A 29. CIKK SZERINTI ADATVÉDELMI MUNKACSOPORT

16/HU
WP 243 rev.01

Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban

Az elfogadás időpontja: 2016. december 13.

Legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.

AZ EGYÉNEKNEK A SZEMÉLYES ADATOK FELDOLGOZÁSA TEKINTETÉBEN VALÓ VÉDELMÉVEL FOGLALKOZÓ MUNKACSOPORT

amelyet az 1995. október 24-i 95/46/EK európai parlamenti és tanácsi irányelvvel hoztak létre,

tekintettel az említett irányelv 29. és 30. cikkére,

tekintettel eljárási szabályzatára,

ELFOGADTA EZT AZ IRÁNYMUTATÁST:

Tartalomjegyzék

1 Bevezetés

A 2018. május 25-én hatályba lépő általános adatvédelmi rendelet (a továbbiakban: GDPR)[1] biztosítja az európai adatvédelem modernizált, elszámoltathatóságon alapuló megfelelőségi keretét. Az adatvédelmi tisztviselők számos szervezet számára ezen új jogi keret középpontjában állnak majd, és megkönnyítik a GDPR rendelkezéseinek való megfelelést.

A GDPR értelmében bizonyos adatkezelők és adatfeldolgozók kötelesek adatvédelmi tisztviselőt kijelölni.[2] Ez a kötelezettség kiterjed minden közhatalmi szervre vagy egyéb, közfeladatot ellátó szervre (függetlenül attól, hogy 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 GDPR kifejezetten nem írja elő adatvédelmi tisztviselő kijelölését, a szervezetek számára bizonyos esetekben hasznosnak bizonyulhat, ha önkéntes alapon jelölnek ki adatvédelmi tisztviselőt. A 29. cikk szerinti munkacsoport (a továbbiakban: Munkacsoport) támogatja ezeket a törekvéseket.

Az adatvédelmi tisztviselő nem újonnan létrehozott intézmény. Bár a 95/46/EK irányelv[3] nem írta elő a szervezeteknek adatvédelmi tisztviselő kijelölését, az adatvédelmi tisztviselő kijelölésének gyakorlata azonban az évek során több tagállamban is kialakult.

A GDPR elfogadását megelőzően a 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.[4] 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.

Az adatvédelmi tisztviselőket nem terheli személyes felelősség a GDPR be nem tartásáért. A GDPR egyértelművé teszi, hogy az adatkezelőnek vagy az adatfeldolgozónak kell biztosítani és bizonyítani, hogy a kezelés a GDPR rendelkezéseivel összhangban történik (24. cikk (1) bekezdése). Az adatvédelmi rendelkezések betartásáért az adatkezelő vagy az adatfeldolgozó felelős.

---

[1] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.). A GDPR EGT-vonatkozású, és az EGT-megállapodásba történő belefoglalását követően alkalmazandó.

[2] 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 szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelv (HL L 119., 2016.5.4., 89–131. o.) 32. cikke, valamint a nemzeti végrehajtási jogszabályok alapján az illetékes hatóságok is kötelesek adatvédelmi tisztviselőt kijelölni. A jelen iránymutatás a GDPR szerinti adatvédelmi tisztviselőkre helyezi a hangsúlyt, ugyanakkor vonatkozik a 2016/680 irányelv szerinti adatvédelmi tisztviselőkre is.

[3] Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (HL L 281., 1995.11.23., 31. o.).

[4] Lásd: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

Az adatkezelő vagy az adatfeldolgozó kulcsfontosságú szerepet játszik abban is, hogy az adatvédelmi tisztviselő hatékonyan végezhesse a feladatait. Az adatvédelmi tisztviselő kijelölése az első lépés, de az adatvédelmi tisztviselők részére elegendő önállóságot és forrást kell biztosítani a feladataik hatékony végrehajtásához.

A GDPR az adatvédelmi tisztviselőt kulcsszereplőként ismeri el az új adatkezelési rendszerben, és meghatározza a tisztviselő kijelölésének szabályait, jogállását és feladatait. A jelen iránymutatás célja a GDPR releváns rendelkezéseinek pontosítása annak érdekében, hogy segítsen az adatkezelőknek és az adatfeldolgozóknak a jogszabályoknak való megfelelésben, továbbá támogatást nyújtson az adatvédelmi tisztviselőknek a szerepkörük ellátásában. Az iránymutatás a legjobb gyakorlatra vonatkozó ajánlásokat is tartalmazza, az egyes uniós tagállamokban szerzett tapasztalatokra építve. A Munkacsoport nyomon követi a jelen iránymutatás végrehajtását, és adott esetben kiegészítheti azt.

2 Az adatvédelmi tisztviselőt kijelölése

2.1. Kötelező kijelölés

A GDPR 37. cikkének (1) bekezdése előírja, hogy adatvédelmi tisztviselőt három esetben kell kijelölni:[5]

a) ha az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik;[6]
b) ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé; vagy
c) ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak[7] vagy[8] a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.[9]

Az alábbiakban a Munkacsoport iránymutatást nyújt a 37. cikk (1) bekezdésében használt kritériumok és terminológia tekintetében.

A Munkacsoport azt ajánlja, hogy az adatkezelők és az adatfeldolgozók dokumentálják az annak eldöntése érdekében készült belső elemzést, hogy kötelesek-e adatvédelmi tisztviselőt kijelölni vagy sem, annak igazolására, hogy a releváns tényezőket megfelelően figyelembe vették, kivéve, ha egyértelmű, hogy a szervezet nem köteles adatvédelmi tisztviselőt kijelölni.[10] Ez az elemzés az elszámoltathatóság elve alapján készült dokumentáció része. Az elemzést a felügyeleti hatóság előírhatja, és szükség esetén aktualizálni kell, például, ha az adatkezelők vagy az adatfeldolgozók

[5] Megjegyzendő, hogy a 37. cikk (4) bekezdése értelmében az uniós vagy tagállami jog más esetekben is előírhatja adatvédelmi tisztviselő kijelölését.

[6] Kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat. Lásd az (EU) 2016/680 irányelv 32. cikkét.

[7] A 9. cikk alapján ezek 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.

[8] A 37. cikk (1) bekezdésének c) pontjában az „*és*” kifejezés szerepel. Az „*és*” helyett a „*vagy*” kifejezés használatának magyarázatával kapcsolatban lásd lentebb a 2.1.5. pontot.

[9] 10. cikk.

[10] Lásd a 24. cikk (1) bekezdését.

olyan új tevékenységeket látnak el vagy olyan új szolgáltatásokat nyújtanak, amelyek a 37. cikk (1) bekezdésében felsorolt esetkör hatálya alá tartoznak.

Amikor egy szervezet önkéntes alapon jelöl ki adatvédelmi tisztviselőt, a 37-39. cikk szerinti követelmények ugyanúgy vonatkoznak e tisztviselő kijelölésére, a jogállására és a feladataira, mintha a kijelölés kötelező lenne.

Semmi akadálya azonban annak, hogy a személyes adatok védelmével kapcsolatos feladatok elvégzésére alkalmazottat vegyen fel, vagy külső tanácsadót vegyen igénybe az a szervezet, amely jogilag nem köteles és önkéntes alapon sem kíván kijelölni adatvédelmi tisztviselőt. Ebben az esetben fontos biztosítani, hogy ne legyen összetéveszthető a jogcímük, státuszuk, jogállásuk és feladataik. Ezért egyértelművé kell tenni a szervezeten belüli, valamint az adatvédelmi hatóságokkal, az érintettekkel és a nyilvánossággal folytatott kommunikációban, hogy ez a személy vagy tanácsadó nem minősül adatvédelmi tisztviselőnek. [11]

Az adatvédelmi tisztviselőt – függetlenül attól, hogy a kijelölés kötelező vagy önkéntes – az adatkezelő vagy az adatfeldolgozó által végzett valamennyi adatkezelési művelet tekintetében jelölik ki.

2.1.1 „KÖZHATALMI SZERV VAGY EGYÉB, KÖZFELADATOT ELLÁTÓ SZERV"

A GDPR nem határozza meg a „*közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv"* fogalmát. A Munkacsoport úgy véli, hogy ezt a fogalmat a nemzeti jog szerint kell meghatározni. Ennek megfelelően a közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv fogalma magában foglalja az országos, regionális és helyi hatóságokat, de a fogalom – az alkalmazandó nemzeti jogszabályok szerint – általában magában foglalja a közjog hatálya alá tartozó más szerveket is.[12] Ebben az esetben az adatvédelmi tisztviselő kijelölése kötelező.

Nem csak közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv láthat el közfeladatot vagy gyakorolhat közhatalmi jogosítványt,[13] hanem a közjog vagy magánjog hatálya alá tartozó egyéb természetes vagy jogi személy is – az egyes tagállamok nemzeti szabályozása szerint – olyan ágazatokban, mint például a tömegközlekedés, a víz- és az energiaellátás, a közúti infrastruktúra, a közszolgálati műsorszolgáltatás, az állami, illetve önkormányzati lakáshoz jutás vagy a szabályozott szakmák fegyelmi testületei.

