

SZABÓ ENDRE

AZ ADATVÉDELMI TISZTVISELŐRŐL

A GDPR szabályainak elemzése

Bevezetés

Az Európai Unió általános adatvédelmi rendeletének¹ 2018. május 25-től alkalmazandó szabályai szerint az adatvédelmi tisztviselő kinevezése számos adatkezelő esetében kötelezővé válik. A kinevezés szabályairól a források általában egy-egy kérdés vagy ágazati szempont kiemelése révén adnak tájékoztatást, ezért szükségesnek látszik egy összefoglaló jellegű írás megjelentetése.

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

Elemzésünkben alapvetően a GDPR normaszövegére, a vonatkozó preambulumbekendésekre, mint értelmező rendelkezésekre támaszkodunk, továbbá az egyes értelmezési kérdésekben bemutatjuk az Európai Unió adatvédelmi hatóságait tömörítve, a 29. cikk szerint működő Adatvédelmi Munkacsoport iránymutatását az adatvédelmi tisztviselőkről.²

Kockázatok és elszámoltathatóság

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

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

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

Az elszámoltathatóság hangsúlyozásával az adatkezelő és adatfeldolgozó oldalán érvényesülő felelősség még világosabban kirajzolódik. Valamennyi szereplő helyzete változik valamilyen módon: az adatkezelők felelősségének kiemelése mellett a megfelelés eszközeinek tárháza is bővül: a jogalkotó új alapelveket fogalmazott meg (privacy by design³ és privacy by default⁴), az adatvédelmi tisztviselő olyan belső ellenőrzési

mechanizmus letéteményese, amelyre eddig nem volt példa. Ha egy mondatban szeretnénk összefoglalni a tisztviselő szerepét, akkor a rendeletet idézve azt mondhatjuk, hogy az adatvédelmi tisztviselő megkönnyíti a GDPR rendelkezéseinek való megfelelést. Mindezt a kockázatokra tekintettel, az elszámoltathatóság jegyében teszi.

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

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

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

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

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

Adatvédelmi tisztviselők⁵

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

A 29-es Munkacsoportnak az adatvédelmi tisztviselőkről készült iránymutatását azzal kezdi, hogy ők az új jogi keret „szívében” lesznek sok adatkezelő szervezetnél, elősegítve a rendeletnek való megfelelést. A Munkacsoport továbbmegy, és azt állítja, hogy az elszámoltathatóság egyik alapköve a tisztviselői intéz-

Az adatkezelő a jogi megfelelés terén a tisztviselő igénybevételén túl más eszközökre is támaszkodhat: magartartási kódexek kidolgozása révén közös, például ágazati erőfeszítések részese lehet és meríthet a közös tudásból, amely az adott területen való megfelelést elősegítheti.

A szerző KRE ÁJK doktorandusz hallgató, a NAIH elnökhelyettese.

mény, és foglalkoztatásuk versenylőnyt jelenthet az üzleti szereplők számára.

A rendelet (77) preambulumbekzdése szerint „a megfelelő intézkedéseknek az adatkezelő általi végrehajtásához, valamint a megfelelés általuk való bizonyításához – különösen ami a kockázat beazonosítását, valamint a kockázat súlyosságának a fel-

a tisztviselők maguk személyesen nem felelősek a jogszabályoknak való megfelelésért, az adatkezelőre vagy az adatfeldolgozóra hárul a felelősség az esetleges jogsértésekért.

mérését illeti –, továbbá a kockázat mérséklésével kapcsolatos útmutatással szolgálhatnak különösen a jóváhagyott magatartási kódexek, a jóváhagyott tanúsítási eljárások, a Tesztület iránymutatásai vagy az adatvédelmi tisztviselő által nyújtott iránymutatások”.⁶

Hozzáteszi az anyag, hogy a tisztviselők maguk személyesen nem felelősek a jogszabályoknak való megfelelésért, az adatkezelőre vagy az adat-

feldolgozóra hárul a felelősség az esetleges jogsértésekért. E szabálynak, amint látni fogjuk, munkajogi vonatkozásai is vannak.

A nemzetközi példák azt mutatják, hogy vannak országok, ahol a belső adatvédelmi felelősök intézménye még nem honosított meg, ezért a GDPR-ra való felkészülés a tisztviselők képzésének jegyében is telik.⁷

Az adatvédelmi tisztviselő kinevezésének kötelezettsége

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

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

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

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

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

A 680/2016-os számú bűnügyi irányelv, amely az adatvédelmi csomag⁸ része, szintén kötelezővé teszi az adatvédelmi tisztviselő kinevezését. Itt tehát a tevékenység jellege az a körülmény, amely a kinevezést indokolja. A kötelezés általános, a tagállam azonban felmentheti a kinevezés kötelezettsége alól az eljáró bíróságokat és egyéb független igazságügyi hatóságokat.

