelelő felsőfokú végzettség). A rendelet más megközelítést alkalmaz a korábbi magyar szabályozáshoz képest, szakmai rátermettségről és feladatai ellátására való alkalmasságról beszél. Az adatvédelmi jogot és gyakorlatot szakértői szinten ismerő személy nevezhető ki, vagy bízható meg.

7.6. A kijelölés kritériumai: minek alapján ítélhető meg a tisztviselőtől elvárt tudás és szakértelem?

A rendelet szerint az adatkezelés sajátosságai és a kezelt adatok számára az adott körülmények között nyújtandó védelem alapján ítélendő meg, hogy milyen ismeretek szükségesek. Ezek tehát az Infotv-ben jelenleg szereplő végzettséget taglaló felsorolás szükségtelenségét vetítik előre. A felkészültséget illetően ugyanakkor meglehetősen konkrét elvárásokat is említ a rendelet: az Európai Unió és az adott ország adatvédelmi jogának és gyakorlatának szakértői szintű ismerete elvárás. Mind a munkáltatónak, mind a tisztviselőnek fontos tájékozódási pontot nyújtana, ha erről valaki igazolást tudna bemutatni, és van is erre igény.

A felkészültség kapcsán hivatkozhatunk az Európai Adatvédelmi Biztos 2010-ben kibocsátott elemzésére, amelyben az uniós intézmények által kinevezett adatvédelmi tisztviselőkkel kapcsolatos szabályokról ad tájékoztatást. Ez a dokumentum öt konkrét képzettséget említ, nevezetesen a CIPP, a CIPP/IT, továbbá a CISSP, a CISA és a CISM képzéseket. A 2010-es dokumentum kibocsátását

követően nyílt meg a CIPP / E képzés, amely kifejezetten az európai adatvédelmi jogra fókuszál a bemutatott képzéscsaládon belül. Az Európai Adatvédelmi Biztos álláspontja szerint ezek megléte fontos szempont az uniós intézménynél dolgozó tisztviselő kiválasztása során.

Az Európai Adatvédelmi Biztos anyaga kapcsán megemlítendő, hogy az nem az általános adatvédelmi rendelet értelmezése céljából készült, továbbá csupán egy szervezet képzéseit említi. A megszerezhető képzettségek és képesítések országonként változók lehetnek. Magyarországon jelenleg egy egyetemi képzés keretében képeznek adatvédelmi szakértőket, illetve adatvédelmi szakembereket.

Az adatvédelmi hatósági tapasztalat fényében a felkészültség alábbi kritériumait tudjuk megfogalmazni, amelyek egyszersmind a tisztviselő saját munkája kapcsán is hasznos áttekintést nyújthatnak:

- A 29-es Munkacsoport szerint az adott ágazat, működési terület ismerete fontos és hasznos, továbbá az adott szervezet belső működésének, eljárásainak ismerete, különösen a közhatalmi területen működő adatkezelőknél.
- Jogszabályi környezet ismerete: ideértve az alapjogi vonatkozásokat (Európai Unió Alapjogi Charta, Alaptörvény, Európai Emberi Jogi Egyezmény, Európa Tanács 108-as egyezménye), valamint a horizontális szabályozás (magyar és európai uniós)
- Az Európai Unió és az Európai Unió jogának megfelelő ismerete
- Az adott ágazati szabályozás ismerete
- Szabályozástörténeti ismeretek bizonyos mértékben – milyen jogintézményi előzmények vezettek az adott szabályozáshoz (például miért fontos a 30. cikk szerinti nyilvántartás a megszűnő adatvédelmi nyilvántartás fényében, vagy a különleges adatkategóriák bővülése a korábbi magyar szabályozáshoz képest)
- Eljárási szabályok ismerete (például jogalkotás, vagy az, hogy miként kerül egy ügy előzetes döntéshozatalra az Európai Unió Bírósága elé)
- Intézményrendszer ismerete (például az Európai Adatvédelmi Testület funkciója)
- Releváns döntések ismerete: bírósági joggyakorlat, hatósági döntések
- Szakmai konzultáció lehetősége – szakértői támogatói kör elérhető a tisztviselő részére
- Ágazati együttműködési fórumban való részvétel
- Adatvédelmi tisztviselői hálózatban részvétel
- Az adott ágazat általános ismerete
- Az adatkezelő szervezet felépítése, története, profilja, korábbi jogi problémái (nem csupán adatvédelmi jogi, hanem például munkaügyi, fogyasztóvédelmi, versenyjogi területen – mindaz, ahol az egyén védelme releváns lehet)
- Az adatkezelő szervezet tevékenységének alapos ismerete, és a kapcsolódó, adott esetben nem rutin kérdésekre való felkészültség (például külföldre való adattovábbítás szabályai), a szervezet által folytatott eljárások ismerete
- Aktuális adatvédelmi vonatkozású hírek figyelemmel kísérése, naprakészség
- Az adatvédelmi hatóság munkájának ismerete
- Releváns honlapok ismerete
- Szakmai tájékozódás lehetősége idegen nyelven, ha szükséges
- Az adott területen elvárható informatikai, információbiztonsági ismeretek
- Belső oktatási feladatokra való felkészültség
- Személyes tulajdonságok (integritás, szakmai morál stb.)