Ezekben az esetekben az érintettek helyzete adott esetben nagyon hasonló lehet ahhoz, amikor adataikat közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv kezeli. Így például az adatokat hasonló célból kezelhetik, és az egyéneknek gyakran kevés vagy semmilyen választási lehetősége nincs az adataik kezelésének módjára vonatkozóan, és így szükségessé válhat az adatvédelmi tisztviselő kijelölése által biztosítható további védelem.

Bár ilyen esetekben nem kötelező, a Munkacsoport jó gyakorlatként azt ajánlja, hogy a közfeladatokat ellátó vagy közhatalmi jogosítványt gyakorló magánjogi szervezetek jelöljenek ki adatvédelmi tisztviselőt. Ezen adatvédelmi tisztviselő tevékenysége kiterjed az összes adatkezelési műveletre,

[11] Ez a néhány vállalatnál már működő adatvédelmi főtisztviselőkre vagy más adatvédelmi szakemberekre is vonatkozik, akik nem minden esetben felelnek meg a GDPR-kritériumoknak, például a rendelkezésre álló források vagy a függetlenség garanciái tekintetében, és amennyiben nem felelnek meg e kritériumoknak, nem tekinthetők adatvédelmi tisztviselőnek.

beleértve azokat is, amelyek nem kapcsolódnak közfeladat ellátásához vagy közhatalmi jogosítvány gyakorlásához (például munkavállalói adatbázis kezelése).

2.1.2 „FŐ TEVÉKENYSÉGEK”

A GDPR 37. cikke (1) bekezdésének b) és c) pontjában az *„az adatkezelő vagy az adatfeldolgozó fő tevékenységei”* kifejezés szerepel. A (97) preambulumbekezdés alapján az adatkezelők fő tevékenységei körébe „*az adatkezelők elsődleges tevékenységei tartoznak, a járulékos tevékenységként végzett személyes adatok kezelése nem”*. A „fő tevékenységek” az adatkezelő vagy az adatfeldolgozó céljainak eléréséhez szükséges legfontosabb műveleteket jelentik.

A „fő tevékenységeket” azonban nem szabad úgy értelmezni, mint amelyek közé nem tartoznak azok a tevékenységek, amelyek során az adatkezelés az adatkezelő vagy az adatfeldolgozó tevékenységének elválaszthatatlan részét képezi. Például egy kórház fő tevékenysége egészségügyi ellátás biztosítása. A kórház azonban nem tudná biztonságosan és hatékonyan biztosítani az egészségügyi ellátásokat egészségügyi adatok kezelése, például a betegek egészségügyi nyilvántartása nélkül. Ezért ezeknek az adatoknak a kezelését a kórház egyik fő tevékenységének kell tekinteni, emiatt a kórházaknak adatvédelmi tisztviselőt kell kijelölni.

Egy másik példa egy több magánbevásárlóközpont és nyilvános hely felügyeletét ellátó biztonsági magánvállalat. A felügyelet a vállalat alapvető tevékenysége, amely viszont elválaszthatatlanul összekapcsolódik a személyes adatok kezelésével. Ezért ennek a vállalatnak is ki kell jelölni adatvédelmi tisztviselőt.

Másrészről, minden szervezet végez bizonyos tevékenységeket, például fizetést ad az alkalmazottaknak, vagy általános informatikai támogató tevékenységeket végez. Ezek a szervezet fő tevékenységéhez vagy fő vállalkozási tevékenységéhez szükséges támogatási funkciók példái. Annak ellenére, hogy ezek a tevékenységek szükségesek vagy nélkülözhetetlenek, általában nem fő tevékenységnek, hanem inkább járulékos funkcióknak tekinthetők.

---

[12] Lásd például a „*közigazgatási szerv”* és a *„közjogi intézmény*” a közszféra információinak további felhasználásáról szóló, 2003. november 17-i 2003/98/EK európai parlamenti és tanácsi irányelv (HL L 345., 2003.12.31., 90. o.) 2. cikkének 1. és 2. pontjában meghatározott fogalmát.

[13] A 6. cikk (1) bekezdésének e) pontja.

2.1.3 „NAGY MÉRTÉKŰ / NAGY SZÁMBAN TÖRTÉNŐ”

A 37. cikk (1) bekezdésének b) és c) pontja előírja, hogy akkor kell adatvédelmi tisztviselőt kijelölni, ha a személyes adatok kezelése nagymértékű, illetve nagy számban történik. A GDPR nem határozza meg, hogy mit jelent a nagymértékű, illetve nagy számban történő adatkezelés, bár a (91) preambulumbekezdés nyújt bizonyos útmutatást.[14]

Valójában nem lehet pontosan megadni sem a kezelt adatok mennyiségét, sem az érintett személyek számát, amely minden helyzetben alkalmazandó lenne. Ez azonban nem zárja ki annak lehetőségét, hogy idővel kialakul egy általános gyakorlat annak pontosabb és/vagy számszerűsített meghatározására, hogy mit jelent a *„nagy mértékű / nagy számban történő”* kifejezés bizonyos típusú adatkezelési tevékenységek tekintetében. A Munkacsoport ezen a téren is hozzá kíván járulni a fejlődéshez oly módon, hogy megosztja és nyilvánosságra hozza az adatvédelmi tisztviselő kijelölése esetén alkalmazott küszöbértékeket.

Mindenesetre a Munkacsoport azt ajánlja, hogy különösen a következő tényezőket vegyék figyelembe annak meghatározásakor, hogy az adatkezelés nagymértékű-e, vagy nagy számban történik-e:

- Az érintettek száma - akár egy 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

[14] A preambulumbekezdés szerint ez különösen vonatkozik *„a nagymértékű adatkezelési műveletekre, amelyek jelentős mennyiségű személyes adat regionális, nemzeti vagy szupranacionális szintű kezelését célozzák, és amelyek az érintettek jelentős számára hatással lehetnek”.* Másrészről, a preambulumbekezdés kifejezetten azt tartalmazza, hogy *„[a] személyes adatok kezelése nem tekinthető nagymértékűnek, ha az adatkezelés egy adott szakorvos, egészségügyi szakember betegei vagy egy adott ügyvéd ügyfelei személyes adataira vonatkozik”*. Fontos megjegyezni, hogy míg a preambulumbekezdés a skála szélső értékeit tartalmazza (egy adott szakorvos általi, illetve egy egész országra vagy egész Európára kiterjedő adatkezelés); e szélső értékek között egy jelentős szürke zóna található. Ezenkívül emlékeztetni kell arra, hogy ez a preambulumbekezdés az adatvédelmi hatásvizsgálatokra vonatkozik. Ez azt jelenti, hogy egyes elemek ebben az összefüggésben lehetnek specifikusak, és nem feltétlenül ugyanúgy vonatkoznak az adatvédelmi tisztviselő kijelölésére.

Példák a nagymértékű vagy nagy számban történő adatkezelésre:

- a betegek adatainak kezelése a kórház szokásos működése keretében
- városi tömegközlekedést használó személyek utazási adatainak kezelése (például menetjegyek nyomon követése)
- egy nemzetközi gyorsétteremlánc ügyfeleire vonatkozó valós idejű helymeghatározási adatok statisztikai célú kezelése egy erre a szolgáltatás nyújtására specializálódott adatkezelő útján
- ügyféladatok kezelése egy biztosító társaság vagy egy bank szokásos üzletmenete keretében
- személyes adatok keresőmotor általi kezelése viselkedésalapú reklám céljából
- adatok (tartalom, forgalom, hely) kezelése telefon- vagy internetszolgáltatók által

Példák arra, mi nem tartozik a nagymértékű vagy nagy számban történő adatkezelés körébe:

- betegek adatainak kezelése egy adott szakorvos által
- a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok kezelése egy adott ügyvéd által

2.1.4 „RENDSZERES ÉS SZISZTEMATIKUS MEGFIGYELÉS"

A GDPR nem határozza meg az érintettek rendszeres és szisztematikus megfigyelésének fogalmát, de *„az érintettek magatartásának megfigyelése"* fogalmát a (24) preambulumbekezdés említi,[15] és egyértelműen magában foglalja az interneten történő nyomon követés és profilalkotás valamennyi formáját, ideértve a viselkedésalapú reklám céljából történő adatkezelést is.

