

GDPR: kit nevezünk ki adatvédelmi tisztviselőnek?

2018. május 25-én hatályba lépett az Európai Unió új általános adatvédelmi rendelete (GDPR). Sok társaságnak sikerült a jogszabályi megfelelést eddig az időpontig megvalósítania, de nagyon sok cég, szervezet esetében a teljes megfelelés érdekében még komoly változtatásokat, fejlesztéseket kell végrehajtani. A felkészülési fázisban szerzett tapasztalatok okán a szakmai diskurzusban is kezdik átvenni az olyan kérdéskörök a hangsúlyt, amik a GDPR szerinti működés praktikus oldalát fogják meg. Ebbe a tendenciába illeszkedik a Nemzeti Adatvédelmi és Információszabadság Hatóságának (NAIH) nemrég közzétett adatvédelmi reformmal kapcsolatos állásfoglalása, ami azt vizsgálja, hogy a GDPR milyen kritériumokat határoz meg az adatvédelmi tisztviselők tekintetében.

A GDPR különleges hangsúlyt helyez az adatvédelmi tisztviselőkre (a magyarban is gyakran használta angol nyelvű kifejezéssel és rövidítéssel *Data Protection Officer, DPO*) szerepére. Ezek a személyek hivatottak arra egyrészt, hogy az egyes szervezetek adatvédelmi megfelelését a szervezeten belülről biztosítsák. Ennek megfelelően e tisztviselő az őt alkalmazó szervezeten belül tanácsokat ad és ellenőriz, ezzel biztosítva azt, hogy mind egyéni, mind szervezeti egység, mind pedig az egész szervezet szintjén a GDPR rendelkezéseinek megfelelően folyjon az adatkezelés és adatfeldolgozás. Másrészről azonban túlmutat a szerepe annak a szervezetnek a keretein, amelyben az előbbi feladatokat ellátja, mivel sok szempontból egyfajta kapcsolatot is jelent a NAIH-al, illetve más tagállamok adatvédelmi hatóságaival. Így együttműködési kötelezettség terheli e hatóság irányába és „kapcsolattartási pont”-ként is funkcionál (majd) a NAIH és az adatkezelő között.

Természetesen nem kötelező mindenkinek, aki adatkezelőnek minősül egy dedikált személy (vagy szervezetet) alkalmazni a GDPR betartására. E kötelezettség bizonyos szempontból kiemelt jelentőségű adatkezelőket terhel. Ezt az adatkezelő sajátossága (így közhatalmat gyakorló szervezetek esetében), a kezelt adatok sajátossága (ilyen lehet bűncselekményekre vonatkozó adatok nagy számban történő kezelése) vagy az adatkezelő (fő)tevékenysége (ami sajátosságai folytán rendszeres és szisztematikus, nagymértékű megfigyelését tesz szükségessé) is megalapozhatja.

Közeledve ahhoz az időponthoz, amikortól e kötelezettség a GDPR hatálya alatt terhel majd egyes adatkezelőket, gyakran felmerült annak a kérdése, hogy mik azok a sarokpontok, amiket mindenképpen figyelembe kell venni az adatvédelmi tisztviselőnk kiválasztásánál. A NAIH ebben a kérdéskörben adott ki állásfoglalást a WP 29-nek (Article 29 Working Party – 29 Cikkely Munkacsoport, az Európai Bizottságnak az adatvédelmi tanácsadó testülete) e tárgyban készített iránymutatására alapozva.

Gyakran felmerült kérdés ezzel kapcsolatban, hogy milyen végzettséggel kell rendelkeznie annak a személynek, aki az adatvédelmi tisztviselői feladatokat fogja ellátni. Ezzel kapcsolatban gyakori volt az a nézet, ami szerint kizárólag jogi diplomával rendelkező személyek tölthetik be ezt a tisztséget, ami abból a szempontból nem feltétlenül tűnhet elvetendőnek, hogy egy jogszabály betartásának mikéntje köré szerveződik az érintett feladatkör, azonban ez a hozzáállás figyelmen kívül hagyja a helyzet számos sajátosságát. Ennek megfelelően a NAIH fentebb is említett állásfoglalása arra konklúzióra jut, hogy nincs meghatározott – felsőfokú vagy egyéb – végzettség, ami általánosan megkövetelhető lenne. Megfelelően a GDPR általános gyakorlatorientált szemléletének, itt sem egy szigorú és általános (és egyértelmű) szabály alkalmazandó, hanem az egyén sajátosságai mérlegelendőek az adatkezelő és az adatkezelés milyensége tükrében. Így egy szempontként értékelendő az adatvédelmi szabályozás kimerítő ismerete, azonban az már nincs megkötve, hogy ezt a tudást miként szerezze meg az illető. Ehelyett át kell látnia és meg kell értenie az adatkezelési műveletek összességét, szüksége van az adott szervezet és üzletág ismeretére, a képességre, hogy a szervezeti gyakorlatot pozitív irányba mozdítsa elő és rendelkeznie kell a megfelelő IT és adatbiztonsági ismeretekkel. Amint ebből is kitűnik, az

adatvédelmi tisztviselővel szemben alkalmazandó mérce nem abszolút, minden esetben ahhoz szükséges mérni a képességeit és a képesítését, hogy milyen konkrét feladatokat fog ellátni és milyen kihívásokkal szembesülhet.

Lehetőség van az adatvédelmi tisztviselői pozíciónak egy szervezet (legvalószínűbb esetekben gazdasági társaság vagy ügyvédi iroda) általi betöltésére is. Ilyen esetekben a fentebb említett állásfoglalás alapján azonban elengedhetetlen, hogy a szervezet valamennyi tagja megfeleljen a GDPR adatvédelmi tisztviselőkre vonatkozó követelményeinek. Itt mind a WP-29 iránymutatása, mind pedig a NAIH állásfoglalása az összeférhetetlenség elkerülését emeli ki példaként. Ilyen esetben erősen ajánlott egy nevesített kapcsolattartót és felelőst kinevezni a feladatellátó szervezetnél. Olyan adatkezelők esetében, amik folyamatos jelenlétet és közreműködést igényelnek az adatvédelmi tisztviselő részéről, ideális megoldás lehet az, hogy egy szervezetet bíznak meg e feladatokkal annak érdekében, hogy egy személy ideiglenes kiesése miatt ne álljon meg az élet.

Az adatvédelmi tisztviselőkről a fentiek szerint vázolt képből kitűnik, hogy minden szervezetnek lehetősége van a maga gyakorlatának és működésének megfelelő személy kiválasztására mindaddig, amíg e személy rendelkezik mindazon ismeretekkel és kvalitásokkal, amik a konkrét adatkezelő tekintetében képessé teszik e tisztség betöltésére.