Bizonyos értelemben érzékeny, vagy nehezen megfogható kritérium az alkalmasság. A Munkacsoport megpróbált ezen a téren is tájékozódási pontokat kijelölni, ilyenek mindenekelőtt a személyes képességek, úgymint az integritás (amely a szervezet integritásának, értékeinek védelme érdekében nélkülözhetetlen), továbbá a magas szintű szakmai etikai elvárások, vagy a diszkréció. Mindezek alapvetőek akkor, amikor az az elvárás a tisztviselővel szemben, hogy a szervezeten belül az adatvédelmi kultúra kialakulását, megerősítését segítse elő.

További lehetséges kritériumként említhető az együttműködés képessége és a megbízhatóság.

Egy szakértői értelmezés szerint a megbízhatóság az összeférhetetlenséggel is szoros összefüggést mutat, és az összeférhetetlenséget – az adott tisztviselő hozzáállásától vagy személyes kvalitásaitól függetlenül – vélelmezni kell a következő személyek esetében: a tulajdonos, a vezető testület tagja, egyéb magas rangú vezető, a betöltött munkakör okán össze nem egyeztethető feladatok ellátói (informatikai vagy humánerőforrás vezető, a napi adatkezelési feladatokat irányító munkatársak), továbbá a felsorolt személyek közeli hozzátartozói.

7.7. A foglalkoztatás szabályai

A tisztviselő foglalkoztatását illetően a rendelet rugalmasságra törekszik. A vállalkozáscsoport közös tisztviselőt is kijelölhet, ha a tisztviselő könnyen elérhető. Az elérhetőség kapcsán nyilvánvalóan a nemzetközi működés sajátosságait is figyelembe kell venni, de mindenképpen szükség van helyben is személyzetre, hiszen a helyi viszonyok ismerete nélkülözhetetlen, az adatalanyokkal való kapcsolattartás pedig például nyelvismeret nélkül nem képzelhető el. A közelség és az elérhetőség tehát meghatározó elvárás. A Munkacsoport szerint elsőbbséget élvez az a megoldás, hogy a tisztviselő az Európai Unióban működik, de elismeri, hogy lehetnek olyan esetek, amikor hatékonyabban láthatja el a feladatát egy harmadik országban tevékenykedve. Az adott szervezet, illetve az érintettek igényeire kell tekintettel lenni ennek mérlegelésekor.

A magánszektorbeli adatkezelők kapcsán meghatározott kategóriába tartozó adatkezelők közös tisztviselőjét nevesíti a rendelet, aki értelemszerűen eljárhat a tagok, illetve az egyesület nevében. Közös tisztviselő kijelölését uniós vagy tagállami jog előírhatja, a későbbi jogalkotás a tisztviselők helyzetét tehát még lényegesen befolyásolhatja.

A foglalkoztatás formáját illetően a rendelet szerint a tisztviselő alkalmazott lehet, vagy szolgáltatási szerződés keretében láthatja el feladatait. Itt is, mint minden hasonló esetben az értelemszerű terminológiai egyezést kell keresni az uniós és a magyar jog között, tehát munkaviszony vagy megbízás keretében is ellátható a tisztviselő feladata, ahogyan eddig is ez volt a magyar gyakorlat.

7.7.1. A tisztviselő adatainak nyilvánossága, elérhetőség

A tisztviselői jogállás fontos jellemzője a nyilvánosság, tehát bárki által megismerhető információ a név és az elérhetőség. Ezt a hatóság nyilván is fogja tartani, a belső adatvédelmi felelősök nyilvántartása tehát feladatként megmarad az ellenőrző szerveknél. Ennek természetesen garanciális jelentősége is van, hogy esetleges panasz esetén a tisztviselő bárki számára elérhető legyen. Az eredeti angol verzió nem említi a tisztviselő nevét, míg a magyar verzió már igen (contact details – nevét és elérhetőségét), mint nyilvános, valamint a hatósággal közlendő adatot. Érdekes módon az irányelv magyar verziója ugyanezzel a fordítási hibával került a hivatalos közlönybe. Az érintettnek a rendelet 13. és 14. cikke alapján nyújtandó tájékoztatásnak szintén része az adatvédelmi tisztviselő elérhetősége.