A megfigyelés fogalma azonban nem korlátozódik az online környezetre, és az online nyomon követés csak az érintettek viselkedése megfigyelésének egyik példája.[16]

A Munkacsoport értelmezése szerint a „rendszeres" kifejezés jelentése az alábbiak közül egy vagy több:

- Folyamatosan vagy bizonyos időközönként történik egy adott időszakban
- Meghatározott időpontokban ismétlődő vagy megismétlik
- Folyamatosan vagy időszakosan történik

A Munkacsoport értelmezése szerint a „szisztematikus" kifejezés jelentése az alábbiak közül egy vagy több:

- Egy adott rendszer szerint fordul elő
- Előre megszervezett, szervezett vagy módszeres
- Az adatkezelésre vonatkozó általános terv részeként történik

[15] *„Annak meghatározása, hogy az adatkezelés az érintettek magatartásának 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 elsősorban a természetes személyre vonatkozó döntéseket hozzanak, valamint, hogy elemezzék vagy előre jelezzék a természetes személy személyes preferenciáit, magatartását vagy beállítottságát."*

[16] Megjegyzendő, hogy a (24) preambulumbekezdés a GDPR országhatáron kívüli alkalmazására irányul. Ezenkívül különbség van az *„érintettek viselkedésének megfigyelése"* (3. cikk (2) bekezdésének b) pontja) és a *„rendszeres és szisztematikus megfigyelés"* (37. cikk (1) bekezdésének b) pontja) kifejezések között, ami azt jelezheti, hogy különböző fogalmakról van szó.

- Egy adott stratégia részeként végzik

Példák olyan tevékenységekre, amelyek során az érintettek rendszeres és szisztematikus megfigyelésére kerülhet sor: távközlési hálózat működtetése; távközlési szolgáltatások nyújtása; célközönség e-mail alapú újbóli meghatározása; adatvezérelt marketing tevékenységek; profilalkotás és pontozás kockázatértékelési célból (például hitelbesorolás, biztosítási díjak megállapítása, csalások megelőzése, pénzmosás felderítése céljából); helymeghatározás, például mobilalkalmazások útján; hűségprogramok; viselkedésalapú reklám; wellness, fitness és egészségügyi adatok megfigyelése viselhető eszközökön keresztül; zárt láncú televízió; csatlakoztatott eszközök, például intelligens mérőberendezések, intelligens gépjárművek, lakásautomatizálás stb.

2.1.5 A SZEMÉLYES ADATOK KÜLÖNLEGES KATEGÓRIÁI, VALAMINT A BÜNTETŐJOGI FELELŐSSÉG MEGÁLLAPÍTÁSÁRA VONATKOZÓ HATÁROZATOKRA ÉS BŰNCSELEKMÉNYEKRE VONATKOZÓ ADATOK

A 37. cikk (1) bekezdésének c) pontja a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok kezelésére vonatkozik. Bár a rendelkezés az „és” kötőszót használja, a két feltétel egyidejűleg történő alkalmazásának nincs gyakorlati indoka. A szöveget ezért a *„vagy”* kötőszóval kell értelmezni.

2.2. Az adatfeldolgozó által kijelölt adatvédelmi tisztviselő:

A 37. cikk az adatvédelmi tisztviselő kijelölése tekintetében mind az adatkezelőkre,[17] mind az adatfeldolgozókra [18] vonatkozik. Attól függően, hogy ki felel meg a kötelező kijelölés kritériumainak, egyes esetekben csak az adatkezelő vagy csak az adatfeldolgozó, míg más esetekben az adatkezelő és az adatfeldolgozó is köteles adatvédelmi tisztviselőt kijelölni (e tisztviselőknek ezt követően együtt kell működniük).

Fontos megjegyezni, hogy még ha az adatkezelő eleget is tesz a kötelező kijelölés kritériumainak, az adatfeldolgozójának nem feltétlenül szükséges adatvédelmi tisztviselőt kijelölni. Ez azonban lehet egy jó gyakorlat.

Példák:

- Egy háztartási készülékeket egyetlen városban forgalmazó családi kisvállalkozás egy olyan adatfeldolgozó szolgáltatásait veszi igénybe, amelynek fő tevékenysége weboldalelemzési szolgáltatások nyújtása, valamint célzott reklám és marketing támogatása. A családi vállalkozás tevékenysége és ügyfelei alapján nem állapítható meg „nagymértékű” adatkezelés, figyelembe véve az ügyfelek kis számát és a viszonylag korlátozott tevékenységeket. A számos, e kisvállalkozáshoz hasonló ügyféllel rendelkező adatfeldolgozó tevékenységei összességében azonban nagymértékű adatkezelést jelentenek. Az adatfeldolgozónak ezért a

[17] Az adatkezelőt a 4. cikk 7. pontja olyan személyként vagy szervként határozza meg, amely a személyes adatok kezelésének céljait és eszközeit meghatározza.

[18] Az adatfeldolgozót a 4. cikk 8. pontja olyan személyként vagy szervként határozza meg, amely az adatkezelő nevében személyes adatokat kezel.

37. cikk (1) bekezdésének b) pontja alapján adatvédelmi tisztviselőt kell kijelölni. Ugyanakkor maga a családi vállalkozás nem köteles kijelölni adatvédelmi tisztviselőt.

- Egy csempegyártó középvállalkozás foglalkozás-egészségügyi szolgáltatások nyújtására egy olyan külső adatfeldolgozóval köt szerződést, amely számos hasonló ügyféllel rendelkezik. Az adatfeldolgozónak a 37. cikk (1) bekezdésének c) pontja értelmében adatvédelmi tisztviselőt kell kijelölni, feltéve, hogy az adatkezelés nagyméretű. Ugyanakkor a gyártó nem feltétlenül köteles adatvédelmi tisztviselő kijelölni.

Az adatfeldolgozó által kijelölt adatvédelmi tisztviselő az adatfeldolgozó szervezet azon tevékenységeit is felügyeli, amikor saját jogán jár el adatkezelőként (például személyzeti ügyek, informatika, logisztika területén).

23. Több szervezet által kijelölt közös adatvédelmi tisztviselő

A 37. cikk (2) bekezdése lehetővé teszi, hogy egy vállalkozáscsoport közös adatvédelmi tisztviselőt jelöljön ki, ha az adatvédelmi tisztviselő *„valamennyi tevékenységi helyről könnyen elérhető*". Az elérhetőség fogalma az adatvédelmi tisztviselő azon feladatára utal, hogy az érintettek[19] és a felügyeleti hatóság[20] felé, valamint a szervezeten belül is kapcsolattartóként szolgál, tekintettel arra, hogy az adatvédelmi tisztviselő egyik feladata az, hogy *„tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet […] szerinti kötelezettségeikkel kapcsolatban"*[21].

Annak biztosítása érdekében, hogy az adatvédelmi tisztviselő – függetlenül, hogy belső vagy külső – elérhető legyen, fontos, hogy az elérhetőségét megadják a GDPR követelményeinek megfelelően.[22]

Az adatvédelmi tisztviselőnek – szükség esetén egy csoport segítségével – képesnek kell lennie hatékonyan tájékoztatni az érintetteket[23] és együttműködni[24] az érintett felügyeleti hatóságokkal. Ez azt is jelenti, hogy a tájékoztatást a felügyeleti hatóságok és az érintettek által használt nyelven vagy nyelveken kell nyújtani. Az adatvédelmi tisztviselő rendelkezésre állása (akár fizikailag ugyanazon a helyen, mint a munkavállalók, forródróton vagy más biztonságos kommunikációs eszközön keresztül) elengedhetetlen annak biztosítása érdekében, hogy az érintettek képesek legyenek az adatvédelmi tisztviselőhöz fordulni.

---

[19] A 38. cikk (4) bekezdése: *„Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak."*

[20] A 39. cikk (1) bekezdésének e) pontja: *„az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele."*

[21] A 39. cikk (1) bekezdésének a) pontja.

[22] Lásd még az alábbi 2.6. pontot.

[23] A 12. cikk (1) bekezdése: *„Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében."*

[24] A 39. cikk (1) bekezdésének d) pontja: *„együttműködik a felügyeleti hatósággal"*.

A 37. cikk (3) bekezdése alapján több közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv közös adatvédelmi tisztviselőt jelölhet ki, az adott szervek szervezeti felépítésének és méretének figyelembevételével. A forrásokra és a tájékoztatásra ugyanazok a szempontok vonatkoznak. Tekintettel arra, hogy az adatvédelmi tisztviselő számos feladatot lát el, az adatkezelőnek vagy az adatfeldolgozónak gondoskodnia kell arról, hogy a közös adatvédelmi tisztviselő – szükség esetén egy csoport segítségével – hatékonyan elvégezhesse ezeket a feladatokat, annak ellenére, hogy több közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv számára jelölték ki.

2.4. Az adatvédelmi tisztviselő elérhető volta és működésének helye

A GDPR 4. szakasza szerint az adatvédelmi tisztviselőt ténylegesen el kell tudni érni.

Annak biztosítása érdekében, hogy az adatvédelmi tisztviselő elérhető legyen, a Munkacsoport azt ajánlja, hogy az adatvédelmi tisztviselő az Európai Unióban telepedjen le, függetlenül attól, hogy az adatkezelő vagy az adatfeldolgozó székhelye az Európai Unióban található-e.

