WP243 MELLÉKLET - GYAKRAN ISMÉTELT KÉRDÉSEK

Jelen melléklet célja, hogy egyszerűsített és könnyen olvasható formában választ adjon néhány kulcsfontosságú kérdésre, amelyek a szervezetek részéről merülhetnek fel a GDPR-nek az adatvédelmi tisztviselő kijelölésére vonatkozó új előírásaival kapcsolatban.

Az adatvédelmi tisztviselő kijelölése (37. cikk)

1 Milyen szervezeteknek kell kijelölni adatvédelmi tisztviselőt? (37. cikk (1) bekezdése)

A GDPR előírja, hogy adatvédelmi tisztviselőt három esetben 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; valamint
- 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 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.

További információkért lásd az iránymutatás 2.1. pontját.

2 Mit jelent a „fő tevékenységek” fogalma? (37. cikk (1) bekezdésének b) és c) pontja

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. Annak ellenére, hogy ezek a tevékenységek szükségesek vagy nélkülözhetetlenek, általában nem fő tevékenységnek, hanem inkább járulékos funkcióknak tekinthetők.

További információkért lásd az iránymutatás 2.1.2. pontját.

3 Mit jelent a „nagy mértékű / nagy számban történő” kifejezés? (37. cikk (1) bekezdésének b) és c) pontja

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 megállapító ítéletekre és bűncselekményekre vonatkozó személyes adatok kezelése egy adott ügyvéd által

További információkért lásd az iránymutatás 2.1.3. pontját.

4 Mit jelent a „rendszeres és szisztematikus megfigyelés”? (37. cikk (1) bekezdésének b) pontja)

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.

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

Példák: távközlési hálózat működtetése; távközlési szolgáltatások nyújtása; célközönség e-mail alapú újbóli meghatározása; 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.

További információkért lásd az iránymutatás 2.1.4. pontját.

5 A szervezetek közösen is kijelölhetnek adatvédelmi tisztviselőt? Ha igen, milyen feltételekkel? (37. cikk (2) és (3) bekezdése)

A GDPR alapján 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 az elérhetőségét megadják a GDPR-nek megfelelően. Az adatvédelmi tisztviselőnek képesnek kell lenni 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 személyes 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.

További információkért lásd az iránymutatás 2.3. pontját.

6 Ki lehet jelölni külső adatvédelmi tisztviselőt (37. cikk (6) bekezdése)?

Igen. A 37. cikk (6) bekezdése alapján 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.

Külső adatvédelmi tisztviselő esetén a 37-39. cikk szerinti összes követelmény vonatkozik ezen adatvédelmi tisztviselőre. Amint az az iránymutatásban szerepel, 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 releváns követelményének.

A jogi egyértelműség és a jó szervezés 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.

További információkért lásd az iránymutatás 2.3, 2.4. és 2.5. pontját.

7 Milyen szakmai képességekkel kell rendelkeznie az adatvédelmi tisztviselőnek (37. cikk (5) bekezdése)?

A GDPR előírja, 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 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.

Szükséges 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

További információkért lásd az iránymutatás 2.4. pontját.

Az adatvédelmi tisztviselő jogállása (38. cikk)

8 Milyen forrásokat kell biztosítani az adatvédelmi tisztviselő részére a feladatai ellátásához?

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”*.

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.

További információkért lásd az iránymutatás 3.2. pontját.

9 Milyen biztosítékok teszik lehetővé az adatvédelmi tisztviselő feladatainak független ellátását (38. cikk (3) bekezdése)?

Számos biztosíték létezik annak érdekében, hogy az adatvédelmi tisztviselő független módon járhasson el, amint azt a (97) preambulumbekezdés megállapítja:

- 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 feladatok ellátása

További információkért lásd az iránymutatás 3.3.–3.5. pontját.

10 Melyek az adatvédelmi tisztviselő által végzett „más feladatok”, amelyekből nem fakadhat összeférhetetlenség (38. cikk (6) bekezdése)?

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 pozíciók lehetnek a felsővezetői pozíciók (például vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, marketing osztályvezető, humán erőforrás vezető vagy informatikai osztályvezetők), de más, struktúrában alacsonyabb szinten lévő pozíciók is, ha ezek a pozíciók az adatkezelés céljainak és eszközeinek meghatározásával járnak.

További információkért lásd az iránymutatás 3.5. pontját.

Az adatvédelmi tisztviselő feladatai (39. cikk)

11 Mit jelent a GDPR-nek való „megfelelés ellenőrzése” (39. cikk (1) bekezdésének b) pontja)?

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, és
- tájékoztatást, szakmai tanácsadást nyújt és ajánlásokat bocsát ki az adatkezelő vagy az adatfeldolgozó részére.

További információkért lásd az iránymutatás 4.1. pontját.

12 Az adatvédelmi tisztviselő személyesen felelős a GDPR be nem tartásáért?

Nem, 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 feldolgozás a GDPR rendelkezéseivel összhangban történik (24. cikk (1) bekezdése). Az adatvédelmi rendelkezések betartásáért az adatkezelő vagy az adatfeldolgozó felelős.

13 Melyek az adatvédelmi tisztviselő feladatai az adatvédelmi hatásvizsgálatok (37. cikk (1) bekezdésének c) pontja) és az adatkezelési tevékenységek nyilvántartása (30. cikk) 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 a GDPR-nek.

További információkért lásd az iránymutatás 4.2. pontját.

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 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.

További információkért lásd az iránymutatás 4.4. pontját.