A külvilág felé történő nyilvánosságra hozatal mellett meg kell említeni a belső nyilvánosságot, amely azt szolgálja, hogy a szervezet munkavállalói személyesen el tudják érni a tisztviselőt. Azt ajánlja ezért a Munkacsoport, hogy a belső névjegyzékekben, telefonkönyvekben a tisztviselő neve és elérhetősége szerepeljen. Az is alapvető elvárás, hogy a szervezet munkavállalói bizalommal kereshessék a tisztviselőt, ezért írja elő a rendelet a tisztviselő számára a titoktartási kötelezettséget, illetve az adatok bizalmas kezelésére vonatkozó kötelezettséget.

A panaszon túl a rendelet az érintettek számára kötelezően elérhetővé rendeli a tisztviselőt akkor, amikor a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódóan bármilyen kérdést

megfogalmaznak. Ez nem jelenti azt, hogy a tisztviselő a kizárólagos kapcsolattartó adatvédelmi ügyekben, de neki kötelessége az adatalanyok rendelkezésére állni, különösen például adatbiztonsági incidensek esetében. Ez lehet e-mail, valamiféle forró vonal, meg lehet könnyíteni a kapcsolatba lépést, továbbá egy webes formula kialakításával.

7.7.2. Teljes-, vagy részmunkaidős foglalkoztatás

A tisztviselőnek nem kell teljes állásban ezt a feladatát betöltenie, illetve egy személy több szervezetnél is elláthat ilyen feladatokat. Sőt, elképzelhető az is, hogy egy csoport látja el a tisztviselői feladatokat, elismeri a Munkacsoport ugyanis, hogy ez hozzájárulhat a tevékenység magasabb szintű ellátásához. Ilyen esetben azonban ki kell jelölni azt a személyt a csoportból, aki valóban felelős az adott szervezet vonatkozásában, a tisztviselői tevékenység tehát nem válhat személytelenné. A szabályozás szelleme és logikája azt mutatja, hogy személyes közreműködésről, függetlenségről és végső soron felelősségről van szó, amelynek címzettje egy természetes személy kell, hogy legyen.

Egy gyakran elfeledett szabály kívánkozik még a tisztviselő jogállásához: a felügyeleti hatóság feladatai kapcsán a rendelet is és az irányelv is előírja, hogy azok ellátása az érintett és az adatvédelmi tisztviselő számára térítésmentes legyen.

7.7.3. Az adatkezelő feladatai a tisztviselő munkájának támogatása terén

Az adatkezelő (a foglalkoztató) az adatvédelmi tisztviselőt megfelelő forrásokkal támogatja, hogy feladatait el tudja látni. Ez magában foglalja a szükséges anyagi forrás, megfelelő helyiség, szükség esetén munkatársak rendelkezésre bocsátását. Azt is biztosítani kell, hogy a személyes adatokhoz, valamint az adatkezelési műveletekhez (ezek megtekintéséhez, megfigyeléséhez) hozzáférése legyen. A 30. cikk szerinti nyilvántartás ebből a szempontból kulcsfontosságú, ezért javasolható a tisztviselőknek, hogy ezt a feladatot személyesen ők lássák el.

További kötelezettség a foglalkoztató oldalán, hogy biztosítja a tisztviselő számára azokat a forrásokat, amelyek szakértői szintű ismereteinek fenntartásához szükségesek. Ezek meglehetősen konkrét elvárások, amelyekből adódik például a munkaidőn belül a továbbképzés feltételeinek megteremtése is.

Az adatkezelő feladata annak szavatolása, hogy a tisztviselő feladatait és kötelezettségeit függetlenül tudja ellátni. A tisztviselő függetlenül látja el tehát feladatait, ez azonban nem jelent felelőtlenséget. A függetlenség azt jelenti, hogy nem fogadhat el senkitől sem utasítást, ennek garantálása az adatkezelő szervezet kötelezettsége. Adatvédelmi ellenőrzési feladatai terén, a jogszerűség megítélése kapcsán tehát még a szervezeten belül sem utasíthatja senki. Nem utasíthatják arra, hogy miként kezeljen egy ügyet, milyen eredményre kell jutni, hogyan vizsgáljon ki egy panaszt, vagy éppen milyen jogértelmezést tegyen magáévá. Mivel az adatkezelés jogszerűségéért az adatkezelő felelős, ezért fontos, hogy a tisztviselő eltérő véleményét hangoztathassa a legmagasabb döntéshozatali fórum előtt is. Lehetővé kell tenni, és ez is egy jó gyakorlat, hogy a tisztviselő évente beszámoljon tevékenységéről a legfelső menedzsmentnek.