Nem zárható ki azonban, hogy bizonyos esetekben, amikor az adatkezelő vagy az adatfeldolgozó tevékenységi helye nem az Európai Unióban található,[25] az adatvédelmi tisztviselő adott esetben hatékonyabban tudja ellátni tevékenységeit, ha az Unión kívül található.

2.5. Az adatvédelmi tisztviselő szakértelme és készségei

A 37. cikk (5) bekezdése úgy rendelkezik, hogy az adatvédelmi tisztviselőt *„szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a 39. cikkben említett feladatok ellátására való alkalmasság alapján kell kijelölni”*. A (97) preambulumbekezdés alapján a szakértői ismeretek szükséges szintjét az adatkezelő által végzett adatkezelés, valamint az általa kezelendő személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni.

- **A szakértelem szintje**

A szükséges szakértelem szintje nincs szigorúan meghatározva, arányosnak kell azonban lennie a szervezet által kezelt adatok érzékenységével, összetettségével és mennyiségével. Ha például az adatkezelési tevékenység különösen bonyolult, vagy nagy mennyiségű érzékeny adatot érint, az adatvédelmi tisztviselőnek adott esetben magasabb szintű szakértelemmel és támogatással kell rendelkezni. Szintén különbség van attól függően, hogy a szervezet rendszeresen továbbít-e személyes adatokat Európai Unión kívüli országba, vagy az ilyen adattovábbításra eseti alapon kerül sor. Az adatvédelmi tisztviselőt ezért körültekintően, a szervezeten belüli adatvédelmi kérdések megfelelő figyelembevételével kell kiválasztani.

- **Szakmai képességek**

Bár a 37. cikk (5) bekezdése nem határozza meg az adatvédelmi tisztviselő kijelölésekor figyelembe veendő szakmai képességeket, fontos elem, hogy az adatvédelmi tisztviselőknek szakértelemmel kell rendelkezni a nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén, valamint alaposan

[25] A területi hatállyal kapcsolatban lásd a GDPR 3. cikkét.

ismernie kell a GDPR-t. Hasznos továbbá, ha a felügyeleti hatóságok elősegítik az adatvédelmi tisztviselők megfelelő és rendszeres képzését.

Hasznos az üzletág és az adatkezelő szervezetének ismerete. Az adatvédelmi tisztviselőnek jól kell ismernie az általa végzendő adatkezelési műveleteket, valamint az adatkezelő információs rendszereit, adatbiztonsági és adatvédelmi igényeit.

Közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv esetében az adatvédelmi tisztviselőnek alaposan kell ismerni a szervezet igazgatási szabályait és eljárásait.

- **Képesség a feladatok ellátására**

Az adatvédelmi tisztviselő feladatainak teljesítésére vonatkozó képességét úgy kell értelmezni, hogy az mind a személyes tulajdonságaira és ismereteire, mind a szervezeten belüli jogállására vonatkozik. A személyes tulajdonságok közé tartozik például az integritás és a magas szintű szakmai morál; az adatvédelmi tisztviselő elsődleges feladata a GDPR-nak való megfelelés lehetővé tétele. Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában, és elősegíti a GDPR alapvető, például az adatok kezelésére vonatkozó elvekre,[26] az érintett jogaira,[27] a beépített és alapértelmezett adatvédelemre,[28] az adatkezelési tevékenységek nyilvántartására,[29] az adatkezelés biztonságára[30], valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra[31] vonatkozó rendelkezéseinek végrehajtását.

- **Az adatvédelmi tisztviselő feladatellátása szolgáltatási szerződés keretében**

Az adatvédelmi tisztviselő tevékenysége az adatkezelő, illetve adatfeldolgozó szervezetén kívül álló magánszeméllyel vagy szervezettel kötött szolgáltatási szerződés keretében is végezhető. Ez utóbbi esetben elengedhetetlen, hogy az adatvédelmi tisztviselő tevékenységeit ellátó szervezet minden tagja megfeleljen a GDPR 4. szakaszában 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 tisztviselői tevékenységek végzésére kötött szolgáltatási szerződés nem szüntethető meg jogellenesen, és az adatvédelmi tisztviselői feladatok elvégzését végző szervezet egyes tagjait sem lehet jogellenesen elbocsátani). Ugyanakkor az egyéni készségek és erősségek egyesíthetők, így több, egy csoportban dolgozó egyén hatékonyabban tudja kiszolgálni az ügyfeleit.

A jogi egyértelműség és a jó szervezés, valamint a csoport tagjai körében az összeférhetetlenség megelőzése érdekében ajánlott egyértelműen elosztani a feladatokat az adatvédelmi tisztviselői csoporton belül, valamint ügyfelenként egyetlen személyt vezető kapcsolattartóként és „felelős” személyként megbízni. Általában hasznos lenne ezeket a pontokat a szolgáltatási szerződésben meghatározni.

2.6. Az adatvédelmi tisztviselő elérhetőségének közzététele és arról való tájékoztatás

[26] II. fejezet.
[27] III. fejezet.
[28] 25. cikk.
[29] 30. cikk.
[30] 32. cikk.
[31] 33. és 34. cikk.

A 37. cikk (7) bekezdése előírja, hogy az adatkezelő vagy az adatfeldolgozó:

- közzéteszi az adatvédelmi tisztviselő elérhetőségét, és
- közli a felügyeleti hatóságokkal az adatvédelmi tisztviselő elérhetőségét.

E követelmények célja annak biztosítása, hogy az érintettek (a szervezeten belül és kívül) és a felügyeleti hatóságok könnyen és közvetlenül tudjanak fordulni az adatvédelmi tisztviselőhöz, anélkül, hogy kapcsolatba kellene lépniük a szervezet más részével. A titoktartás ugyanilyen fontos: például a munkavállalók nem szívesen nyújtanak be panaszt az adatvédelmi tisztviselőnél, ha közlésük bizalmas kezelése nem biztosított.
Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti (38. cikk (5) bekezdése).

Az adatvédelmi tisztviselő elérhetőségének olyan információkat kell tartalmazni, amelyek révén az érintettek és a felügyeleti hatóságok könnyen el tudják érni az adatvédelmi tisztviselőt (levelezési cím, erre a célra fenntartott telefonszám és/vagy erre a célra fenntartott e-mail cím). Adott esetben a nyilvánosság tájékoztatása céljából más kommunikációs eszközök is alkalmazhatók, például egy erre a célra fenntartott forródrót vagy a szervezet honlapján az adatvédelmi tisztviselőhöz vezető kapcsolatfelvételi űrlap.

A 37. cikk (7) bekezdése nem írja elő, hogy a közzétett elérhetőségnek tartalmazni kell az adatvédelmi tisztviselő nevét. Bár ez jó gyakorlat lehet, az adatkezelőnek vagy az adatfeldolgozónak és az adatvédelmi tisztviselőnek kell eldöntenie, hogy ez az adott körülmények között szükségesnek vagy hasznosnak bizonyul-e.[32]

Mindazonáltal 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 (39. cikk (1) bekezdésének e) pontja).

A Munkacsoport jó gyakorlatként azt is ajánlja, hogy a szervezet tájékoztassa alkalmazottait az adatvédelmi tisztviselő nevéről és elérhetőségéről. Például az adatvédelmi tisztviselő neve és elérhetősége az intraneten, a belső telefonkönyvben és a szervezeti ábrákon is feltüntethető.

3 Az adatvédelmi tisztviselő jogállása

3.1. Az adatvédelmi tisztviselőnek a személyes adatok védelmével kapcsolatos összes ügybe történő bekapcsolódása

[32] Megjegyzendő, hogy a 37. cikk (7) bekezdésétől eltérően a 33. cikk (3) bekezdésének b) pontja, amely adatvédelmi incidens esetén a felügyeleti hatóság és az érintettek részére közlendő információkat rögzíti, kifejezetten előírja az adatvédelmi tisztviselő nevének (nem csak az elérhetőségének) a megadását.

A GDPR 38. cikke értelmében az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő *„a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon”.*

Rendkívül fontos, hogy az adatvédelmi tisztviselő vagy csoportja a lehető legkorábbi szakaszban bekapcsolódjon az adatvédelemmel kapcsolatos valamennyi ügybe. Az adatvédelmi hatásvizsgálatokkal kapcsolatban a GDPR kifejezetten rendelkezik az adatvédelmi tisztviselő korai bevonásáról, és előírja, hogy az adatkezelő köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát az ilyen hatásvizsgálatok elvégzésekor.[33] Annak biztosítása, hogy az adatvédelmi tisztviselőt előzetesen tájékoztatják és konzultálnak vele, megkönnyíti a GDPR-nak való megfelelést, előmozdítja a beépített adatvédelmet, ezért általános szervezetirányítási eljárásként kell alkalmazni. Ezenkívül fontos, hogy az adatvédelmi tisztviselőt a szervezeten belül tárgyalópartnernek lehessen tekinteni, és hogy tagja legyen a szervezeten belüli adatkezelési tevékenységekkel foglalkozó munkacsoportoknak.