Kinevezési kötelezettséget eredményező adatkezelés az adatok típusára tekintettel:

Végül a rendelet felsorolja azokat az adatokat, amelyeknek a kezelése, ha a fő tevékenységi körhöz tartozik, és nagy számban kezelnek ilyen adatokat, akkor a tisztviselő kinevezése kötelező: a különleges adatok⁹ tartoznak ide, ahol a rendelet külön kategóriaként határozza meg a büntetőjogi felelősséggel kapcsolatos adatokat.¹⁰

Figyelmet érdemel a jelenlegi magyar szabályozás és a rendelet szövegének az összehasonlítása, ugyanis a rendelet alkalmazásától olyan adatok is a különleges adatok körébe tartoznak majd, amelyek most még nem: ilyen a biometrikus adatok és a genetikai adatok köre.¹¹

Értelmezési kérdések – fő tevékenység, nagymértékű adatkezelés

Fő tevékenység

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

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

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

Nagymértékű adatkezelés

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

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

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

Mindezek alapján a nagymértékű adatkezelés körébe tartozó adatkezelésnek tekintendő:

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

Rendszeres és szisztematikus megfigyelés

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

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

A rendszeres kitételhez a munkacsoporti iránymutatás az alábbi támpontokat nyújtja:

- Folyamatos vagy rendszeres időközönként történik;
- Meghatározott időnként ismétlődik;

A szisztematikus kitétel tartalma a Munkacsoport szerint az alábbi:

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

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

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

Az adatkezelőnek vagy az adatfeldolgozónak kell kineveznie az adatvédelmi tisztviselőt?

A feltett kérdésre nincs általános válasz, de az eddigi tapasztalataink alapján az adatkezelőknél mintha természetesebben adódna a kinevezési kötelezettség, mint az adatfeldolgozónál.¹² Az, hogy az adatkezelőnél ki kell nevezni tisztviselőt, nem jár automatikusan kinevezési kötelezettséggel az adatfeldolgozó oldalán.

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

A kinevezés mérlegelése, a mérlegelés dokumentálása

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

Adatvédelmi tisztviselő önkéntes kinevezése

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

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

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

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

Az adatvédelmi tisztviselő jogállása

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

A kijelölés kritériumai: minek alapján ítéhető meg a tisztviselőtől elvárt tudás és szakértelem?

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

A felkészültség kapcsán hivatkozhatunk az Európai Adatvédelmi Biztos 2010-ben kibocsátott elemzésére¹³, amelyben az uniós intézmények által kinevezett adatvédelmi tisztviselőkkel kapcsolatos szabályokról ad tájékoztatást.¹⁴ Ez a dokumentum öt konkrét képzettséget említi, nevezetesen a CIPP¹⁵, a CIPP

A rendelet más megközelítést alkalmaz a korábbi magyar szabályozáshoz képest, szakmai rátermettségről és feladatai ellátására való alkalmasságról beszél.

/ IT¹⁶, továbbá a CISSP¹⁷, a CISA¹⁸ és a CISM¹⁹ képzéseket. A 2010-es dokumentum kibocsátását követően nyílt meg a CIPP / E képzés²⁰, amely kifejezetten az európai adatvédelmi jogra fókuszál a bemutatott képzéscsaládon belül. Az Európai Adatvédelmi Biztos álláspontja szerint ezek megléte fontos szempont az uniós intézménynél dolgozó tisztviselő kiválasztása során.

Az Európai Adatvédelmi Biztos anyaga kapcsán megemlítenőd, hogy az nem az általános adatvédelmi rendelet értelmezése

A megszerezhető képzettségek és képesítések országonként változók lehetnek.

céljából készült, továbbá csupán egy szervezett képzéseit említi. A megszerezhető képzettségek és képesítések országonként változók lehetnek. Magyarországon jelenleg egy egyetemi képzés keretében képeznek adatvédelmi szakértőket, illetve adatvédelmi szakembereket.