Munkajogilag is értelmezhető védettséget jelent a számára, hogy feladatai ellátásával összefüggésben nem bocsátható el, de még csak szankcióval sem sújtható. A szankció természetesen tágan értelmezendő, és minden egyébként járó előny elmaradása is szankciónak tekintendő, amennyiben az a feladatai ellátásával összefüggést mutat. Ilyen lehet például az előmenetel hátráltatása, a többi munkavállalónak járó előnytől való megfosztás. Mivel kényes egyensúlyról van szó, ezért nem csupán a bekövetkezett hátrányok minősülnek jogellenesnek, hanem az ezzel való fenyegetés is, amennyiben az a tisztviselő munkájának befolyásolására irányul.

Természetesen vannak esetek, amikor a tisztviselő jogviszonya jogszerűen szüntethető meg. A Munkacsoport példájánál maradva ilyen lehet, amikor a tisztviselőt lopáson érik, vagy pszichésen, fizikailag, vagy akár szexuálisan zaklatja munkatársait, vagy hasonló súlyos visszaélést követ el.

Nem változtat a rendelet azon a már meglévő magyar szabályon, hanem megerősíti, hogy a tisztviselő a szervezet legfelső vezetésének tartozik felelősséggel. Feladatai ellátásához nélkülözhetetlen a vezetői szintű támogatás. Bármilyen munkakör ellátását el lehet ugyanis lehetetleníteni azzal, ha egyszerűen nem hagynak rá időt, ezért a tisztviselő esetében is elvárás és munkacsoporti ajánlás a megfelelő idő biztosítása. Jó gyakorlat, ha százalékosan határozzák meg a tisztviselői feladatokra fordítható idő mennyiségét. Ha szükséges, akkor további munkavállalókat kell a tisztviselő rendelkezésére bocsátani, hogy feladatait hatékonyan el tudja látni.

A tisztviselő munkájának támogatása körében említendő még a házon belüli szolgáltatásokhoz való hozzáférés, úgymint a HR, a jogi, a biztonsági, az IT terület annak érdekében, hogy támogatást, a közös feladatokhoz segítséget, továbbá információkat kaphasson.

7.7.4. Összeférhetetlenség

Ha több feladatot is ellát a tisztviselő, akkor az adatkezelőnek kell biztosítani azt, hogy ezekből a feladatokból ne fakadjon összeférhetetlenség. Első helyen kell említeni azokat a munkaköröket és feladatokat, ahol a tisztviselőnek például az adatkezelés célját és eszközeit illetően kellene döntést hoznia. Ezek mindenképpen összeférhetetlenek a független tanácsadói, megfigyelői, illetve ellenőrző funkciójával. Ennek megfelelően nem lehet például ügyvezetői pozícióban, vagy HR, esetleg IT vezető. Szintén konfliktust eredményezhet, ha egy külső tisztviselőt azzal bíznak meg, hogy a szervezetet képviselje a bíróság előtti eljárásban, és ilyen módon kerül abba a helyzetbe, hogy az adatkezelő álláspontját a saját meggyőződésétől függetlenül kell képviselnie. Jó gyakorlat, ha az összeférhetetlenség érdekében megfogalmazott elvárásokat belső szabályzatban rögzítik.

A bajor adatvédelmi biztos 2016 októberében nyilvánosságra hozott közleményében mutatott be egy olyan ügyet, amelyben az adatkezelő szervezet a tisztviselőre vonatkozó összeférhetetlenségi szabályokat szegte meg. A vonatkozó szabályok szerint azon szervezetek, amelyek a személyes adatok automatikus feldolgozása területén legalább tíz főt foglalkoztatnak, kötelesek adatvédelmi tisztviselőt kinevezni. A bajor hatósági álláspont kiemelte, hogy ha valakit erre a pozícióra kineveztek, akkor nem kaphat olyan feladatokat, amelyek a tisztviselői funkcióval konfliktust eredményezhetnek. Ilyen konfliktus és összeférhetetlenség áll fenn, ha a tisztviselő egyúttal IT vezető is a szervezetnél. Ebben az esetben ugyanis a tisztviselő nem tudja az adatvédelmi ellenőrző szerepét függetlenül ellátni, hiszen ilyenkor a saját munkáját kellene ellenőriznie. A tisztviselői feladattal összeegyeztethetetlen az adatkezelést érintő döntések meghozatala, illetve az ezekért viselt felelősség. Mindennek megfelelően azon szervezetek, amelyek adatvédelmi tisztviselő kinevezésére kötelesek, csak olyan személyt nevezhetnek ki, aki ezt a feladatát minden külső befolyás nélkül tudja ellátni. Azok a szervezetek pedig, amelyek ismételt felhívás ellenére sem tesznek eleget e kötelezettségüknek, szükségszerűen pénzbüntetéssel kell, hogy számoljanak a bajor hatóság közleménye szerint.

