Dr. Boros Anita
ELTE ÁJK Polgári Jogi Tanszék
Témavezető: dr. Balogh Zsolt György egyetemi docens, Budapesti Corvinus Egyetem, Gazdálkodástudományi Kar, Infokommunikációs Tanszék

DOI: 10.55052/themis.2022.2.6.32

Az adatvédelmi tisztviselő mint az elszámoltathatóság sarokköve

I. Bevezetés

A 2018. május 25-én hatályba lépett európai uniós általános adatvédelmi rendelet (a továbbiakban: GDPR) biztosítja az európai adatvédelem modernizált, elszámoltathatóságon alapuló megfelelőségi keretét.

Az adatvédelmi tisztviselők sok szervezetben ezen új jogi keret középpontjában állnak, és megkönnyítik a GDPR rendelkezéseinek való megfelelést. Így az elszámoltathatóság eszközeinek (például az adatvédelmi hatásvizsgálatok megkönnyítése, auditok végzése vagy elősegítése) végrehajtása mellett az adatvédelmi tisztviselők közvetítő szerepet töltenek be az érdekelt felek (például a felügyeleti hatóságok, az érintettek és a szervezeten belüli részlegek) között.

A GDPR elfogadását megelőzően az adatvédelmi munkacsoport arra hivatkozott, hogy az adatvédelmi tisztviselő az elszámoltathatóság sarokköve, és az adatvédelmi tisztviselő kijelölése elősegítheti a jogszabályoknak való megfelelést, továbbá versenyelőnyt jelenthet a vállalkozások számára. [1]

E kijelentésből kiindulva, az alábbi tanulmányban vizsgálni fogjuk az adatvédelmi tisztviselő kinevezése (GDPR 37. cikk) és az elszámoltathatóság elvének való megfelelés (GDPR 5. cikk (2) bekezdés) közötti kapcsolatot és kölcsönhatást, amelynek tisztázása kiemelkedő fontossággal bír az adatvédelmi vállalati megfelelés során.

[1] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 5.

Elemzésünk első felében meghatározzuk az elszámoltathathatóság fogalmát, eszközeit és betartásának előnyeit, majd körbejárjuk az adatvédelmi tisztviselő szerepét a vállalati megfelelésben, arra keresve a választ, hogy az adatvédelmi tisztviselő jelenléte a vállalati struktúrában hogyan segíti elő az elszámoltathatóság követelményeinek való megfelelést. Elemzésünk során alapvetően a GDPR normaszövegére, a vonatkozó preambulumbekezdésekre, mint értelmező rendelkezésekre támaszkodunk, majd az egyes értelmezési kérdésekben hivatkozni fogunk a 29. cikk szerint működő adatvédelmi munkacsoport iránymutatásaira is. Továbbá, megemlítünk néhány olyan adatvédelmi hatóság által kiszabott bírságot, amelyek relevánsak e témában.

II. Az elszámoltathatóság fogalma

Míg az etika és a kormányzás terén az elszámoltathatóság fogalma a felelősségvállalási és a számadási kötelezettségben merül ki, a szervezeti vezetői szerepekben az elszámoltathatóság az intézkedések, a döntések és a politikák iránti felelősség vállalása.[2] Az adatvédelem világán kívül is létezik néhány példa az elszámoltathatóság elvére. Ezek olyan megfelelési rendszerek, amelyek konkrétan meghatározzák az adatkezelőnek a jogszabályi előírásoknak történő megfelelést szolgáló politikáit és eljárásait. Ilyenek például a pénzügyi szolgáltatásokról szóló jogszabályok. Más esetekben csak ajánlott, de nem kötelező rendelkezni megfelelési programmal, mint például a versenyjog terén.[3]

Az adatvédelmi megfelelés területén az „elszámoltathatóság" (accountability) mint fogalom, mely az angolszász világból származik, magába foglalja egyrészt, hogy az adatkezeléssel kapcsolatban hogyan érvényesül az adatkezelő felelőssége, másrészt pedig, hogy ez hogyan bizonyítható. A felelősség és az elszámoltathatóság egyazon érme két oldala. Ez nem jelent mást, minthogy az adatkezelőnek az adatkezelés megtervezésétől, az adatkezelés megvalósításán keresztül egészen az adatok törléséig vagy az adatkezelés megszűnéséig, figyelnie kell, hogy bármikor bizonyítani tudja, hogy a hatályos rendelkezéseknek eleget tesz. Az elszámoltathatósági elv célja, hogy megerősítse és növelje az adatkezelők felelősségét a személyes adatok kezelése során. Ennek

[2] Christopher 2006, 5.
[3] A 29. cikk szerinti adatvédelmi munkacsoport 3/2010 véleménye az elszámoltathatóság elvéről, 7.

alapján, valamennyi a rendeletben megfogalmazott kötelezettség teljesítését, az elszámoltathatóság szemszögéből kell megközelíteni.[4]

Az elv bevezetését az európai adatvédelmi szabályozásba a 29. cikk szerinti adatvédelmi munkacsoport is szorgalmazta. A 3/2010 számú véleménye alapján *„az általános adatvédelmi elveket konkrét, az adatkezelő szintjén meghatározott politikákra és eljárásokra fordítaná le."* Ezáltal az adatvédelem sokkal gyakorlatiasabban és hatékonyabban tud működni. Ugyancsak e vélemény hangsúlyozza azt is, hogy az elszámoltathatóságra vonatkozó új rendelkezés *„nem irányul arra, hogy az adatkezelőket újabb elveknek vesse alá, hanem a már létezőknek történő valós, hatékony megfelelést biztosítja."*

III. Az elszámoltathatóság elemei

Az elszámoltathatóság elvének való megfelelés átfogó megközelítést igényel, amely egy sor kulcsfontosságú elemet magában foglal.

A megfelelés részeként az adatkezelőnek szükséges folyamatosan figyelemmel kísérni a vállalati tevékenységeket, hogy azok érintenek-e személyes adatokat. Ha igen, akkor megfelelő intézkedéseket kell arra rendszeresítenie, hogy az adatvédelmi megfelelést ellenőrizze és naprakészen tartsa, és nem utolsó sorban mindezeket dokumentálnia szükséges.

A GDPR 5. cikk (2) bekezdése értelmében tehát az elszámoltathatóság legfontosabb eleme, hogy az adatkezelő és az adatfeldolgozó felelősséget vállaljon az általa végzett adatkezelésért. 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 jelentő, 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 adatkezelési tevékenységet tekintve arányos, ennek részeként az adatkezelő megfelelő belső adatvédelmi szabályokat is alkalmaz.[5]

[4] Árvai 2018, 5-7.
[5] Ibidem

Ez nem jelent mást, mint hogy az adatkezelőnk az intézkedéseit a szervezetük konkrét sajátosságaihoz és a kérdéses adatkezelési műveletekhez kell igazítania. Az elszámoltathatóság elve alapján megkövetelt technikai és szervezeti intézkedéseknek a 24. cikkben meghatározott két tényezőre, nevezetesen az adatfeldolgozás jellegére, valamint a kockázat valószínűségére és súlyosságára tekintettel megfelelőnek kell lenniük.

A természetes személyek jogait és szabadságait veszélyeztető kockázatok a GDPR (75) preambulumbekezdése alapján a következőkből származhatnak:

- olyan személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat;
- az olyan adatkezelésekből, amelyek következtében az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett;
- olyan személyes adatok kezeléséből, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak;
- az olyan adatkezelésekből, melyek esetén személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes p referenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából;
- ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor;
- ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki.