Következésképpen, a szervezetnek biztosítania kell például az alábbiakat:

- Az adatvédelmi tisztviselőt rendszeresen meghívják a közép- és felsővezetés megbeszéléseire.
- A részvétele ajánlott, amikor adatvédelmi vonatkozású döntéseket hoznak. Minden releváns információt időben kell átadni az adatvédelmi tisztviselőnek annak érdekében, hogy megfelelő tanácsot adhasson.
- Az adatvédelmi tisztviselő véleményét mindig kellő súllyal kell figyelembe venni. Nézetkülönbség esetén a Munkacsoport jó gyakorlatként azt ajánlja, hogy rögzítsék annak okát, hogy miért nem az adatvédelmi tisztviselő tanácsa szerint járnak el.
- Az adatvédelmi tisztviselővel haladéktalanul konzultálni kell, ha adatvédelmi vagy más incidens következett be.

Adott esetben az adatkezelő vagy az adatfeldolgozó olyan adatvédelmi iránymutatásokat vagy programokat dolgozhat ki, amelyek meghatározzák, hogy mely esetekben kell az adatvédelmi tisztviselővel konzultálni.

3.2. Szükséges források

A GDPR 38. cikkének (2) bekezdése értelmében a szervezet támogatja az adatvédelmi tisztviselőt azáltal, hogy *„biztosítja számára azokat az forrásokat, amelyek [...] feladat[ai] végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek”.* Különösen a következőket kell figyelembe venni:

- Az adatvédelmi tisztviselő tevékenységének aktív támogatása a felsővezetés részéről (például igazgatósági szinten).
- Az adatvédelmi tisztviselő részére elegendő idő biztosítása a feladatai ellátására. Ez különösen fontos abban az esetben, ha részmunkaidős belső adatvédelmi tisztviselőt jelölnek ki, vagy ha a külső adatvédelmi tisztviselő az adatvédelmi tevékenységet más feladatok mellett végzi. Ellenkező esetben az egymásnak ellentmondó prioritások eredményeként az adatvédelmi

[33] A 35. cikk (2) bekezdése.

tisztviselő elhanyagolhatja a feladatait. Rendkívül fontos, hogy az adatvédelmi tisztviselő elegendő időt szenteljen a feladatokra. Jó gyakorlat az adatvédelmi tisztviselő által végzett tevékenység időtartamának százalékos meghatározása abban az esetben, ha a feladatellátás nem teljes munkaidőben történik. További jó gyakorlat a feladat elvégzéséhez szükséges időt, az adatvédelmi tisztviselő által végzett feladatok megfelelő prioritási szintjének meghatározása, valamint az adatvédelmi tisztviselő (vagy a szervezet) számára munkaterv készítése.

- Adott esetben megfelelő támogatás a pénzügyi források, infrastruktúra (helyiségek, berendezések, eszközök) és személyzet tekintetében.
- Valamennyi alkalmazott hivatalos tájékoztatása az adatvédelmi tisztviselő kijelöléséről annak biztosítása érdekében, hogy jelenléte és működése ismertté váljon a szervezeten belül.
- Egyéb, például a személyzeti, jogi, informatikai, biztonsági stb. szolgáltatásokhoz való hozzáférés biztosítása, így az adatvédelmi tisztviselők lényeges támogatást, ráfordítást és információkat szerezhetnek e szolgáltatások részéről.
- Folyamatos képzés. Az adatvédelmi tisztviselőknek lehetőséget kell adni arra, hogy naprakészek maradjanak az adatvédelem terén elért fejlődések tekintetében. A cél az, hogy folyamatosan növeljék az adatvédelmi tisztviselők szaktudásának szintjét, és ösztönözni kell őket arra, hogy vegyenek részt adatvédelmi tanfolyamokon és a szakmai fejlődés egyéb formáiban, például a magánélet védelmével foglalkozó fórumokon, műhelyekben stb.
- Tekintettel a szervezet méretére és szerkezetére, előfordulhat, hogy létre kell hoznia egy – az adatvédelmi tisztviselőből és alkalmazottaiból álló – adatvédelmi tisztviselői csoportot. Ilyen esetekben világosan meg kell határozni a csoport belső struktúráját, valamint az egyes tagok feladatait és felelősségét. Hasonlóképpen, ha az adatvédelmi tisztviselő tevékenységét külső szolgáltató végzi, az ennél a szervezetnél dolgozó személyek csoportja az ügyfél számára kijelölt vezető kapcsolattartó felelőssége mellett csoportként ténylegesen elláthatja az adatvédelmi tisztviselő feladatait.

Általában véve, minél összetettebbek és / vagy érzékenyebbek az adatkezelési műveletek, annál több forrást kell biztosítani az adatvédelmi tisztviselőnek. Az adatvédelmi tevékenységnek hatékonynak kell lennie és megfelelő forrásokkal kell rendelkeznie az elvégzendő adatkezelés tekintetében.

3.3. A „kötelezettségeik és feladataik független ellátásával” kapcsolatos iránymutatások:

A 38. cikk (3) bekezdése bizonyos alapvető garanciákat biztosít annak biztosítására, hogy az adatvédelmi tisztviselők képesek legyenek a szervezetükön belül megfelelő szintű önállósággal ellátni feladataikat. Mindenekelőtt, az adatkezelő és az adatfeldolgozó köteles biztosítani, hogy az adatvédelmi tisztviselő *„a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el”*. A (97) preambulumbekezdés ezt kiegészíti azzal, hogy az adatvédelmi tisztviselők *„– függetlenül attól, hogy az adatkezelő alkalmazásában állnak-e – módjában kell, hogy álljon kötelezettségeik és feladataik független ellátása”*.

Ez azt jelenti, hogy a 39. cikk szerinti feladataik teljesítése során az adatvédelmi tisztviselők nem utasíthatók arra, hogyan kezeljenek egy ügyet, például milyen eredményeket kell elérni, hogyan kell kivizsgálni egy panaszt, vagy kell-e konzultálni a felügyelő hatósággal. Ezenkívül nem utasíthatók arra, hogy az adatvédelmi joggal kapcsolatos valamely ügyben – például a jogszabály egy adott értelmezését illetően – egy bizonyos álláspontot képviseljenek.

Az adatvédelmi tisztviselők önállósága azonban nem jelenti azt, hogy döntéshozatali jogkörük meghaladja a 39. cikk szerinti feladataikat.

Az adatkezelő vagy az adatfeldolgozó felelős továbbra is az adatvédelmi jogszabályoknak való megfelelésért, és képesnek kell lenniük e megfelelés igazolására.[34] Ha az adatkezelő vagy az adatfeldolgozó olyan döntéseket hoz, amelyek nem egyeztethetők össze a GDPR-rel és az adatvédelmi tisztviselő tanácsával, akkor az adatvédelmi tisztviselőnek lehetőséget kell biztosítani arra, hogy eltérő véleményét bemutathassa a legfelső vezetésnek, valamint a döntéshozó személyeknek. E tekintetben a 38. cikk (3) bekezdése úgy rendelkezik, hogy az adatvédelmi tisztviselő *„közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel”*. Az ilyen közvetlen jelentéstétel biztosítja, hogy a felső vezetés (például az igazgatótanács) ismerje – az adatvédelmi tisztviselőnek az adatkezelő vagy adatfeldolgozó tájékoztatására és tanácsadására irányuló küldetése részeként – az adatvédelmi tisztviselő tanácsát és ajánlásait. A közvetlen jelentéstétel másik példája a legfelső vezetés részére éves jelentés készítése az adatvédelmi tisztviselő tevékenységeiről.

3.4. Az adatvédelmi tisztviselő elbocsátása és szankcionálása a feladatai ellátásával összefüggésben

A 38. cikk (3) bekezdése értelmében az adatvédelmi tisztviselőket *„feladatai[k] ellátásával összefüggésben nem bocsáthatj[ák] el és szankcióval nem sújthatj[ák]”*.

Ez a követelmény erősíti az adatvédelmi tisztviselők önállóságát, és biztosítja, hogy függetlenül járnak el, és megfelelő védelmet élveznek az adatvédelmi feladataik ellátása során.

A GDPR alapján a szankció kizárólag akkor tilos, ha azt az adatvédelmi tisztviselőként végzett feladatainak ellátása következményeként szabták ki az adatvédelmi tisztviselőre. Például az adatvédelmi tisztviselő úgy ítélheti meg, hogy egy adott adatkezelés nagy valószínűséggel magas kockázattal járhat, és adatvédelmi hatásvizsgálat elvégzését tanácsolja az adatkezelőnek vagy az adatfeldolgozónak, de az adatkezelő vagy az adatfeldolgozó nem ért egyet az adatvédelmi biztos értékelésével. Ebben az esetben az adatvédelmi tisztviselőt nem lehet elbocsátani e tanácsa miatt.