A jogeset kapcsán adódik a kérdés, vajon hasonló ügyekre és bírságokra lehet-e számítani a rendelet alkalmazása idején is? Bár a leírt eset a német (bajor) jog alapján ítélendő meg, a rendelet is a szankcionálandó mulasztások között említi az adatvédelmi tisztviselőre vonatkozó kötelezettségeket. Ennek megfelelően az adatvédelmi felügyeleti hatóságok a jövőben hasonló ügyeket a bajor példához viszonyítva ítélhetnek majd meg.

7.8. Az adatvédelmi tisztviselő feladatai – tanácsadás, ellenőrzés, kapcsolattartás

Minden adatvédelmi ügybe be kell vonni a tisztviselőt, méghozzá megfelelő időben. Nem választható el ez a rendelkezés a beépített adatvédelem elvétől, kellő időben és a folyamat kialakítása során nem túl későn kell az érdemi vélemény-nyilvánítást lehetővé tenni. A rendelet sok ponton tesz említést a kockázatokról, a tisztviselő is köteles az adatkezeléssel együtt járó, az érintettek helyzetére vonatkozó kockázatokra tekintettel végezni a munkáját.

Az adatvédelmi tisztviselő a jogszabályokról és azok alkalmazásához kapcsolódó kötelezettségekről tanácsot ad az adatkezelőnek és az alkalmazottainak.

Ellenőrzi a jogszabályoknak és a belső szabályoknak való megfelelést a személyes adatok kezelése terén. Feladata annak ellenőrzése, hogy a személyzet megfelelő adatvédelmi tudatossággal látja-e el tevékenységét, továbbá a képzést is ellenőrzi. Ezeken túl az úgynevezett kapcsolódó auditokat is ellenőrizheti. A tisztviselő tanácsot ad az előzetes adatvédelmi hatásvizsgálat során, és figyelemmel kíséri a hatásvizsgálat elvégzését.

Nevesített feladata a hatósággal való együttműködés, az előzetes adatvédelmi hatásvizsgálat kapcsán ő a kapcsolattartó a hatóság felé, és bármilyen adódó ügyben konzultációt folytathat a hatósággal. Abban, hogy kapcsolatba lép-e a hatósággal, szintén olyan kérdés, amiben nem adható neki utasítás, ebben a tekintetben a titoktartás nem akadályozhatja meg őt.

A Munkacsoport jó gyakorlatként javasolja, hogy a tisztviselőt a vezetői megbeszélésekre rendszeresen hívják meg. Ha bármilyen fórumon adatvédelmet is érintő döntést hoznak, a tisztviselő jelenléte kívánatos. Helyes gyakorlat, ha a szervezet azokban az esetekben, amikor nem követi a tisztviselő tanácsait, rögzíti, hogy ezt miért nem teszi.

Bármilyen incidens, így adatvédelmi incidens esetén javasolt azonnal konzultációt kezdeményezni a tisztviselővel. Szintén javasolt a szervezet adatvédelmi szabályaiban meghatározni, hogy mikor kötelező a tisztviselővel konzultálni. Mind a rendelet, mind az irányelv a hatósággal közlendő információk között említi a tisztviselő nevét és elérhetőségét.

7.8.1. A tisztviselő feladatai az adatvédelmi hatásvizsgálat kapcsán

A tisztviselő az adatkezelő kérésére szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, illetve nyomon követi annak elvégzését. Ha van kinevezett tisztviselő, őt az adatkezelő köteles bevonni. Ha az adatkezelő szervezet nem tisztviselőt, hanem adatvédelmi tanácsadót foglalkoztat (mert nem terheli a tisztviselő kinevezésének kötelezettsége), akkor az ő bevonása nem kötelező.

A Munkacsoport szerint a tisztviselő bevonása magában foglalja a tisztviselő részvételével annak mérlegelését, hogy el kell-e végezni a hatásvizsgálatot, milyen módszertan szerint tegyék ezt, házon belüli vagy külsős szereplők bevonásával történjen-e, milyen intézkedéseket kell tenni a kockázatok mérséklése érdekében, végül annak értékelését, hogy a hatásvizsgálatot helyesen hajtották-e végre, és annak eredménye a rendelettel összhangban van-e.

A hatásvizsgálattal összefüggő dokumentációnak része az ajánlás szerint annak bemutatása, ha a tisztviselő javaslatától eltértek.

7.8.2. Kötelező erejű vállalati szabályok és tisztviselők konferenciája

A kötelező erejű vállalati szabályok kapcsán a rendelet kötelező tartalmi elemként említi a kijelölt adatvédelmi tisztviselő feladatait.