A kockázat valószínűségét és súlyosságát minden esetben az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni. A kockázatot felmérése mindig objektív

értékelés alapján történik, amelynek során szükséges megállapítani, hogy az adatkezelési műveletek kockázattal, illetve nagy kockázattal járnak-e.[6]

Továbbá a „megfelelő” szó az elszámoltathatóság skálázhatóságára utal, ami lehetővé teszi az adatkezelő számára, hogy figyelembe véve többek között a szervezet típusát, legyen az nagy vagy kicsi, valamint a személyes adatok típusát, jellegét és összességét, ő maga döntse el, hogy éppen milyen intézkedések alkalmazása szükség.[7]

A szervezeti intézkedések közé tartozik egyrészt az adatvédelmi megfelelést igazoló dokumentáció fenntartása. A rendelet számos ilyen dokumentáció fenntartásáról tesz említést, mint például adatkezelési műveletek nyilvántartása, az adatvédelmi incidensek nyilvántartása vagy az adatvédelmi hatásvizsgálat dokumentálása. A dokumentáció szempontjából szintén fontos az adatkezelési tájékoztatók elkészítése, a belső adatkezelési szabályzatok, az adatfeldolgozói szerződésnek az adatvédelmi kitételei vagy mellékletei, mint ahogy az adattovábbításokkal kapcsolatos adatvédelmi garanciák, szerződéses kikötések beiktatása is. Ugyancsak a dokumentálási követelményekhez tartozik az érdekmérlegelési tesztek eredményeinek rögzítése, a megfelelő belső szabályzatok elkészítése, amelyek – a fent említetteken túl – szólhatnak a megőrzésről vagy az informatikai biztonságról. Ugyancsak dokumentálandó az érintetti megkeresések, az arra adott válaszok, a munkahelyi eszközök használata, a személyzet megfigyelésének szabályozása és az adatkezelő belső adatvédelmi tréningjei is.[8]

A fent említett dokumentáció elkészítése mellett szervezeti intézkedések végrehajtása is szükséges. Ilyen például: az adatvédelmi projekt vezetése és felügyelete; az adatvédelmi tisztviselő kinevezése; a kockázatfelmérés (beleértve a hatásvizsgálatot); az adatfeldolgozók gondos kiválasztása; az átláthatóság biztosítása; a képzés és tudatosság növelése a szervezeten belül; az ellenőrzés; a válaszadás, a panaszkezelés és a végrehajtás. Ezek mind olyan intézkedések, amelyeket vagy a törvény, egy adott tanúsítvány vagy magatartási kódex szabályai írhatnak elő, vagy a szervezet hatékonyabb működése céljából szükségesek. De mindegyik esetben átfogó adatvédelmi vállalatirányítási rendszert képeznek, ami nemcsak a legalapvetőbb szinten biztosítja a vonatkozó szabályok betartását, de széles körű további előnyökkel is járhat a szervezet és más érdekelt felek számára is, különösen akkor, ha

[6] GDPR (76) preambulumbekezdés
[7] Kuner 2020, 562.
[8] Ibidem 6.

az elszámoltathatósági intézkedések túllépnek a törvényben előírt minimális kereteken.[9]

A megfelelő technikai intézkedések pontos tartalmának és eszközeinek meghatározása szintén az adatkezelő feladata. A rendeletben fellelhető néhány ilyen intézkedés mellett, gyakorlati szempontból az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (ENISA) ajánlása is segítséget nyújthat, ami felsorol néhány adatvédelmi tervezési stratégiát.[10] Az első négy stratégia magára az adatkezelésre, adattárolásra vonatkozik, majd a következő négy általános alapelvet fogalmazza meg. Ezek a következőek:

1. Adatminimalizáció

Az adatminimalizáció szorosan összefügg az adattakarékosság elvével, mely szerint a kezelt adatok csak a célhoz szükséges megfelelő, releváns, korlátozott mértékben gyűjthetőek. Esetenként egyéni vizsgálatra van szükség, ami alapján megállapítható, mely adatok feltétlenül szükségesek a cél teljesítése érdekében.

2. Titkosítás

A titkosítás az egyik legmegbízhatóbb adatvédelmi módszer, különösen bizalmas vagy kényes adatok esetén, amit a GDPR 32. cikk (1) bekezdésének a) pontja is megemlít. Ez a stratégia magába foglalja mind az információ átvitelekor történő titkosítási eljárásokat (kódolt üzenetek, titkos nyelvezet használata stb.), mind az anonimizálás és álnevesítés eszközeinek használatát. Fontos szempont és elvárás az anonimizációval során, hogy a kapcsolat ne legyen többé helyreállítható. Ez elsőre talán egyszerűnek tűnik, viszont a fejlődő technológiának köszönhetően nem egyszerű feladat az adat és a természetes személy közötti kapcsolat végérvényes megszüntetése.

3. Szétválasztás

A harmadik tervezési stratégia a szétválasztás, melynek lényege, hogy a gyűjtött személyes adatokat különálló részekre kell tagolni és ezeket, amikor csak lehetséges, külön adatbázisokban kell tárolni. Ezáltal kiküszöbölhető a profilalkotás lehetősége.[11]

4. Összesített, aggregált adatok használata

---

[9] Markus Heyder, Sam Grogan, 'The role of DPAs in incentivizing accountability', www.iapp.org/news/a/the-role-of-dpas-in-incentivizing-accountability/?fbclid=IwAR1FrLNz7Rv9Te-MRFFXSZvy-vJf9hiE_vtxCSzLwcoXPAt554rslOr0evs (2022.05.23.)

[10] European Union Agency for Network and Information Security (ENISA), 'Privacy and Data Protection by Design– from policy to engineering', 18-22. www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport , (2022.05.23.)

[11] Ibidem, 18-22.

Az aggregáció esetén, olyan egymástól különálló adatelemek vagy részek csoportosítása vagy összekapcsolása történik, amelyek önmagukban nem képesek az egyén azonosítására, viszont a kívánt cél eléréséhez (többnyire statisztikai elemzések végrehajtásához) elegendő információt nyújtanak. A rendelet szerint *"a statisztikai célú adatkezelés eredménye nem személyes adat, hanem összesített [aggregált] adat, ha ezt az eredményt vagy a személyes adatokat nem használják fel konkrét természetes személyekre vonatkozó intézkedések vagy döntések alátámasztására."* [12]

5. Tájékoztatás

Bármely adatkezelési művelet során fontos figyelembe venni a transzparencia elvét, és biztosítani az érintettek megfelelő tájékoztatását. 12. cikk szerinti tájékoztatás követelményei a következőek: tömör, átlátható, érthető és könnyen hozzáférhető forma tiszteletben tartása. Figyelni kell, hogy a közölni kívánt információ eredményesen célba érjen. Éppen ezért a tájékoztatónak minden más általános szerződési feltételtől vagy bármilyen más információtól különállónak kell lennie.

6. Átláthatóság

Biztosítani kell továbbá, hogy az érintettek rendelkezhessenek az adataik felett. Ez a stratégia nagymértékben összefügg az átláthatóság elvével és a tájékoztatási kötelezettséggel. Az érintettek adatok feletti rendelkezésének biztosítása a rendeletben feltüntetett érintetti jogok tiszteletben tartásán is túlmutat, hiszen az azt is jelenti, hogy a felhasználók eldönthetik, hogy egy bizonyos rendszert használnak-e, ha igen a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogyan tekintenek bele vagy milyen egyéb módon kezelik, abba milyen adatokat és milyen céllal gyűjtenek.