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

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

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

További lehetséges kritériumként említhető az együttműködés képessége és a megbízhatóság. Egy szakértői értelmezés szerint a megbízhatóság az összeférhetetlenséggel is szoros összefüggést mutat, és az összeférhetetlenséget – az adott tisztviselő hozzáállásától vagy személyes kvalitásaitól függetlenül – vélelmezni kell a következő személyek esetében: a tulajdonos, a vezető testület tagja, egyéb magas rangú vezető, a betöltött munkakör okán össze nem egyeztethető feladatok ellátói (informatikai vagy humán erőforrás vezető, a napi adatkezelési feladatok irányító munkatársak), továbbá a felsorolt személyek közeli hozzátartozói.²¹

A foglalkoztatás szabályai

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

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

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

A tisztviselő adatainak nyilvánossága, elérhetőség

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

A külvilág felé történő nyilvánosságra hozatal mellett meg kell említeni a belső nyilvánosságot, amely azt szolgálja, hogy

a szervezet munkavállalói személyesen el tudják érni a tisztviselőt. Azt ajánlja ezért a Munkacsoport, hogy a belső névjegyzékekben, telefonkönyvekben a tisztviselő neve és elérhetősége szerepeljen. Az is alapvető elvárás, hogy a szervezet munkavállalói bizalommal kereshessék a tisztviselőt, ezért írja elő a rendelet a tisztviselő számára a titoktartási kötelezettséget, illetve az adatok bizalmas kezelésére vonatkozó kötelezettséget.

A panaszon túl a rendelet az érintettek számára kötelezően elérhetővé rendeli a tisztviselőt akkor, amikor a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódóan bármilyen kérdést megfogalmaznak. Ez nem jelenti azt, hogy a tisztviselő a kizárólagos kapcsolattartó adatvédelmi ügyekben, de neki kötelessége az adatainak rendelkezésére állni, különösen például adatbiztonsági incidensek esetében. Ez lehet e-mail, valamiféle forró vonal, meg lehet könnyíteni a kapcsolatba lépést továbbá egy webes formula kialakításával.

Teljes-, vagy részmunkaidős foglalkoztatás

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

Egy gyakran elfeledett szabály kívánczik még a tisztviselő jogállásához: a felügyeleti hatóság feladatai kapcsán a rendelet is és az irányelv is előírja, hogy azok ellátása az érintett és az adatvédelmi tisztviselő számára térítésmentes legyen.²²

Az adatkezelő feladatai a tisztviselő munkájának támogatása terén

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

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

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

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

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

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

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

Összeférhetetlenség

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

A bajor adatvédelmi biztos 2016 októberében nyilvánosságra hozott közleményében²³ mutatott be egy olyan ügyet, amelyben az adatkezelő szervezet a tisztviselőre vonatkozó összeférhetetlenségi szabályokat szegte meg. A vonatkozó szabályok szerint azon szervezetek, amelyek a személyes adatok automatikus feldolgozása területén legalább tíz főt foglalkoztatnak, kötelesek adatvédelmi tisztviselőt kinevezni. A bajor hatósági álláspont kiemelte, hogy ha valakit erre a pozícióra kineveztek, akkor nem kaphat olyan feladatokat, amelyek a tisztviselői funkcióval konfliktust eredményezhetnek. Ilyen konfliktus és összeférhetetlenség áll fenn, ha a tisztviselő egyúttal IT vezető is a szervezetenél. Ebben az esetben ugyanis a tisztviselő nem tudja az adatvédelmi ellenőrző szerepét függetlenül ellátni, hiszen ilyenkor a

Ha több feladatot is ellát a tisztviselő, akkor az adatkezelőnek kell biztosítani azt, hogy ezekből a feladatokból ne fakadjon összeférhetetlenség.

saját munkáját kellene ellenőriznie. A tisztviselői feladattal összeegyeztethetetlen az adatkezelést érintő döntések meghozatala, illetve az ezekért viselt felelősség. Mindennek megfelelően azon szervezetek, amelyek adatvédelmi tisztviselő kinevezésére kötelesek, csak olyan személyt nevezhetnek ki, aki ezt a feladatát minden külső befolyás nélkül tudja ellátni. Azok a szervezetek pedig, amelyek ismételt felhívás ellenére sem tesznek eleget e kötelezettségüknek, szükségszerűen pénzbüntetéssel kell, hogy számoljanak a bajor hatóság közleménye szerint.

A jogeset kapcsán adódik a kérdés, vajon hasonló ügyekre és bírságokra lehet-e számítani a rendelet alkalmazása idején is? Bár a leírt eset a német (bajor) jog alapján ítéendő meg, a rendelet is a szankcionálandó mulasztások között említi az adatvédelmi tisztviselőre vonatkozó kötelezettségeket.²⁴ Ennek megfelelően az adatvédelmi felügyeleti hatóságok a jövőben hasonló ügyeket a bajor példához hasonlóan ítéelhetnek majd meg.