Sokféle szankció létezhet, amelyek lehetnek közvetlenek vagy közvetettek. Például az adatvédelmi tisztviselőt nem léptetik elő vagy az előléptetést késleltetik: megakadályozzák az előremenetelt; megtagadják azokat a juttatásokat, amelyeket a többi alkalmazott megkap. Nem szükséges, hogy ezeket a szankciókat ténylegesen alkalmazzák is, a puszta fenyegetés is elegendő, ha ezzel az adatvédelmi tisztviselőt az adatvédelmi tisztviselői tevékenységeivel kapcsolatban szankcionálják.

A szokásos irányítási szabályok keretében, valamint bármely más alkalmazottra vagy vállalkozóra vonatkozó alkalmazandó nemzeti szerződési vagy munkajogi, büntetőjogi szabályok alapján, az adatvédelmi tisztviselőt is jogszerűen el lehet bocsátani az adatvédelmi tisztviselőként végzett feladataitól eltérő okból (például lopás, fizikai, pszichológiai vagy szexuális zaklatás vagy más hasonlóan súlyos kötelességszegés esetén).

Ebben az összefüggésben meg kell jegyezni, hogy a GDPR nem határozza meg, hogyan és mikor bocsátható el vagy cserélhető le az adatvédelmi tisztviselő. Minél stabilabb azonban az adatvédelmi tisztviselő szerződése, és minél több garancia létezik a jogellenes elbocsátással szemben, annál

[34] Az 5. cikk (2) bekezdése.

valószínűbb, hogy független módon járhatnak el. Ezért a Munkacsoport üdvözölné a szervezetek ilyen irányú erőfeszítéseit.

3.5. Összeférhetetlenség

A 38. cikk (6) bekezdése alapján az adatvédelmi tisztviselő *„más feladatokat is elláthat”*. A rendelkezés előírja, hogy a szervezetnek biztosítani kell, hogy *„e feladatokból ne fakadjon összeférhetetlenség”*.

Az összeférhetetlenség hiánya szorosan kapcsolódik a független működéshez fűződő követelményhez. Bár az adatvédelmi tisztviselőknek lehetnek más feladataik, csak olyan egyéb feladatokkal bízhatók meg, amelyek nem okoznak összeférhetetlenséget. Ez különösen azt jelenti, hogy az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit. Az egyes szervezetek sajátos szervezeti felépítése miatt ezt eseti alapon kell megállapítani.

Ökölszabályként, az összeférhetetlenséget okozó szervezeten belüli pozíciók lehetnek a felsővezetői pozíciók (például vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, marketing osztályvezető, humán erőforrás 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. Ezenkívül összeférhetetlenség merülhet fel például, ha a külső adatvédelmi tisztviselőt az adatkezelő vagy az adatfeldolgozó bíróság előtti képviseletére kérik fel adatvédelmi kérdéseket érintő ügyekben.

A szervezet tevékenységeitől, méretétől és szerkezetétől függően jó gyakorlat lehet az adatkezelők vagy az adatfeldolgozók számára:

- azon pozíciók meghatározása, amelyek összeegyeztethetetlenek az adatvédelmi tisztviselő tevékenységével
- e célból belső szabályok megállapítása az összeférhetetlenség elkerülése érdekében
- általánosabb magyarázat nyújtása az összeférhetetlenségről
- e követelmény tudatosításának módjaként nyilatkozat arról, hogy az adatvédelmi tisztviselő nem összeférhetetlen az adatvédelmi tisztviselőként végzett feladatai tekintetében
- a szervezet belső szabályaiban biztosítékok szerepeltetése, és annak biztosítása, hogy az adatvédelmi tisztviselői pozíció betöltésére vagy szolgáltatási szerződés megkötésére vonatkozó felhívás kellően pontos és részletes az összeférhetetlenség elkerülése érdekében. Ebben az összefüggésben emlékeztetni kell arra is, hogy az összeférhetetlenség számos formát ölthet attól függően, hogy az adatvédelmi tisztviselőt a szervezeten belülről vagy kívülről választják-e ki

4 Az adatvédelmi tisztviselő feladatai

4.1. A GDPR-nek való megfelelés ellenőrzése

A 39. cikk (1) bekezdésének b) pontja kötelezi az adatvédelmi tisztviselőt – többek között – a GDPR-nak való megfelelés ellenőrzésére. A (97) preambulumbekezdés emellett úgy szól, hogy az

adatvédelmi tisztviselő *„az adatkezelőt vagy az adatfeldolgozót az e rendeletnek való belső megfelelés ellenőrzésében [...] segíti”*.

A megfelelés ellenőrzésére vonatkozó feladatai részeként az adatvédelmi tisztviselők különösen az alábbiakat tehetik:

- 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

A megfelelés ellenőrzése nem jelenti azt, hogy az adatvédelmi tisztviselő személyesen felelős a rendelkezések be nem tartásáért. A GDPR egyértelművé teszi, hogy nem az adatvédelmi tisztviselő, hanem az adatkezelő köteles *„megfelelő technikai és szervezési intézkedéseket [...] végre[hajtani] annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik”* (24. cikk (1) bekezdése). Az adatvédelmi rendelkezések betartása nem az adatvédelmi tisztviselő, hanem az adatkezelő szervezeti felelőssége.

4.2. Az adatvédelmi tisztviselő szerepe az adatvédelmi hatásvizsgálat tekintetében

A 35. cikk (1) bekezdése alapján az adatkezelő feladata – szükség esetén – az adatvédelmi hatásvizsgálat elvégzése. Ugyanakkor az adatvédelmi tisztviselő nagyon fontos és hasznos szerepet tölthet be az adatkezelő támogatásában. A beépített adatvédelem elve értelmében a 35. cikk (2) bekezdése kifejezetten előírja, hogy az adatkezelő az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő *„szakmai tanácsát köteles kikérni”*. A 39. cikk (1) bekezdésének c) pontja pedig azt a feladatot írja elő az adatvédelmi tisztviselő részére, hogy *„kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat 35. cikk szerinti elvégzését”*.

A Munkacsoport azt ajánlja, hogy az adatkezelő az adatvédelmi tisztviselő szakmai tanácsát különösen az alábbi kérdésekben kérje ki: [35]

- 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 a GDPR-nek

Ha az adatkezelő nem ért egyet az adatvédelmi tisztviselő tanácsával, akkor az adatvédelmi hatásvizsgálat dokumentációjában kifejezetten indokolnia kell, hogy miért nem vették figyelembe a tanácsot.[36]

[35] A 39. cikk (1) bekezdése határozza meg az adatvédelmi tisztviselő feladatait, és jelzi, hogy az adatvédelmi tisztviselőnek *„legalább”* a következő feladatokat kell ellátni. Ezért nincs akadálya annak, hogy az adatkezelő az adatvédelmi tisztviselőt a 39. cikk (1) bekezdésében kifejezetten említettektől eltérő feladatokkal is megbízza, vagy hogy ezeket a feladatokat részletesebben meghatározza.

A Munkacsoport emellett azt ajánlja, hogy az adatkezelő egyértelműen határozza meg – különösen az adatvédelmi hatásvizsgálat elvégzésével kapcsolatban – az adatvédelmi tisztviselő pontos feladatkörét és jogkörét, például az adatvédelmi tisztviselő szerződésében, valamint a munkavállalók, a vezetés (és adott esetben egyéb érdekeltek) számára nyújtott tájékoztatás formájában.

4.3. Együttműködés a felügyeleti hatósággal és kapcsolattartóként való eljárás

A 39. cikk (1) bekezdés d) és e) pontja alapján az adatvédelmi tisztviselő *„együttműködik a felügyeleti hatósággal”*, és *„az adatkezeléssel összefüggő ügyekben – ideértve a 36. cikkben említett előzetes konzultációt is – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.”*

Ezek a feladatok az adatvédelmi tisztviselőnek a jelen iránymutatás bevezető részében említett „elősegítő” szerepét jelzik. Az adatvédelmi tisztviselő kapcsolattartó pontként szolgál, hogy elősegítse a felügyeleti hatóság hozzáférését az 57. cikkben említett feladatok teljesítéséhez szükséges dokumentumokhoz és információkhoz, valamint az 58. cikkben említett vizsgálati, korrekciós, engedélyezési és tanácsadási hatásköre gyakorlásához. Amint már említettük, az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti (38. cikk (5) bekezdése). A titoktartási, illetve bizalmas kezelésre vonatkozó kötelezettség azonban nem tiltja, hogy az adatvédelmi tisztviselő a felügyeleti hatósághoz forduljon és kikérje tanácsát. A 39. cikk (1) bekezdésének e) pontja szerint az adatvédelmi tisztviselő adott esetben bármely egyéb kérdésben konzultációt folytat a felügyeleti hatósággal.