7-8. Végrehajtás és elszámoltathatóság

Végezetül a 7. és 8. stratégia szorosan kapcsolódik egymáshoz, és a beépített adatvédelem alapját képezik. Ezek a végrehajtás és az elszámoltathatóság, melyek megkövetelik olyan technikai és szervezeti politikák implementálását, amelyek mind a rendelet alapelveit, mind az érintettek adatkezeléssel kapcsolatos jogait tiszteletben tartják.

Fontos kiemelni, hogy a rendelet nem határozza meg pontosan a bizonyítás eszközeit. Legtöbb esetben ennek kiválasztását az adatkezelőre bízza. Ugyanakkor mindegy ajánlásként a rendeletben több helyen is megjelenik a jóváhagyott magatartási kódexekhez vagy jóváhagyott tanúsítási mechanizmushoz való csatlakozás a bizonyítás eszközeként.

[12] GDPR (162) preambulumbekezdés

Ilyen például a 24 cikk (3) bekezdése, mely szerint a 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti kötelezettségeit. A 32. cikk (3) bekezdése alapján ezen tanúsítási mechanizmusokhoz való csatlakozással az adatbiztonsági kötelezettségek betartását is bizonyítani lehet. A 25. cikk (3) bekezdése alapján a 42. cikk szerinti jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy az adatkezelő a beépített és alapértelmezett adatvédelem követelményeinek eleget tesz.

A (77) preambulumbekezdés megemlíti ugyanakkor, hogy *„a megfelelő intézkedéseknek az adatkezelő vagy adatfeldolgozó általi végrehajtásához, valamint a megfelelés általuk való bizonyításához, 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.”*

A gyakorlatban a megfelelés bizonyítására szolgáló eszköz mindig az adatkezelés jellegétől fog függeni. Az ebből eredő, a megfelelés biztosítása érdekében hozott megfelelő intézkedések bizonyításának szükségessége nagyban megkönnyíti az alkalmazandó szabályok végrehajtását.

IV. Az elszámoltathatóság előnyei

Az első és legfontosabb előny az elszámoltathatóság elismerése az adatvédelmi bírságok kiszabása esetén. Alapvetően a rendelet nem tesz különbséget multinacionális vállalatok, KKV-k, intézmények vagy egyéb szervezetek, sőt magánszemélyek között, így az egyéni vállalkozókat is ugyanazok a kötelezettségek terhelik, mint a nagyobb adatkezelőket. Sőt mi több, a felügyeleti hatóságok különböző szankciókat alkalmazhatnak a jogszabály rendelkezéseinek nem felelő betartásával szemben és bírságot is kiszabhatnak rájuk, melynek mértéke szintén nem az adatkezelő vagy adatfeldolgozó méretétől vagy az adatkezelés mértékétől függ. A 29. cikk alapján létrehozott adatvédelmi munkacsoport 2017. október 3-án

iránymutatást adott ki a bírság alkalmazásáról,[13] ami a felügyeleti hatóságok számára ad iránymutatást a bírság kiszabásával kapcsolatban. Ez alapján a felügyeleti hatóságnak egyenként kell azonosítania és értékelnie a jogsértéseket és a leginkább megfelelő korrekciós intézkedést (szankciót) kell alkalmaznia, figyelembe véve, többek között az adatkezelő vagy az adatfeldolgozó felelősségének mértékét, tekintettel az általa foganatosított technikai és szervezési intézkedésekre.[14] E véleményből kitűnik, hogy az elszámoltathatóság elvének való megfelelés enyhítő körülménynek tekinthető egy esetleges bírság kiszabása esetén.

További előnyt jelenthet multinacionális cégeknél az elszámoltathatóság magas szintjének biztosítása, ami lehetővé teszi továbbá a vállalaton belüli globális harmonizáció előmozdítását és az interoperabilitás és a globális adatáramlás megkönnyítését is.

Nem elhanyagolható következmény az sem, hogy egy megfelelő adatvédelmi vállalatirányítási rendszer kialakítása hasznos eszközként szolgál az adatvédelmi szempontból biztonságos adatfeldolgozók kiválasztásakor.

Nem utolsó sorban az elszámoltathatóság végrehajtása nemcsak a vállalatok, hanem az érintett magánszemélyek javát is szolgálja, hiszen biztonságossá és ellenőrizhetővé válik a személyes adataik kezelése, így az adatkezelők és adatfeldolgozók iránt megnő a vevői, fogyasztói bizalom. Ugyanis ezen intézkedések betartása garantálja, hogy a vállalkozás nem él vissza a személyes adataikkal.[15]

Láthatjuk tehát, hogy az elszámoltathatóság elvének való magas szintű megfelelés számos előnnyel járhat bármely vállalkozás számára, de ennek költségei egyáltalán nem elhanyagolható mértékűek. Így nem meglepő, hogy a kis- és középvállalkozások többsége a törvényben meghatározott minimum követelményeknek igyekszik eleget tenni.

V. Az adatvédelmi tisztviselő fogalma. Jogfejlődés

[13] A 29. cikk szerinti adatvédelmi munkacsorport: Iránymutatás az automatizált döntéshozatallal és a profilalkotással kapcsolatban a 2016/679 rendelet alkalmazásához

[14] Markus Heyder, *op.cit.*

[15] Center for Information Policy Leadership, The Central Role of Organisational Accountability in Data Protection Discussion Paper 2 (of 2), Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf., (2022.05.23.)

Az adatvédelmi tisztviselő fogalma (angolul: *Data protection officer*) amerikai nagyvállalatoknál már nagyon régóta jelen van a vállalati kultúrában. A *„privacy officer", „chief privacy officer*" egy adott szervezeten belül olyan munkatárs, akinek feladata az adatvédelmi szabályok ismerete és a belső folyamatok felügyeletét jelenti.[16] Ugyanakkor az adatvédelmi tisztviselő intézménye Magyarországon sem minősül újdonságnak.[17] Már az Infotörvény is tartalmazott iránymutatásokat azzal kapcsolatban, hogy ki lehet adatvédelmi felelős és annak milyen feladatokat kell ellátnia.[18]

A GDPR 37. cikkében fellelhető adatvédelmi tisztviselőre vonatkozó rendelkezéseket részben az adatvédelmi irányelv[19] 18. cikkének (2) bekezdése inspirálta, amely szerint az adatvédelmi tisztviselő kijelölése nem volt kötelező, csupán feltétele volt annak, hogy az adatkezelő mentesüljön az adatkezelési tevékenységének a felügyelő hatóság felé történő értesítési kötelezettség alól vagy az értesítést egyszerűbb formában végezhesse.

Ebben az esetben az adatvédelmi tisztviselő szerepét és feladatait az adatvédelmi irányelv 18. cikke határozta meg, amely szerint az adatvédelmi tisztviselő felelt az irányelv alapján elfogadott nemzeti rendelkezések belső alkalmazásának független biztosításáért, valamint az adatkezelő által végzett adatfeldolgozási műveletek nyilvántartásának vezetéséért is.

Az irányelv emellett megemlítette az adatvédelmi tisztviselők függetlenségének szükségességét, és a (49) preambulumbekezdése is kijelentette: *„az adatvédelmi tisztviselőt, függetlenül attól, hogy az adatkezelő alkalmazottja-e vagy sem, olyan hatáskörrel kell felruházni, hogy feladatát teljesen függetlenül gyakorolhassa."*

Ezen túlmenően az adatvédelmi tisztviselőre vonatkozó rendelkezéseket alapvetően az Európai Parlement és a Tanács 2000. december 18-i 45/2001. EK rendelete ihlette, amely előírta az adatvédelmi tisztviselő kötelező kinevezését az EU minden közösségi intézménye és szerve számára.