Az adatvédelmi tisztviselő feladatai – tanácsadás, ellenőrzés, kapcsolattartás

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

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

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

Nevesített feladata a hatósággal való együttműködés, az előzetes adatvédelmi hatásvizsgálat kapcsán ő a kapcsolattartó a hatóság felé, és bármilyen adódó ügyben konzultációt folytathat a hatósággal.

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

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

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

A tisztviselő feladatai az adatvédelmi hatásvizsgálat kapcsán

A tisztviselő az adatkezelő kérésére szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, illetve nyomon kö-

veti annak elvégzését. Ha van kinevezett tisztviselő, őt az adatkezelő köteles bevonni. Ha az adatkezelő szervezet nem tisztviselőt, hanem adatvédelmi tanácsadót foglalkoztat (mert nem terheli a tisztviselő kinevezésének kötelezettsége), akkor az ő bevonása nem kötelező.

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

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

Kötelező erejű vállalati szabályok és tisztviselők konferenciája

A kötelező erejű vállalati szabályok kapcsán a rendelet kötelező tartalmi elemként említi a kijelölt adatvédelmi tisztviselő feladatait.²⁵

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

A rendelet 30. cikke szerinti nyilvántartás az adatkezelési tevékenységekről²⁶

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

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

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

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

Ezeket túl azokat az információkat tartalmazza, amelyek az áttekinthetőség érdekében észszerűen adódnak, így az adatkezelés célját, az érintettek kategóriáit és a kezelt személyes ada-

tok kategóriáit, a címzettek kategóriáit, a törlés határidejét, az adatbiztonsági intézkedések általános leírását. Mindezeket túl a harmadik országba irányuló adattovábbítás esetén a címzettek és az adatok védelmét szolgáló garanciákat is be kell mutatni.

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

A nyilvántartás vezetése alóli mentesség és a kockázatalapú megközelítés

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

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

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

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

A személyes adatok különleges kategóriáinak kezelése esetében minden adatkezelő köteles a nyilvántartást vezetni, sem a

kkv minőség, sem az alkalmi jelleg nem nyújt felmentést e kötelezettség alól.

A 29-es Munkacsoport a GDPR alkalmazandóvá válását megelőzően már úgy foglalt állást, hogy a 250 főnél kevesebb személyt foglalkoztató adatkezelő csak az adatkezelési típusokról köteles nyilvántartást vezetni a 30. cikk (5) bekezdése alapján.²⁷ Ez jelentős adminisztratív könnyítést jelent a szektor számára.

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

Összegzés

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

Kívánatos, hogy Magyarországon is erősödjön az adatvédelmi tisztviselők közötti együttműködés, a hasznos információk megosztásának fórumai tovább épüljenek.

Függelék

Az adatvédelmi tisztviselő említési helyei a GDPR-ban:

- (77), (97) preambulumbekkezdés
- 13. cikk (1) bek. b) pont
- 14. cikk (1) bek. b) pont
- 30. cikk (1) bek. a) pont
- 30. cikk (2) bek. a) pont
- 33. cikk (3) bek. b) pont
- 35. cikk (2) bek.
- 36. cikk (3) bek. d) pont
- 37–39. cikk
- 47. cikk (2) bek. h) pont
- 57. cikk (3) bek.

Az adatvédelmi tisztviselő említési helyei a bünyügyi irányelvben:

- (63) preambulumbekkezdés
- 13. cikk (1) bek. b) pont
- 24. cikk (1) bek. a) pont
- 24. cikk (2) bek. a) pont
- 30. cikk (3) bek. b) pont
- 32–34. cikkek
- 46. cikk bek. (3) pont

Jegyzetek

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).

2 A 29. cikk szerinti Adatvédelmi Munkacsoport, Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban, WP 243 rev.01, az elfogadás időpontja: 2017. április 5.