4.4. Kockázatalapú megközelítés

A 39. cikk (2) bekezdése értelmében az adatvédelmi tisztviselő feladatait *„az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi”*.

Ez a cikk egy általános és a józan ésszel kapcsolatos elvre emlékeztet, amely adott esetben az adatvédelmi tisztviselő mindennapi munkájának számos elemére vonatkozhat. A rendelkezés lényegében azt írja elő, hogy az adatvédelmi tisztviselők rangsorolják a tevékenységeiket, és a magasabb adatvédelmi kockázatot jelentő ügyekre összpontosítsanak. Ez nem jelenti azt, hogy nem kell ellenőrizniük az olyan adatkezelési műveletek megfelelését, amelyek viszonylag alacsonyabb kockázati szintet jelentenek, hanem arra utal, hogy elsősorban a magasabb kockázatú területekre kell összpontosítaniuk.

Ez a szelektív és gyakorlatias megközelítés segíti az adatvédelmi tisztviselőt az adatkezelő részére az azzal kapcsolatos tanácsok nyújtásában, hogy milyen módszereket alkalmazzon az adatvédelmi hatásvizsgálat elvégzésekor, mely területeket kell belső vagy külső adatvédelmi auditnak alávetni,

[36] A 24. cikk (1) bekezdése szerint: *„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.”*

milyen belső képzéseket kell biztosítani az adatkezelési tevékenységekért felelős alkalmazottaknak vagy vezetésnek, és mely adatkezelési műveletek igényelnek több időt és forrást.

4.5. Az adatvédelmi tisztviselő szerepe a nyilvántartások tekintetében

A 30. cikk (1) és (2) bekezdése alapján nem az adatvédelmi tisztviselő, hanem az adatkezelő vagy az adatfeldolgozó köteles *„a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet[ni]”*, vagy *„nyilvántartást vezet[ni] az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról”.*

A gyakorlatban az adatvédelmi tisztviselők gyakran készítenek és vezetnek nyilvántartást az adatkezelési műveletekről a személyes adatok kezelését végző szervezeti egységek által a részére bocsátott információk alapján. Ezt a gyakorlatot számos hatályos nemzeti jogszabály, valamint az uniós intézmények és szervek adatvédelmi szabályai hozták létre.[37]

A 39. cikk (1) bekezdése az adatvédelmi tisztviselő minimálisan elvégzendő feladatait sorolja fel. Ezért nincs akadálya annak, hogy az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt megbízza az adatkezelő vagy az adatfeldolgozó felelősségébe tartozóan végzett adatkezelési műveletekről történő nyilvántartás vezetésével. Ezt a nyilvántartást 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.

Mindenesetre a 30. cikk értelmében előírt nyilvántartást olyan eszközként is kell tekinteni, amely lehetővé teszi az adatkezelő és – kérésre – 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.

[37] A 45/2001/EK rendelet 24. cikke (1) bekezdésének d) pontja.

5 MELLÉKLET - IRÁNYMUTATÁS AZ ADATVÉDELMI TISZTVISELŐKKEL KAPCSOLATBAN TUDNIVALÓK

Jelen melléklet célja, hogy egyszerűsített és könnyen olvasható formában választ adjon néhány kulcsfontosságú kérdésre, amelyek a szervezetek részéről merülhetnek fel az általános adatvédelmi rendeletnek (a továbbiakban: GDPR) az adatvédelmi tisztviselő kijelölésére vonatkozó új előírásaival kapcsolatban.

Az adatvédelmi tisztviselő kijelölése

1 Milyen szervezeteknek kell kijelölni adatvédelmi tisztviselőt?

Adatvédelmi tisztviselőt kell kijelölni:

- ha az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik (attól függetlenül, hogy milyen adatokat kezelnek)
- ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé
- ha az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban

Megjegyzendő, hogy az uniós vagy tagállami jog más esetekben is előírhatja adatvédelmi tisztviselő kijelölését. Végül, abban az esetben, ha nem kötelező adatvédelmi tisztviselőt kijelölni, a szervezetek számára bizonyos esetekben hasznosnak bizonyulhat, ha önkéntes alapon jelölnek ki adatvédelmi tisztviselőt. A 29. cikk szerinti munkacsoport (a továbbiakban: Munkacsoport) támogatja ezeket a törekvéseket. Amikor egy szervezet önkéntes alapon jelöl ki adatvédelmi tisztviselőt, ugyanazok a követelmények vonatkoznak e tisztviselő kijelölésére, a jogállására és a feladataira, mintha a kijelölés kötelező lenne.

Forrás: GDPR 37. cikkének (1) bekezdése

2 Mit jelent a „fő tevékenységek” fogalma?

A „fő tevékenységek” az adatkezelő vagy az adatfeldolgozó céljainak eléréséhez szükséges legfontosabb műveleteket jelentik. E tevékenységek körébe tartozik az összes olyan tevékenység is, amely során az adatkezelés az adatkezelő vagy az adatfeldolgozó tevékenységének elválaszthatatlan részét képezi. Az egészségügyi adatok kezelését, például a betegek egészségügyi nyilvántartását a kórházak egyik fő tevékenységének kell tekinteni, emiatt a kórházaknak adatvédelmi tisztviselőt kell kijelölni.

Másrészről, minden szervezet végez bizonyos támogató tevékenységeket, például fizetést ad az alkalmazottaknak, vagy általános informatikai támogató tevékenységeket végez. Ezek a szervezet fő tevékenységéhez vagy fő vállalkozási tevékenységéhez szükséges támogatási funkciók példái. Annak ellenére, hogy ezek a tevékenységek szükségesek vagy nélkülözhetetlenek, általában nem fő tevékenységnek, hanem inkább járulékos funkcióknak tekinthetők.

Forrás: GDPR 37. cikke (1) bekezdésének b) és c) pontja

3 Mit jelent a „nagy mértékű / nagy számban történő” kifejezés?

A GDPR nem határozza meg, hogy mit jelent a nagymértékű, illetve nagy számban történő adatkezelés. A Munkacsoport azt ajánlja, hogy különösen a következő tényezőket vegyék figyelembe annak meghatározásakor, hogy az adatkezelés nagymértékű-e, illetve nagy számban történik-e:

- az érintettek száma - akár egy 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

Példák a nagymértékű vagy nagy számban történő adatkezelésre:

- a betegek adatainak kezelése a kórház szokásos működése keretében
- városi tömegközlekedést használó személyek utazási adatainak kezelése (például menetjegyek nyomon követése)
- egy nemzetközi gyorsétteremlánc ügyfeleire vonatkozó valós idejű helymeghatározási adatok statisztikai célú kezelése egy ilyen tevékenység végzésére specializálódott adatkezelő útján
- ügyféladatok kezelése egy biztosító társaság vagy egy bank szokásos üzletmenete keretében
- személyes adatok keresőmotor általi kezelése viselkedésalapú reklám céljából
- adatok (tartalom, forgalom, hely) kezelése telefon- vagy internetszolgáltatók által

Példák arra, mi nem tartozik a nagymértékű vagy nagy számban történő adatkezelés körébe:

- betegek adatainak kezelése egy adott szakorvos által
- a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok kezelése egy adott ügyvéd által

Forrás: GDPR 37. cikke (1) bekezdésének b) és c) pontja

4 Mit jelent a „rendszeres és szisztematikus megfigyelés”?

A GDPR nem határozza meg az érintettek rendszeres és szisztematikus megfigyelésének fogalmát, de egyértelműen magában foglalja az interneten történő nyomon követés és profilalkotás valamennyi formáját, ideértve a viselkedésalapú reklám céljából történő adatkezelést is. A megfigyelés fogalma azonban nem korlátozódik az online környezetre.

Példák olyan tevékenységekre, amelyek során az érintettek rendszeres és szisztematikus megfigyelésére kerülhet sor: távközlési hálózat működtetése; távközlési szolgáltatások nyújtása; célközönség e-mail alapú újbóli meghatározása; adatvezérelt marketing tevékenységek; profilalkotás és pontozás kockázatértékelési célból (például hitelbesorolás, biztosítási díjak megállapítása, csalások megelőzése, pénzmosás felderítése céljából); helymeghatározás, például mobilalkalmazások útján; hűségprogramok; viselkedésalapú reklám; wellness, fitness és egészségügyi adatok megfigyelése viselhető eszközökön keresztül; zárt láncú televízió; csatlakoztatott eszközök, például intelligens mérőberendezések, intelligens gépjárművek, lakásautomatizálás stb.