A 45/2001. EK rendelet meghatározta továbbá az adatvédelmi tisztviselő feladatait is, amelyeket az adatvédelmi rendelet is átvett. Ilyen

[16] Justine Brown, *Rise of the Chief Privacy Officer*, Government Technology , https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html, (2022.05.23.)

[17] Péterfalvi, Révész, Buzás 2018, 245.

[18] Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) 2018. VII. 25. előtt hatályos 24. §-a

[19] Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, 18. cikk és (49) preambulumbekezdés

például: tájékoztatja az adatkezelőket és az adatok jogosultjait azok jogaikról és kötelezettségeikről; válaszol az európai adatvédelmi biztos megkereséseire, és együttműködik az európai adatvédelmi biztossal; független módon biztosítja a rendelet rendelkezéseinek belső alkalmazását; vezeti az adatkezelő által végzett adatfeldolgozási műveletek nyilvántartását.[20]

VI. Kinevezési kötelezettség a GDPR szerint

Az adatvédelmi megfelelés során a szervezetek számára fontos kérdés annak meghatározása, hogy szükségük van-e adatvédelmi tisztviselőre. A GDPR értelmében bizonyos adatkezelők és adatfeldolgozók kötelesek adatvédelmi tisztviselőt kijelölni.

Ez a kötelezettség kiterjed minden közhatalmi szervre vagy egyéb, közfeladatot ellátó szervre (függetlenül attól, milyen adatokat dolgoz fel), valamint egyéb olyan szervezetekre, amelyek fő tevékenysége az egyének szisztematikus, nagymértékű megfigyelése, vagy amelyek a személyes adatok különleges kategóriáit nagy számban kezelik.

Abban az esetben, ha a szervezet nem teljesíti a GDPR által meghatározott kritériumokat, bizonyos esetekben hasznosnak bizonyulhat, ha önkéntes alapon jelölnek ki adatvédelmi tisztviselőt. Mivel az adatkezelők számára sok esetben nem követhető, mily módon történik az egyének személyes adatainak kezelése, így fontos olyan független adatvédelmi tisztviselő jelenléte, aki kívülről szemlélve belelát az adatkezelési folyamatokba és szakértői szemmel képes irányítani az adatvédelmi megfelelést.

A GDPR értelmében az adatvédelmi tisztviselő (DPO) kinevezése tehát nem kötelező, kivéve, ha a meghatározott feltételek fennállnak, illetve ha a szervezet úgy dönt, hogy érdekében áll e pozíció betöltése. A GDPR nem ír elő határidőt a DPO kijelölésére, de a felügyeleti hatósághoz való bejelentés minden esetben szükséges.

A Rendelet 37. cikke alapján az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt köteles kijelölni, amennyiben:

[20] Az Európai Parlament és a Tanács 45/2001/EK rendelete a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, 24. cikk

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;

A GDPR nem határozza meg a „közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv" fogalmát. E fogalom meghatározásban a 29. cikke szerint létrehozott adatvédelmi munkacsoport az adatvédelmi tisztviselőkkel kapcsolatban kibocsátott 243. számú iránymutatása nyújt segítséget. A munkacsoport állásfoglalása alapján e fogalmat elsősorban a nemzeti jog hivatott meghatározni, továbbá kiemeli, hogy a közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv fogalma magában foglalja az országos, regionális és helyi hatóságokat és a közjog hatálya alá tartozó más szerveket is. Ilyenek többek között a tömegközlekedés, a víz és energiaellátás, a közúti infrastruktúra, vagy a közszolgálati műsorszolgáltatás terén működő természetes vagy jogi személyek, amelynél az adatvédelmi tisztviselő kijelölése kötelező.[21]

Ami a nemzeti szabályozást illeti, az Infotv. a közfeladat ellátásának a funkcióját tekinti feltételnek az adatvédelmi tisztviselő kijelöléséhez. A 25/L.§ (1) bekezdés a) pontja kijelenti: "*Az adatkezelő és az adatfeldolgozó a személyes adatok kezelésére vonatkozó jogi előírások teljesítésének és az érintettek jogai érvényesülésének elősegítése érdekében adatvédelmi tisztviselőt alkalmaz, ha az adatkezelő, illetve az adatfeldolgozó állami feladatot vagy jogszabályban meghatározott egyéb közfeladatot lát el - kivéve a bíróságokat (…)"*

A Nemzeti Adatvédelmi és Információszabadság Hatóság álláspontja szerint a magyar jogalkotó egyértelműen feladatközpontúan rendeli alkalmazni a közhatalom gyakorlását, nem pedig szervhez, személyhez rendelve, amely alapján az adatvédelmi tisztviselő kijelölésére vonatkozó kötelezettség a közhatalom gyakorlásának, mint feladatnak, hatáskörnek a címzettjét terheli.[22]

Az igazságszolgáltatási feladatkörükben eljáró bíróságok az igazságszolgáltatás függetlenségének általános elve alapján mentesülnek az adatvédelmi tisztviselő kötelező kijelölése alól, amit a GDPR 55. cikk (3) bekezdése, valamint 20 preambulumbekezdés fogalmaz meg.

Ez alapján továbbá *„lehetővé kell tenni, hogy az ilyen adatkezelési műveletek felügyeletével a tagállamok igazságügyi rendszerén belül olyan szakosodott szerveket bízzanak meg, amelyek elsősorban biztosítják az e rendeletben foglalt szabályoknak való megfelelést, növelik a bírói kar*

[21] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 7.

[22] NAIH/2020/2870

tudatosságát az e rendelet szerinti kötelezettségeik tekintetében és kezelik az említett adatkezelési tevékenységgel kapcsolatos panaszokat."

Így a fent említett szervek is önkéntesen bármikor kijelölhetnek adatvédelmi tisztviselőt.

Nem utolsó sorban a 37. cikk (4) bekezdésével összhangban az uniós vagy tagállami jog emellett olyan jogalkotási intézkedéseket fogadhat el azon helyzetek számának növelése érdekében, amelyekben az adatvédelmi tisztviselő kijelölése köz- vagy magánszervezetek által kötelező.

Fontos ugyanakkor megjegyezni, hogy az adatvédelmi munkacsoport ajánlása alapján adatvédelmi tisztviselőt – függetlenül attól, hogy a kijelölés kötelező vagy önkéntes – az adatkezelő vagy az adatfeldolgozó által végzett valamennyi adatkezelési művelet tekintetében kell kijelölni.[23] Így az adatvédelmi tisztviselő tevékenysége kiterjed az összes adatkezelési műveletre, beleértve azokat is, amelyek nem kapcsolódnak a közfeladat ellátásához vagy a hivatali feladatok gyakorlásához, mint például munkavállalói nyilvántartások kezelése.

Adatvédelmi tisztviselőt kell kijelölni továbbá, ha:

b) fő tevékenysége olyan adatkezelési műveleteket foglal magában, amelyhez az érintettek rendszeres és szisztematikus, nagymértékű megfigyelésé szükséges;

A (97) preambulumbekezdés alapján az adatkezelő fő tevékenységei körébe *„az adatkezelők elsődleges tevékenységei tartoznak, a járulékos tevékenységként végzett személyes adatok kezelése nem"*.