A rendelet nem tesz említést az adatvédelmi tisztviselőkkel való szakmai kapcsolattartásról, rendszeres konferenciákról. Mivel az a magyar szabályozás, amely szerint a belső adatvédelmi felelősök konferenciáját az adatvédelmi hatóság évente egyszer összehívja, teljesen összeegyeztethető a rendelet szövegével és céljával, ez a fórum várhatóan továbbra is része lesz a magyar gyakorlatnak.

7.8.3. A rendelet 30. cikke szerinti nyilvántartás az adatkezelési tevékenységekről

A 30. cikk szerinti nyilvántartás nem tartozik a tisztviselő kötelező feladatai közé. Ennek ellenére megfontolandó, hogy ezt a feladatot a tisztviselő vállalja el. Egyrészt a regiszter vezetése már önmagában egyfajta ellenőrzést is jelent, másrészt ennek birtokában és felelőseként a tisztviselő igényt tarthat annak naprakészen tartására, szükség szerint kiegészítésére.

Az adatvédelmi nyilvántartás nem újdonság a magyar jogalkalmazó számára, ugyanis az Infotv. 24. (2) bekezdés e) pontja szerint a belső adatvédelmi felelős vezeti a belső adatvédelmi nyilvántartást. A nyilvántartás tartalmát az említett magyar jogszabály közelebbről nem határozza meg, azonban annak tartalma hozzávetőlegesen jól tervezhető, továbbá az egyelőre létező központi adatvédelmi nyilvántartáshoz hasonló, szervezeten belüli szerepe van, tehát annak felépítéséhez hasonló regisztert érdemes létrehozni.

Ilyen előzmények után a rendelet tárgyalt szabálya nem új és nem is éri meglepetésként a magyarországi adatkezelőket. Új elem ugyanakkor az adatfeldolgozókat terhelő nyilvántartási kötelezettség, amelynek tartalmát a rendelet szintén meghatározza. A nyilvántartás funkciója egyértelműen az elszámoltathatóság. A vonatkozó (82) preambulum bekezdés szerint az adatkezelő vagy az adatfeldolgozó a rendeletnek való megfelelés érdekében vezeti a nyilvántartást, a felügyeleti hatósággal való együttműködés keretében az adatkezelési műveletek ellenőrzése érdekében köteles azt hozzáférhetővé tenni.

A nyilvántartás egy belső feladat eredményeként jön létre, azonban annak tartalma egyértelműen az adatkezelővel való kapcsolatfelvételt is támogatja, hiszen tartalmaznia kell az adatkezelő nevét és elérhetőségét, továbbá az adatvédelmi tisztviselő nevét és elérhetőségét.

Ezeken túl azokat az információkat tartalmazza, amelyek az áttekinthetőség érdekében ésszerűen adódnak, így az adatkezelés célját, az érintettek kategóriáit és a kezelt személyes adatok kategóriáit, a címzettek kategóriáit, a törlés határidejét, az adatbiztonsági intézkedések általános leírását. Mindezeken túl a harmadik országba irányuló adattovábbítás esetén a címzetteket és az adatok védelmét szolgáló garanciákat is be kell mutatni.

Az adatfeldolgozó által vezetett nyilvántartás tartalma jellegében eltér az adatkezelő által vezetett regisztertől. Ez is tartalmazza ugyan az adatkezelő képviselőjének nevét és elérhetőségét, az adatvédelmi tisztviselő nevét és elérhetőségét, a harmadik országba irányuló adattovábbítás esetén a címzettet, valamint az adatok védelmét szolgáló garanciákat az adatfeldolgozónak is be kell mutatnia. Az adatkezelés egyes körülményeit azonban nem kell feltüntetnie, ami logikus is, hiszen azt az adatkezelő ismeri elsődlegesen, az adatfeldolgozó csupán az adatkezelő megbízása alapján lát el részfeladatokat. Ennek megfelelően csupán az adatkezelési tevékenységek kategóriáit kell megjelölnie. Itt is tetten érhető az elszámoltathatósági elvárás, hiszen ez már elegendő támpontot ad az érintett számára a felelősség tekintetében való tájékozódáshoz.

7.8.4. A nyilvántartás vezetése alóli mentesség és a kockázatalapú megközelítés

A nyilvántartás vezetésének kötelezettsége adminisztratív terhet ró az adatkezelőre. A jogalkotás során fontos szempont volt, hogy fölösleges adminisztratív feladatok ne nehezítsék a rendeletnek való megfelelést, azokat csupán a legszükségesebb mértékben szabad megállapítani. Ennek megfelelően figyelmet érdemel, hogy mely szereplők mentesülnek a nyilvántartási tevékenység alól.