A Munkacsoport értelmezése szerint a „rendszeres” kifejezés jelentése az alábbiak közül egy vagy több:

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

A Munkacsoport értelmezése szerint a „szisztematikus” kifejezés jelentése az alábbiak közül egy vagy több:

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

Forrás: GDPR 37. cikke (1) bekezdésének b) pontja

5 A szervezetek közösen is kijelölhetnek adatvédelmi tisztviselőt? Ha igen, milyen feltételekkel?

Igen. Egy vállalkozáscsoport közös adatvédelmi tisztviselőt jelölhet ki, ha az adatvédelmi tisztviselő *„valamennyi tevékenységi helyről könnyen elérhető*”. Az elérhetőség fogalma az adatvédelmi tisztviselő azon feladatára utal, hogy az érintettek és a felügyeleti hatóság felé, valamint a szervezeten belül is kapcsolattartóként szolgál. Annak biztosítása érdekében, hogy az adatvédelmi tisztviselő – függetlenül, hogy belső vagy külső – elérhető legyen, fontos, hogy megadják az elérhetőségét. Az adatvédelmi tisztviselőnek – szükség esetén egy csoport segítségével – képesnek kell lennie hatékonyan tájékoztatni az érintetteket és együttműködni az érintett felügyeleti hatóságokkal. Ez azt jelenti, hogy a tájékoztatást a felügyeleti hatóságok és az érintettek által használt nyelven vagy nyelveken kell nyújtani. Az adatvédelmi tisztviselő rendelkezésre állása (akár fizikailag ugyanazon a helyen, mint a munkavállalók, forródróton vagy más biztonságos kommunikációs eszközön keresztül) elengedhetetlen annak biztosítása érdekében, hogy az érintettek képesek legyenek az adatvédelmi tisztviselőhöz fordulni.

Több közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv közös adatvédelmi tisztviselőt jelölhet ki az adott szervek szervezeti felépítésének és méretének figyelembevételével. A forrásokra és a tájékoztatásra ugyanazok a szempontok vonatkoznak. Tekintettel arra, hogy az adatvédelmi tisztviselő számos feladatot lát el, az adatkezelőnek vagy az adatfeldolgozónak gondoskodnia kell arról, hogy a közös adatvédelmi tisztviselő – szükség esetén egy csoport segítségével – hatékonyan elvégezhesse ezeket a feladatokat, annak ellenére, hogy több közhatalmi szerv vagy egyéb, közfeladatot ellátó szerv számára jelölték ki.

Forrás: GDPR 37. cikkének (2) és (3) bekezdése

6 Hol kell tartózkodnia az adatvédelmi tisztviselőnek?

Annak biztosítása érdekében, hogy az adatvédelmi tisztviselő elérhető legyen, a Munkacsoport azt ajánlja, hogy az adatvédelmi tisztviselő az Európai Unióban telepedjen le, függetlenül attól, hogy az adatkezelő vagy az adatfeldolgozó székhelye az Európai Unióban található-e. Nem zárható ki azonban, hogy bizonyos esetekben, amikor az adatkezelő vagy az adatfeldolgozó tevékenységi helye nem az Európai Unióban található, az adatvédelmi tisztviselő adott esetben hatékonyabban tudja ellátni tevékenységeit, ha az Unión kívül található.

7 Ki lehet jelölni külső adatvédelmi tisztviselőt?

Igen. Az adatvédelmi tisztviselő az adatkezelő vagy az adatfeldolgozó alkalmazottja lehet (belső adatvédelmi tisztviselő), vagy szolgáltatási szerződés keretében láthatja el a feladatait. Ez azt jelenti,

hogy ki lehet jelölni külső adatvédelmi tisztviselőt, és ebben az esetben a tevékenysége magánszeméllyel vagy szervezettel kötött szolgáltatási szerződés keretében is végezhető.

Ha az adatvédelmi tisztviselő tevékenységét külső szolgáltató végzi, az ennél a szervezetnél dolgozó személyek csoportja az ügyfél vonatkozásában kijelölt vezető kapcsolattartó és „felelős személy" felelőssége mellett csoportként ténylegesen elláthatja az adatvédelmi tisztviselő feladatait. Ebben az esetben elengedhetetlen, hogy az adatvédelmi tisztviselő tevékenységeit ellátó külső szervezet minden tagja megfeleljen a GDPR összes alkalmazandó követelményének.

A jogi egyértelműség és a jó szervezés, valamint a csoport tagjait illetően az összeférhetetlenség megelőzése érdekében az iránymutatás szerint ajánlott egyértelműen elosztani a feladatokat az adatvédelmi tisztviselői csoporton belül, valamint az ügyfél vonatkozásában egyetlen személyt vezető kapcsolattartóként és „felelős" személyként megbízni.

Forrás: GDPR 37. cikkének (6) bekezdése

8 Milyen szakmai képességekkel kell rendelkeznie az adatvédelmi tisztviselőnek?

Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a feladatai ellátására való alkalmasság alapján kell kijelölni.

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 és támogatással kell rendelkezni.

Releváns készségek és szakértelem 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

Forrás: GDPR 37. cikkének (5) bekezdése

9 Milyen forrásokat kell biztosítania az adatkezelőnek vagy az adatfeldolgozónak az adatvédelmi tisztviselő részére?

Az adatvédelmi tisztviselőnek rendelkeznie kell a feladatai ellátásához szükséges forrásokkal.

Az adatkezelési műveletek jellegétől, valamint a szervezet tevékenységeitől és méretétől függően a következő forrásokat kell biztosítani az adatvédelmi tisztviselő részére:

- az adatvédelmi tisztviselő tevékenységének aktív támogatása a felsővezetés részéről
- az adatvédelmi tisztviselő részére elegendő idő biztosítása a feladatai ellátására
- adott esetben megfelelő támogatás a pénzügyi források, infrastruktúra (helyiségek, berendezések, eszközök) és személyzet tekintetében
- az összes alkalmazott hivatalos tájékoztatása az adatvédelmi tisztviselő kijelöléséről
- a szervezeten belüli egyéb szolgáltatásokhoz való hozzáférés biztosítása, így az adatvédelmi tisztviselők lényeges támogatást, ráfordítást és információkat szerezhetnek e szolgáltatások részéről
- folyamatos képzés

Forrás: GDPR 38. cikkének (2) bekezdése

10 Milyen biztosítékok teszik lehetővé az adatvédelmi tisztviselő feladatainak független ellátását? Mit jelent az „összeférhetetlenség”?

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 szankcionálják az adatvédelmi tisztviselőt a feladatai ellátásával összefüggésben
- nem okoz összeférhetetlenséget más lehetséges feladatok ellátása

Az adatvédelmi tisztviselő által végzett más feladatokból nem fakadhat összeférhetetlenség. Ez először is azt jelenti, hogy az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit. Az egyes szervezetek sajátos szervezeti felépítése miatt ezt eseti alapon kell megállapítani.

Ökölszabályként, az összeférhetetlenséget okozó szervezeten belüli pozíciók lehetnek a felsővezetői pozíciók (például vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, marketing osztályvezető, humán erőforrás 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. Ezenkívül összeférhetetlenség merülhet fel például, ha a külső adatvédelmi tisztviselőt az adatkezelő vagy az adatfeldolgozó bíróság előtti képviseletére kérik fel adatvédelmi kérdéseket érintő ügyekben.

Forrás: GDPR 38. cikkének (3) és (6) bekezdése

Az adatvédelmi tisztviselő feladatai

11 Mit jelent a „megfelelés ellenőrzése”?

A megfelelés ellenőrzésére vonatkozó feladatai részeként az adatvédelmi tisztviselők különösen az alábbiakat tehetik:

- 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

Forrás: GDPR 39. cikke (1) bekezdésének b) pontja

12 Az adatvédelmi tisztviselő személyesen felelős az adatvédelmi követelmények be nem tartásáért?

Nem. Az adatvédelmi tisztviselőket nem terheli személyes felelősség az adatvédelmi követelmények be nem tartásáért. Az adatkezelőnek vagy az adatfeldolgozónak kell biztosítani és bizonyítani, hogy a feldolgozás a GDPR rendelkezéseivel összhangban történik. Az adatvédelmi rendelkezések betartásáért az adatkezelő vagy az adatfeldolgozó felelős.

13 Melyek az adatvédelmi tisztviselő feladatai az adatvédelmi hatásvizsgálatok és az adatkezelési tevékenységek nyilvántartása tekintetében?

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

Az adatkezelési tevékenységek nyilvántartását illetően nem az adatvédelmi tisztviselőnek, hanem az adatkezelőnek vagy az adatfeldolgozónak kell nyilvántartást vezetni az adatkezelési műveletekről. Nincs azonban annak akadálya, hogy az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt megbízza az adatkezelő vagy az adatfeldolgozó felelősségébe tartozóan végzett adatkezelési műveletekről történő nyilvántartások vezetésével. 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.

Forrás: GDPR 39. cikke (1) bekezdésének c) pontja és 30. cikke

Kelt Brüsszelben, 2016. december 13-án

a munkacsoport részéről
Az Elnök

Isabelle FALQUE-PIERROTIN

Legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.

a munkacsoport részéről
Az Elnök

Isabelle FALQUE-PIERROTIN