A rendeletben fellelhető általános megfogalmazásnak köszönhetően a gyakorlatban nagyon sok értelmezési kérdés merül fel, így a vállalatok nem minden esetben tudják egyértelműen eldönteni, hogy adatvédelmi kötelezettségük-e a tisztviselő kijelölése.

A munkacsoport iránymutatásai alapján az adatkezelő vagy az adatfeldolgozó által végzett fő tevékenység megállapításához szükséges figyelembe venni az adatkezelések célját. Ennek megfelelően a fő tevékenységek az adatkezelő vagy az adatfeldolgozó céljainak eléréséhez szükséges legfontosabb műveleteket jelentik.[24] A „fő tevékenység" azonban nem értelmezhető úgy, hogy kizárják azokat a tevékenységeket,

[23] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 7.

[24] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 8.

amelyek esetében az adatkezelés a szervezet tevékenységének elválaszthatatlan részét képezi. Ilyenek például nyilvános helyek felügyeletét ellátó biztonsági magánvállalatok, amelyeknek a fő tevékenysége a felügyelet, ami viszont elválaszthatatlanul összekapcsolódik a személyes adatok kezelésével.

Másrészt minden szervezet ellát bizonyos tevékenységeket, például fizeti az alkalmazottait, vagy standard informatikai tevékenységeket végez, amelyek a fő tevékenységet támogató funkciók. Ennek ellenére, még ha ezek a tevékenységek szükségesek vagy alapvető fontosságúak is, általában ezeket inkább kiegészítő funkcióknak, mint fő tevékenységnek kell tekinteni.

Előfordulhat továbbá, hogy egy kisvállalkozás mint adatkezelő különböző szolgáltatásai tekintetében nagy adatközpontokat üzemeltető vállalat szolgáltatásait veszi igényben (mint adatfeldolgozó). Ebben az esetben az adatfeldolgozó és nem az adatkezelő köteles adatvédelmi tisztviselőt kinevezni.[25]

Jól látszik tehát, hogy a fő tevékenységet mint kritériumot mindig az adott kontextusban kell értelmezni, és azt esetről esetre, az adott szervezet elsődleges rendeltetése alapján kell helyesen megítélni, hiszen a mulasztás akár adatvédelmi bírságot is eredményezhet.

2020 júniusában például a Glovo App 25 000 eurós bírságot kapott a DPO kinevezésének elmulasztása miatt. Az említett, igény szerinti futárszolgálatok mentesülnek az adatvédelmi tisztviselő kijelölésének kötelezettsége alól, viszont a spanyol adatvédelmi hatóság másképp érvelt. Megállapították, hogy mivel a Glovo napi rendszerességgel több ezer ügyfél adatait dolgozza fel, a vállalat "fő tevékenységként" "nagymértékű" adatkezelést végez, és ezért nem mentesül a GDPR-ban 37. cikkében megfogalmazott követelmény alól.[26]

Mivel a nagymértékű/nagy számban történő kifejezést nem határozza meg a Rendelet, szintén nagyon nehéz eldönteni, pontosan hol a határ, milyen számértékekhez viszonyítva szükséges meghatároznia egy adatkezelő vállalatnak, hogy e kritériumot teljesíti köteles-e. A (97) preambulum bekezdés értelmében nagymértékű adatkezelési műveletnek számít amennyiben jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelését célozzák, vagy amelyek az érintettek jelentős számára hatással lehetnek.

---

[25] Kuner 2020, 693.

[26] Jane Murphy, *Spanish DPA imposes a 25.000 EUR fine for not appointing a DPO and not notifying the DPA on time,* https://edpo.com/news/spanish-dpa-imposes-a-25-000-eur-fine-for-not-appointing-a-dpo-and-not-notifying-the-dpa-on-time/, letöltve: 2022.05.12

Ezen a szintén általános megfogalmazáson túl az adatvédelmi munkacsoport is igyekezett némi támpontot nyújtani, és azt javasolja, hogy különösen a következő tényezőket érdemes figyelembe venni annak meghatározásakor, hogy az adatkezelés nagymértékű-e, vagy nagy számban történik-e:

- az érintettek száma, akár konkrét szám, akár az adott népesség arányában;
- az adatok mennyisége és/vagy a kezelésre kerülő különböző adatok köre;
- az adatkezelési tevékenység időtartama vagy állandósága;
- az adatkezelési tevékenység földrajzi kiterjedése.[27]

Láthatjuk tehát, hogy itt is esetről esetre, a konkrét tevékenységet figyelembe véve szükséges mérlegelni, hogy az adatkezelő vagy adatfeldolgozó a fent említett kritériumnak eleget tesz.

A GDPR szerint annak meghatározása érdekében, hogy az adatkezelés az érintettek magatartása rendszeres és szisztematikus megfigyelésének minősül-e, meg kell megvizsgálni, hogy a természetes személyeket nyomon követik-e az interneten, illetve ezt követően a természetes személy profiljának megalkotását is magában foglaló adatkezelési technikákat alkalmaznak-e annak érdekében, hogy a természetes személyre vonatkozó döntéseket hozzanak, valamint, hogy elemezzék vagy előre jelezzék a természetes személy személyes preferenciáit, magatartását vagy beállítottságát.[28]

Az érintettek "rendszeres és szisztematikus" nyomon követése magában foglalja tehát a nyomon követés és profilalkotás minden formáját, mind online, mind offline, mint például a viselkedésalapú reklámozást.

Az adatvédelmi munkacsoport ajánlása szerint „rendszeres” megfigyelésről beszélünk, ha az adatkezelés:

- folyamatosan vagy bizonyos időközönként történik egy adott időszakban;
- meghatározott időpontokban ismétlődő vagy megismétlik; vagy
- folyamatosan vagy időszakosan történik.

Illetve „szisztematikus” adatkezelésről van szó, ha az adatkezelés:

- egy adott rendszer szerint fordul elő;
- előre megszervezett, szervezett vagy módszeres;
- az adatkezelésre vonatkozó általános terv részeként történik;

[27] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 9.

[28] GDPR (24) preambulumbekezdés

- egy adott stratégia részeként végzik.[29]

Ugyancsak adatvédelmi tisztviselőt kell kijelölni, amennyiben

c) különleges adatok vagy **büntetőjogi felelősség** megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban;

A GDPR 9. cikke értelmében a különleges adatok kezelése csak meghatározott feltételek mellett lehetséges. Nem meglepő tehát, hogy a rendelet az ilyen adatkezelések esetén adatvédelmi tisztviselő kijelölését írja elő. Ilyen adatok a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre, vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok is.

Továbbá a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok kezelése szintén kiemelt kockázatnak tekinthető, ami szintén indokolja az adatvédelmi tisztviselő kinevezését. [30]

VII. Az adatvédelmi tisztviselő kijelölése, státusza és összeférhetetlensége

A DPO státusza szerint lehet belső munkavállaló vagy külső szolgáltató. Belső munkavállaló esetén nagyon szigorúak az összeférhetetlenségi szabályok, illetve azok a rendelkezések, amelyek meghatározzák, ki és hogyan adhat utasításokat neki vagy hogyan lehet elbocsátani.

A GDPR szerint az adatvédelmi tisztviselő független kell legyen mind az adatkezelői, mind az adatfeldolgozói utasításoktól, és közvetlenül az adatkezelő vezetőjének felügyelete alá tartozik. Számos biztosíték létezik annak érdekében, hogy az adatvédelmi tisztviselő függetlenül járhasson el: az adatkezelők vagy az adatfeldolgozók nem utasítják az adatvédelmi tisztviselőt a feladatai ellátásával kapcsolatban, nem bocsátják el vagy nem szankcionálhatják az adatvédelmi tisztviselőt a feladatai ellátásával összefüggésben. Az adatvédelmi tisztviselő által végzett más feladatokból

[29] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 10.