A GDPR kapcsán akár közhelynek is tekinthető, de az adatvédelmi tisztviselőnek is a kockázatok figyelembe vételével kell tevékenységét elvégeznie. Ez nem azt jelenti, hogy bizonyos területeket elhanyagolhat, de azt jelenti, hogy a kockázatokkal arányosan kíséri figyelemmel az adatkezelési műveleteket, illetve a hangsúlyos területeken kell elsősorban az adatkezelő rendelkezésére állnia tanácsaival.

A rendelet (75) preambulum bekezdése a kockázatokról részletes listát ad. Ha ezek a kockázatok valószínűsíthetően együtt járnak az adatkezeléssel, akkor még a kis- és középvállalatok számára nyújtott kivétel szabály (250 főnél kevesebb személyt foglalkoztató szervezet) sem alkalmazható. A valószínűsíthető kockázatok kapcsán mindenképpen rendszerszintű problémák jönnek szóba. Semmilyen külső vagy belső szabályozás nem képes kiszűrni az egyéni jogsértéseket, mindazonáltal ezekre is kell gondolni, amikor a garanciákat kialakítják. Ha tehát a kkv kategória alá eső szervezet megfelelő garanciákat alkalmaz a kockázatok megelőzésére, élhet a rendelet által kínált kivételszabállyal, és nem kötelező az adatkezelési tevékenységeiről részletes nyilvántartást vezetni.

Nagyobb szervezetek csak akkor mentesülhetnek, ha az adatkezelés alkalmi jellegű. Ennek meghatározására nézve a rendelet nem nyújt további támpontot.

A személyes adatok különleges kategóriáinak kezelése esetében minden adatkezelő köteles a nyilvántartást vezetni, sem a kkv minőség, sem az alkalmi jelleg nem nyújt felmentést e kötelezettség alól.

A 29-es Munkacsoport a GDPR alkalmazandóvá válását megelőzően már úgy foglalt állást, hogy a 250 főnél kevesebb személyt foglalkoztató adatkezelő csak az adatkezelési típusokról köteles nyilvántartást vezetni a 30. cikk (5) bekezdése alapján. Ez jelentős adminisztratív könnyítést jelent a szektor számára.

A nyilvántartás tehát a rendeletnek megfelelő adatkezelés egyik garanciája, amely annak elérhetősége révén az elszámoltathatóságot erősíti.

7.9. Az adatvédelmi tisztviselő az Infotv. szabályaiban

Az adatvédelmi tisztviselő alkalmazásának, feladatkörének Infotv.-beli szabályozása nagyjából megfeleltethető annak, ahogyan a GDPR 37.-39. cikkei az adatvédelmi tisztviselő (pontosabban a közhatalmi, vagy egyéb közfeladatot ellátó szervnél kijelölt adatvédelmi tisztviselő) jogállását és feladatait szabályozzák. A GDPR párhuzamos szabályai kapcsán írtak megismétlése nélkül elég a következő eltérésekre rámutatni:

1. A GDPR 38. cikk (3) bekezdése erős garanciákkal biztosítja az adatvédelmi tisztviselő szervezeten belüli függetlenségét, amennyiben előírja annak biztosítását, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.

Az Infotv. utal ugyan arra, hogy az adatvédelmi tisztviselőt fel kell ruházni a feladatai ellátáshoz szükséges erőforrásokkal és jogkörökkel, nem tartalmaz a fentiekhez hasonlóan részletes garanciális szabályozást. A törvényalkotó feltehetőleg azt tartotta szem előtt, hogy az Infotv. hatálya alá tartozó bűnügyi, honvédelmi és nemzetbiztonsági célú adatkezelések esetében olyan hierarchikus szervezeti viszonyok között történik a feladatellátás, amelyektől idegen lenne a GDPR 38. cikk (3) bekezdésében meghatározottakhoz hasonlóan részletezett jogállási szabályok alkalmazása. Ugyanakkor úgy véljük, hogy az adatvédelmi tisztviselő munkájának eredményességéhez nélkülözhetetlen legalább annyi szervezeten belüli függetlenség, hogy

- feladatainak ellátása során ne legyen utasítható, továbbá
- észrevételeit és javaslatait közvetlenül a legfelső vezetési szint elé tárhassa,

ezért kívánatos legalább ennyit belefoglalni azoknak az Infotv. hatálya alá tartozó szervezeteknek a belső normáiba (például Szervezeti és Működési Szabályzat, Ügyrend), amelyeknél adatvédelmi tisztviselőt alkalmaznak.

2. Az Infotv. külön nevesíti az adatvédelmi tisztviselő azon feladatát, hogy közreműködik a belső adatvédelmi és adatbiztonsági szabályzat megalkotásában.