3 A rendelet 25. cikk (1) bekezdése határozza meg a beépített adatvédelem elvének tartalmát.

4 A rendelet 25. cikk (2) bekezdése határozza meg az alapértelmezett adatvédelem elvének tartalmát.

5 Kapcsolódó joganyag: a rendelet 37–39. cikke, továbbá a (97) preambulumbekkezdés.

6 A 29-es Munkacsoport tisztviselőkről készített vélemények melléklete kérdések és válaszok formájában foglalja össze a legfontosabb tudnivalókat az adatvédelmi tisztviselőkről. Ez nem csak a tisztviselőknek lehet hasznos, hanem a szervezeten belüli egyeztetések során is szerepet játszhat, hiszen viszonylag rövid terjedelemben mutatja be

a tisztviselővel kapcsolatos legfontosabb tudnivalókat és elvárásokat

7 Az IAPP (International Association of Privacy Professionals) 2016. július 19-én nyilvánosságra hozott elemzése (GDPR conundrums: The data protection officer requirement) csupán négy európai uniós országot emel ki, ahol kötelező ki nevezés érvényesül: Németország, Horvátország, Magyarország és Spanyolország. Még ha az elemzés némiképp vázlatos is, jól mutatja, hogy a tisztviselői pozíció korántsem vált a mindennapi gyakorlat részévé valamennyi tagállamban.

8 Az Európai Parlament és a Tanács (EU) 680/2016 számú irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről.

9 A rendelet 9. cikkében meghatározott adatkör.

10 A rendelet 10. cikke a „természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok” kezelését is a személyes adatok különleges kategóriájaként határozza meg.

11 A rendelet 10. cikke a „természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok” kezelését is a személyes adatok különleges kategóriájaként határozza meg.

12 A rendelet 4. cikk 8. pontja szerint az adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

13 Az Európai Adatvédelmi Biztos által 2010. október 14-én nyilvánosságra hozott anyaga: „Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001.

14 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról három, illetve hét éves szakmai tapasztalatot vár el a kinevezett tisztviselőktől.

15 Certified Information Privacy Professional.

16 Certified Information Privacy Professional / Information Technology.

17 Certified Information Systems Security Professional.

18 Certified Information System Auditor.

19 Certified Information Security Manager.

20 Certified Information Privacy Professional / Europe.

21 Holger Lutz, a Baker & McKenzie partnerének véleménye, Germany: BayLDA's DPO fine „not surprising”, dataguidance.com, 2016. október 27.

22 A rendelet 57. cikk (3) bekezdése, illetve az irányelv 46. cikk (3) bekezdése szerint.

23 Pressemitteilung: Datenschutzbeauftragter darf keinen Interessenkonflikten unterliegen, Ansbach, den 20. 10. 2016.

24 A GDPR 83. cikk (4) bekezdésének a) pontja szerint az adatvédelmi tisztviselőre vonatkozó kötelezettségek megsértése esetén az adatkezelő, illetve az adatfeldolgozó legfeljebb 10 millió Euró összegű közigazgatási bírsággal, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világműködésének legfeljebb 2%-át kitevő összeggel sújtható (a kettő közül a magasabb összeget kell kiszabni).

25 A rendelet 47. cikk (2) bekezdésének h) pontja határozza meg ezt a tartalmi elemet.

26 Hasonló kötelezettséget ír elő a bünyügyi irányelv 24. cikke.

27 A 29-es cikk szerinti Munkacsoport állásfoglalása a GDPR 30. cikk (5) bekezdésében foglalt adatkezelési tevékenységekre vonatkozó nyilvántartási kötelezettségtől való eltérésekről.

GDPR – ÁLTALÁNOS ADATVÉDELMI RENDELET ÉS A KAPCSOLÓDÓ JAVASLATOK

A népszerű jogszabálygyűjtemény-sorozatot a jövőben a Novissima Kiadó és a HVG-ORAC Kiadó közösen jelentetik meg. A GDPR-t, valamint a kapcsolódó jogi környezetet tartalmazza a sorozatnak ez a kötete:

• 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 rendelet hatályon kívül helyezéséről (Általános Adatvédelmi Rendelet, GDPR)

• Az Európai Parlament és a Tanács rendelete (javaslat)

Az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet)

• 2011. évi CXII. törvény

Az információs önrendelkezési jogról és az információszabadságról (Infotv.)

• Előterjesztés

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXXII. törvény (Infotv.) jogharmonizációs célú módosításáról

A gyűjteményt 2018. március 26-án zártuk le. Az Elektronikus hírközlési adatvédelmi rendeletből és az Infotv. módosításáról szóló törvényből ekkor még elfogadott, kihirdetett szöveg nem állt rendelkezésünkre, így az ekkor ismert javaslatokat használtuk a 2018. május 25-én hatályos állapot megállapításához. A jogszabályok végleges szövege ettől eltérhet. Az Infotv. az előterjesztés által bevezetendő módosításokat is tartalmazza.



Ára: 2590 Ft

WEBES VÁSÁRLÁS
-5%