[30] Szabó 2019, 79.

nem fakadhat összeférhetetlenség, azaz nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit. Ilyen összeférhetetlenséget okozó szervezeten belüli pozíciók lehetnek a felsővezetői pozíciók, például vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, marketing osztályvezető, humánerőforrás vezető vagy informatikai osztályvezetők, de más, a szervezeti struktúrában alacsonyabb szinten lévő pozíciók is, ha ezek a pozíciók az adatkezelés céljainak és eszközeinek meghatározásával járnak.

Amennyiben a tisztviselőként eljáró személy nem a szervezet közvetlen alkalmazottja, fontos figyelembe venni, hogy az adatvédelmi tisztviselői tevékenységet ellátó szervezet minden tagja megfeleljen a GDPR 4. cikkében foglalt valamennyi alkalmazandó követelménynek (például lényeges, hogy senkinél se merüljön fel összeférhetetlenség). Ugyanilyen fontos, hogy minden tag részére védelmet biztosítanak a GDPR rendelkezései (például az adatvédelmi tisztviselő tevékenységek végzésére kötött szolgáltatási szerződés nem szüntethető meg jogellenesen, és az adatvédelmi tisztviselői feladatok elvégzését végző szervezet egyes tagjait sem lehet jogellenesen elbocsátani).

Akár külső, akár belső személy, az adatvédelmi tisztviselőt megfelelően integrálni kell a szervezetbe. Alapvető kötelezettség, hogy függetlenül legyen képes tevékenykedni, ami azt jelenti, hogy közvetlenül a legfelső vezetéshez kapcsolódhat csak a személye. Függetlenségének garanciáit az alábbi módon lehet összefoglalni:

- Nem kaphat utasitást a munkájára nézve: ez a követelmény nem jelenti azt, hogy nem lehet ellenőrzési terv, amelyet egyeztet a vállalati vezetéssel, hanem sokkal inkább azt, hogy a döntések során kell függetlennek lennie;
- Az eredeti munkája és a tisztviselői tevékenysége között nem lehet érdekellentét (nem fordulhat elő olyan szituáció, amikor saját magát ellenőrzi). Az érdekellentétek elkerülése érdekében nem lehet adatkezelési folyamatok résztvevője sem (nyilvánvalóan nem lehet HR igazgató, IT igazgató);
- A DPO nem lehet ideiglenes, vagy határozott idejű munkavállaló;
- A DPO-nak nem kell jelentenie csak a felső menedzsmentnek, ezzel is megőrizve véleményének függetlenségét;
- Saját költségvetéssel kell rendelkeznie, amelyből gazdálkodni tud (szakkönyvek vásárlása, konferencia részvétel);

- A DPO-t rendszeresen meg kell hívni a közép- és felsővezetés megbeszéléseire, különösképpen ha adatvédelmi tárgyú döntés szerepel napirenden;
- Minden információt időben át kell adni a DPO-nak, hogy felkészülhessen és megfelelő tanácsot adhasson.

Az adatvédelmi tisztviselő szervezeten belüli kijelölése több szempontból megfontolt döntés kell, hogy legyen. Semmi esetre sem tanácsos a látszólagos megfelelés érdekében egy már alkalmazott személyt adatvédelmi tisztviselői feladatokkal felruházni. Az ilyen kijelöléseket az adatvédelmi hatóságok a joggyakorlat alapján komolyan veszik, és komoly bírsággal büntetik.

2020 áprilisában a belga adatvédelmi hatóság 50.000 eurós bírságot szabott ki egy vállalatra a GDPR szerinti összeférhetetlenségi szabályok be nem tartása miatt. Az ellenőrzött vállalatról kiderült, hogy a megfelelési, ellenőrzési és kockázatkezelési vezetőt nevezte ki adatvédelmi tisztviselőnek. A vizsgálatot követően a hatóság megállapította, hogy ez a kombináció olyan összeférhetetlenséget eredményezett, amely sértette a GDPR követelményeit.[31]

Egy másik esetben szintén a belga hatóság ugancsak az összeférhetetlenség kritériumának megsértése miatt 75.000 eurós bírságot szabott ki egy belga bankkal szemben.[32]

VIII. Az adatvédelmi tisztviselő felelőssége

A DPO ellenőrzési és vizsgálati funkcióval rendelkezik, így nyilvánvalóan ezekért a tevékenységekért felelősséggel tartozik. Nem terheli azonban személyes felelősség az adatvédelmi követelmények be nem tartásáért. A Rendelet egyértelművé teszi, hogy az adatkezelőnek vagy adatfeldolgozónak kell biztosítania és bizonyítania, hogy az adatkezelés a Rendelet követelményeivel összhangban történik. Ennek ellenére természetesen különféle feltételek fennállása esetén munkajogi vagy polgári jogi felelőssége megállapítható.

Mivel a DPO belsős és külsős is lehet, eltér a felelősség mércéje is:

[31] Beslissing ten gronde 18/2020 van 28 april 2020, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-18-2020.pdf, (2022.05.13.)

[32] Décision quant au fond 141/2021 du 16 décembre 2021, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-141-2021.pdf, (2022.05.13.)

a) Belső munkavállaló esetén

A magyar szabályozás szerint a munkavállalóként tevékenykedő tisztviselő természetszerűen csak a Munka törvénykönyve (Mt.) szerinti felelősségi rendszer szerint vonható felelősségre. A Mt. 179. § általános szabályai szerint a munkavállaló köteles munkáját személyesen, az általában elvárható szakértelemmel és gondossággal, a munkájára vonatkozó szabályok, előírások, utasítások és szokások szerint végezni. Ha munkavállaló a munkaviszonyból származó kötelezettségének nem tesz eleget – ha nem úgy jár el, ahogy az adott helyzetben elvárható –, és ezzel a munkáltatónak kárt okoz, akkor azt köteles megtéríteni. A kötelezettségszegés megnyilvánulhat tevőlegesen, de az akár lehet mulasztás is.

A munkavállaló a teljes kárt csak szándékosság vagy súlyos gondatlanság esetén köteles megtéríteni, amennyiben gondatlanul járt el, a kártérítés mértéke nem haladhatja meg a munkavállaló négyhavi távolléti díjának összegét.[33]

b) Külső DPO esetén

A külsős vagy akár csoportszintű tisztviselők esetén nagyon nehéz megítéli a felelősség mértékét. Az ilyen felelősség a megbízási kötelmekkel kapcsolatban, különösen az ügyvédi megbízási szerződés esetén megszokott mértékéhez igazodik.

IX. Milyen készségekkel kell rendelkezni az adatvédelmi tisztviselőnek?

A GDPR 37. cikkének (5) bekezdése előírja, hogy az adatvédelmi tisztviselőnek az adatvédelem területén szakértelemmel kell rendelkeznie, de nem határozza meg az e szintre vonatkozó minimumkövetelményeket. A szakértői ismeretek szükséges szintjét az adatkezelő által végzett adatkezelés, valamint az általa kezelendő személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni. Ha például az adatkezelési tevékenység különösen bonyolult, vagy nagy mennyiségű érzékeny adatot érint, az adatvédelmi tisztviselőnek adott esetben magasabb szintű szakértelemmel kell rendelkezni.[34]

[33] 2012. évi I. törvény a munka törvénykönyvéről, 179. §

[34] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 13.