3. Az adatkezelő, illetve az adatfeldolgozó tájékoztatja a Hatóságot az adatvédelmi tisztviselő nevéről, postai és elektronikus levélcíméről, ezen adatok változásáról, valamint ezen adatokat nyilvánosságra hozza. A Hatóság évente legalább egyszer a szakmai kapcsolattartás céljából konferenciára hívja össze az adatvédelmi tisztvisdelőket.

4. Az Infotv. titoktartási kötelezettséget ír elő az adatvédelmi tisztviselő számára a tevékenységével, annak ellátásával kapcsolatban tudomására jutott személyes adatot, minősített adatot, illetve törvény által védett titoknak és hivatás gyakorlásához kötött titoknak minősülő adatot, valamint minden olyan adatot, tényt vagy körülményt illetően, amelyet az őt alkalmazó adatkezelő vagy adatfeldolgozó nem köteles törvény előírásai szerint a nyilvánosság számára hozzáférhetővé tenni. A titoktartási kötelezettség a jogviszony megszűnését követően is fennmarad.

7.10. Összegzés

Az adatvédelmi tisztviselők az adatvédelmi előírásoknak való megfelelés terén jelentős és szerteágazó feladatokat fognak ellátni. A bemutatott szabályok alapján jól látható, hogy munkájuk sok téren európai, illetve globális keretek közé kerül, ezért is fontos a felkészültségük, folyamatos képzésük. Kívánatos, hogy Magyarországon is erősödjön az adatvédelmi tisztviselők közötti együttműködés, a hasznos információk megosztásának fórumai tovább épüljenek. Mindezek hozzájárulnak ahhoz, hogy a rendelet alatti intézményrendszer fontos szereplőivé váljanak az adatvédelmi tisztviselők, az adatkezelő szervezetekkel való együttműködésükben erősítve a jogbiztonságot, az adatalanyokkal való kapcsolataikban pedig a hatékony jogérvényesítést.

8. JOGSZABÁLYTÁR

1. Magyarország Alaptörvénye
2. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [Infotv.]
3. az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről [általános adatvédelmi rendelet, GDPR]
4. az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

9. IRODALOMJEGYZÉK

1. A 29-es Munkacsoport 1/2010. számú WP 169-es véleménye az „adatkezelő” és az „adatfeldolgozó” fogalmáról; URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (utolsó letöltés: 2018.08.23.)
2. A 29-es cikk szerinti munkacsoport állásfoglalása a GDPR 30. cikk (5) bekezdésében foglalt adatkezelési tevékenységekre vonatkozó nyilvántartási kötelezettségektől való eltérésekről; URL: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422 (utolsó letöltés: 2018.08.23.)
3. Information Commissioner’s Office: Data controllers and data processors 20140506; elérési út: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf (utolsó letöltés: 2018.08.23.)
4. Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e (WP 248); URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 (utolsó letöltés: 2018.08.23.)
5. Iránymutatás az adatvédelmi incidensek (EU) 2016/679 rendelet szerinti bejelentésről (WP 250); URL: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 (utolsó letöltés: 2018.08.23.)
6. Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban (WP243); URL: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100 (utolsó letöltés: 2018.08.23.)
7. Szabó Endre Győző: Az Európai Unió általános adatvédelmi rendeletének egyes kérdéseiről II. Beépített és alapértelmezett adatvédelem, adatvédelmi incidensek bejelentése., Pázmány Law Working Papers, 2016/27, URL: http://plwp.eu/docs/wp/2016/2016-27_Szabo.pdf (utolsó letöltés: 2018.08.23.)
8. Szabó Endre Győző: Az adatvédelmi tisztviselőről – A GDPR szabályainak elemzése, Infokommunikáció és Jog XV. évfolyam 70. szám 2018/1.; 3–10. o.
9. 3/2010 vélemény az elszámoltathatóság elvéről (WP 173); URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (utolsó letöltés: 2018.08.23.)

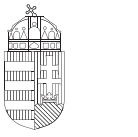
A Nemzeti Közszolgálati Egyetem kiadványa.

Nemzeti Közszolgálati Egyetem;
Államtudományi és Közigazgatási Kar
www.uni-nke.hu

Felelős Kiadó:
Prof. Dr. Kis Norbert Dékán
Címe:
1083 Budapest, Üllői út 82.
Kiadói szerkesztő:
Kiss Eszter
Tördelőszerkesztő:
Bödecs László

978-615-5870-97-2 (PDF)

A kiadvány
a KÖFOP-2.1.1-VEKOP-15-2016-00001
„A közszolgáltatás komplex kompetencia,
életpálya-program és oktatás technológiai
fejlesztése” című projekt keretében készült
el és jelent meg.



MAGYARORSZÁG
KORMÁNYA

Európai Unió
Európai Szociális
Alap

BEFEKTETÉS A JÖVŐBE