Mindezek ellenére túlzás lenne ezen rendelkezésbe olyan további szakmai tulajdonságok meglétét beleolvasni, amelyek vélelmezhetően kötelezőek lehetnének, mint például az, hogy az adatvédelmi tisztviselőnek jogász végzettséggel vagy jogi diplomával kell rendelkeznie. Ezzel szemben a jogszabály "az adatvédelmi jog és gyakorlat" terén szerzett megfelelő ismeretekre utal, amely az adatvédelmi ügyekkel kapcsolatos folyamatos szakmai kitettséggel is bizonyítható. Az adatvédelmi munkacsoport iránymutatása továbbá hangsúlyozza, hogy "az üzleti szektor és az adatkezelő szervezetének ismerete" szintén hozzájárul a szükséges szakmai kvalitások megalapozásához, hatóságok esetében pedig az adatvédelmi tisztviselőnek "a közigazgatás igazgatási szabályainak és eljárásainak alapos ismeretével" kell rendelkeznie.[35]

Ilyen releváns készségek és szakértelem lehet például szakértelem a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén, beleértve a GDPR alapos ismeretét; az elvégzett adatkezelési műveletek ismerete; az információs technológiák és az adatbiztonság ismerete; az üzletág és a szervezet ismerete; a szervezeten belül az adatvédelmi kultúra előmozdításának képessége.

Romániában a nemzeti jog igyekezett a rendelet általános szabályait kiegészíteni, és ezáltal új követelményeket is támasztott. A 2018. évi 74 számú Nemzeti Képesítési Hatóság döntése által jóváhagyott foglalkozási standard szerint az adatvédelmi tisztviselőnek rendelkeznie kell felsőoktatási végzettséggel, legalább 1 év munkatapasztalattal, szakértelemmel, jó kommunikációs készséggel, illetve a képességeit igazoló oklevéllel, melyet az adott szakágban szervezett képzésen/kurzuson szerzett meg. Az adatvédelmi tisztviselőnek továbbá: felelősségteljesnek, komolynak, pontosnak, empatikusnak, szintézis és elemzési képességgel rendelkezőnek kell lennie.[36]

X. Az adatvédelmi tisztviselő feladatköre

Az adatvédelmi tisztviselő feladatait a rendelet 39. cikke foglalja össze. A "legalább" szó használata nyomatékosítja, a felsorolás illusztratív és nem korlátozó jellegű, a DPO hatásköre ugyanis nem merül ki a felsorolt

[35] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 14.

[36] Autoritatea Națională pentru Calificări, Standard ocupational pentru Responsabil cu protecția datelor cu caracter personal http://www.anat.ro/wp-content/uploads/2018/03/Standard-ocupatioan-Responsabil-cu-protectia-datelor-cu-protectia-datelor.pdf , (2022.07.23.)

feladatkörökben, az adatkezelő más feladatokkal is megbízhatja, vagy ezeket a feladatokat részletesebben is meghatározhatja.

Az adatvédelmi tisztviselő a megfelelés biztosítása érdekében három területen is fontos feladatokat lát.

1. Feladatai a kinevező szervezettel szemben:

a) tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó adatvédelmi kötelezettségeikkel kapcsolatban;

Az adatvédelmi tisztviselő szerepe szerint részt vesz a vállalat adatkezeléssel kapcsolatos tevékenységeinek tervezésében, szakértőként tanácsokkal, információnyújtással támogatja a munkafolyamatokat.

b) ellenőrzi a személyes adatok védelmével kapcsolatos szabályoknak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

Megfelelés ellenőrzésére vonatkozó feladatai részeként az adatvédelmi tisztviselő különösen az alábbiakat teheti: információt gyűjt az adatkezelési tevékenységek meghatározása érdekében; elemzi és ellenőrzi az adatkezelési tevékenységek megfelelőségét; tájékoztatást, szakmai tanácsadást nyújt és ajánlásokat bocsát ki az adatkezelő vagy az adatfeldolgozó részére.

c) kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR 35. cikk szerinti elvégzését.

Az adatvédelmi hatásvizsgálatot illetően az adatkezelő vagy az adatfeldolgozó köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát különösen az alábbi kérdésekben:

- kell-e adatvédelmi hatásvizsgálatot végezni;
- milyen módszereket kell követni az adatvédelmi hatásvizsgálat elvégzésekor;
- az adatvédelmi hatásvizsgálatot szervezeten belül végezzék-e el, vagy kiszervezzék-e azt;
- milyen biztosítékokat (beleértve a technikai és szervezési intézkedéseket) kell alkalmazni az érintettek jogait és érdekeit érintő kockázatok enyhítésére;
- az adatvédelmi hatásvizsgálatot megfelelően végezték-e el, és a következtetései (lehet-e folytatni az adatkezelést, és milyen

biztosítékokat kell alkalmazni) megfelelnek-e az adatvédelmi követelményeknek.[37]

2. Feladatai az érintettekkel szemben

A rendelet alapján az érintettek (alkalmazott, fogyasztó vagy partner) számára a tisztviselőnek kötelezően elérhető kell lennie, amikor a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódóan bármilyen kérdést megfogalmaznak.[38] Ezáltal az érintettek jogainak biztosítása is a DPO feladatkörébe tartozik.

A Rendelet 37. cikk (7) bekezdése alapján "*az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét"*.

A DPO elérhetőségének nyilvánosságra hozatala megkönnyíti az érintettek számára az adatvédelmi jogaik gyakorlását, és elősegíti a panaszok és kérdések adatvédelmi tisztviselő általi helyi szintű kezelését. Ez azonban nem akadályozza meg az érintettet abban, hogy közvetlenül az európai adatvédelmi hatósághoz forduljon, amennyiben adatvédelmi jogainak megsértését tapasztalja.[39]

3. Feladatai a hatósággal szemben

Szintén az adatvédelmi tisztviselő feladatkörébe tartozik az adatvédelmi hatóság és a szervezet közötti együttműködés elősegítése, különösen a vizsgálatok, a panaszkezelés és az előzetes konzultáció keretében. Ennek megfelelően a DPO egyik legfontosabb feladata az adatvédelmi hatósággal való együttműködés. Amennyiben a hatóság kivizsgálás céljából felveszi a kapcsolatot a vállalattal, az várhatóan a hozzájuk bejelentett DPO-n keresztül fog történni. Az adatvédelmi tisztviselő nevének a felügyelő hatósággal történő közlése alapvető fontosságú annak érdekében, hogy az adatvédelmi tisztviselő kapcsolattartóként szolgáljon a szervezet és a felügyeleti hatóság között (GDPR 39. cikk (1) bekezdésének e) pontja).

XI. Következtetések

[37] A 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban, 20.

[38] Szabó 2018, 7.

[39] European Data Protection Supervisor, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf, 6. (2022.05.21.)

Mint az a fenti elemzésből is jól látszik, az adatvédelmi rendelet egyik központi eleme, az elszámoltathatóság alapelve, ami nem számít újdonságnak e területen, hiszen az adatkezelés jogszerűségéért eddig is az adatkezelő felelt, de a bizonyítás terhe csak reaktív módon, bírósági eljárás során terhelte. A jelenlegi szabályozás alapján az elszámoltathatóság magában foglalja az adatkezelő legfontosabb feladatát, akinek ezentúl nem csak felelősséget kell vállalnia a rendeletben megfogalmazott alapelvek és kötelezettségek betartásáért, de képesnek kell lennie bizonyítani is a megfelelését.

Az elszámoltathatóság elvének megértése a hatékony adatvédelem sarokkövévé és az EU adatvédelmi törvény, politika és szervezeti gyakorlat domináns trendjévé vált. Ezen alapelv betartása nélkül nem beszélhetünk adatvédelmi megfelelésről, amiről a vállalatok többsége megfeledkezik.

Láthatjuk továbbá azt is, hogy egy sikeres adatvédelmi megfelelés megszervezése összetett vállalkozás. Az adatkezelőnek folyamatosan lépést kell tartania az értelmezési és törvényi változásokkal, figyelnie kell mind a külső, mind a belső tényezők lehetséges veszélyeit, biztosítania kell a meglévő vagy a megfelelés során kialakult szervezeti gyakorlatok betartását, reagálnia kell az érdekelt felek kérdéseire, és mindenek felett olyan vezetői készséggel kell rendelkeznie, mely biztosítja a szervezeten belüli megfelelő hozzáállást. Az adatvédelmi hatóság, az ügyfelek, az alkalmazottak vagy akár üzleti partnerek egyaránt felelősségre vonhatják a szervezetet az adatvédelmi szabályok be nem tartása miatt, így egyre több vállalat kifejezett figyelmet fordít e területre. Éppen ezért a legtöbb adatkezelést végző vállalatnak szüksége van adatvédelmi tisztviselőre vagy legalább adatvédelmi kérdésekben jártas, az uniós szabályozást, a törvényt és az adatvédelmi gyakorlatot jól ismerő szakemberre. Az átláthatóság elvének történő megfelelés érdekében nagyon sok esetben szakmai nézőpontra, tudásra, véleményre lehet szükség. A Rendelet, de még a munkacsoport iránymutatásai is többnyire általános jellegűek, emiatt nagyon sok helyen értelmezési kérdések adódhatnak.

Nincs ez másképp az adatvédelmi tisztviselőre vonatkozó rendelkezések kapcsán sem, így sok esetben az adatkezelő önmaga, szakmai segítség nélkül nem tudja teljes bizonyossággal eldönteni, hogy a Rendelet alapján adatvédelmi kötelezettsége-e a tisztviselő kinevezése vagy sem. Hibás az a kis- és középvállalatok szintjén bevett gyakorlat, amely szerint a vállalati struktúrában eddig egyéb feladatokat ellátó kollégából napok alatt adatvédelmi szakértőt faragnak, aki az eddigi feladatköre mellé kapja meg

az egyébként teljes feladatkört igénylő DPO funkciót. Egyrészt az összeférhetetlenség miatt, másrészt az ilyen adatvédelmi tisztviselők szakmai tudása is igencsak megkérdőjelezhető.

A Rendelet bár nem teszi kötelezővé minden szervezet számára DPO kinevezését, az elszámoltathatósági kötelezettség bevezetésével egyértelművé tette, hogy a megfeleléshez minden szervezetnek adatvédelmi tudatosságra és szakmai felkészültségre is szüksége van, amelyet leginkább egy adatvédelmi tisztviselő kinevezése tud biztosítani, feltéve ha az a fentebb elemzett kritériumoknak valóban megfelel.

Mindezek ellenére egy adatvédelmi szakember beillesztése a vállalati struktúrába komoly anyagi vonzatot jelent, amit nem minden szervezet képes megengedni magának.

Felhasznált irodalom

A GDPR 29. cikk szerinti adatvédelmi munkacsoport iránymutatása az adatvédelmi tisztviselőkkel kapcsolatban

A GDPR 29. cikk szerinti adatvédelmi munkacsoport 3/2010 véleménye az elszámoltathatóság elvéről

Árvai Viktor György (2018): Az elszámoltathatóság alapelve és az adatkezelő kötelezettségei, NKE, Budapest

Autoritatea Națională pentru Calificări, Standard ocupational pentru Responsabil cu protecția datelor cu caracter personal http://www.anat.ro/wp-content/uploads/2018/03/Standard-ocupatioan-Responsabil-cu-protectia-datelor-cu-protectia-datelor.pdf

Beslissing ten gronde 18/2020 van 28 april 2020, https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-18-2020.pdf

Center for Information Policy Leadership (2018): The Central Role of Organisational Accountability in Data Protection Discussion Paper 2 (of 2), Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf

Christopher Kuner, Lee A. Bygrave (2020): The EU general data protection regulation (GDPR). A commentary, Oxford University Press, United Kingdom. DOI: https://doi.org/10.1093/oso/9780198826491.001.0001

Christopher Williams (2006): Leadership accountability in a globalizing world, Palgrave Macmillan, London. DOI: https://doi.org/10.1057/9780230596825

Décision quant au fond 141/2021 du 16 décembre 2021, https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-141-2021.pdf

European Union Agency for Network and Information Security (2014): Privacy and Data Protection by Design – from policy to engineering, file:///C:/Users/anita/Downloads/Privacy%20and%20Data%20Protection%20by%20Design%20(3).pdf

Jane Murphy: Spanish DPA imposes a 25.000 EUR fine for not appointing a DPO and not notifying the DPA on time. https://edpo.com/news/spanish-dpa-imposes-a-25-000-eur-fine-for-not-appointing-a-dpo-and-not-notifying-the-dpa-on-time

Justine Brown: Rise of the Chief Privacy Officer, Government Technology. https://www.govtech.com/data/rise-of-the-chief-privacy-officer.html

Justine Brown (30 May 2014): "Rise of the Chief Privacy Officer". Government Technology. Retrieved 23 May 2019.

Markus Heyder, Sam Grogan (2018): 'The role of DPAs in incentivizing accountability', IAPP.org: www.iapp.org/news/a/the-role-of-dpas-in-incentivizing-accountability/?fbclid=IwAR1FrLNz7Rv9Te-MRFFXSZvy-vJf9hiE_vtxCSzLwcoXPAt554rslOr0evs

Péterfalvi Attila, Révész Balázs, Buzás Péter: *Magyarázat a GDPR-ról.* Wolters Kluwer, Budapest, 2018

Szabó Endre: *Az adatvédelmi tisztviselőről, a GDPR szabályainak elemzése*. HVG-ORAC, Infokommunikáció és jog, 2018/1.

Szabó Endre Győző: Az Európai Unió Általános Adatvédelmi Rendeletében biztosított védelem szintjének elemzése. Doktori értekezés, Károli Gáspár Református Egyetem Állam- és Jogtudományi Doktori Iskola, 2019.

***

Data protection officer as the cornerstone of accountability

Summary

One of the central elements of the Data Protection Regulation is the principle of accountability, which is not new in this area, as the controller has always been responsible for the lawfulness of data processing, but the burden of proof has only been placed on him in a reactive manner in court proceedings. Under the current regime, accountability includes the most important task of the controller, who must now not only take responsibility for compliance with the principles and obligations set out in the Regulation, but must also be able to demonstrate compliance.

Understanding the principle of accountability has become a dominant trend in EU data protection law, policy and organizational practice.

In this accountability-based compliance framework the Data Protection Officers ('DPO's) will be at the heart of this new legal norm.

Prior to the adoption of the GDPR, the Data protection Working Party stated that the DPO is the cornerstone of accountability and that the appointment of a DPO can facilitate compliance and provide a competitive advantage for businesses.

Building on this statement, the following paper will examine the relationship and interaction between the appointment of a DPO (Article 37 GDPR) and compliance with the principle of accountability (Article 5(2) GDPR), trying to highlight the most important issues in the context of corporate data protection compliance.