Ügyszám: NAIH/2018/2068/2/K

[…] részére
[…]

Tisztelt […]!

A Nemzeti Adatvédelmi és Információszabadság Hatóságnak elektronikus úton küldött levelében a GDPR alkalmazására való felkészülés érdekében számos kérdéssel kapcsolatban kér állásfoglalást, elsősorban a kis- és középvállalkozásokat érintő változásokat illetően, amelyekkel összefüggésben az alábbiakat hozom szíves tudomására.

1./ Azt, hogy az új szabályok kikre vonatkoznak, a GDPR hatálya határozza meg, amelyről az 1-3. cikkek rendelkeznek. E rendelkezések alapján látható, hogy a személyi hatály tekintetében annak semmi jelentősége nincs, hogy valaki magánszemélyként, kis- vagy középvállalkozásként, vagy egyéb vállalkozási formában folytat-e adatkezelői (vagy adatfeldolgozói) tevékenységet. Ha a kis- vagy középvállalkozás adatkezelési (adatfeldolgozói) tevékenysége a rendelet hatálya alá tartozik, akkor rá is alkalmazni kell a GDPR-t. Kérdésére válaszolva röviden: a pék, a kisbolt, az egyszemélyes gazdasági társaság, az egyéni vállalkozó és a webáruházak adatkezelésének is meg kell felelnie a GDPR szabályainak.

A GDPR hatálya alá tartoznak, illetve a GDPR szabályainak meg kell felelnie az automatizált (azaz elektronikus úton, egyszerűn: számítógéppel végzett) adatkezelések mellett a kézi (manuális) adatkezeléseknek is. Nem tartoznak a rendelet hatálya alá az olyan adatkezelések, amelyeket természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végeznek, azaz amely semmilyen szakmai vagy üzleti tevékenységgel nem hozhatók összefüggésbe [ld. GDPR (15) preambulumbekezdése]. A teljesség érdekében meg kell említeni, hogy eltérő nemzeti szabályok vonatkoznak a nemzetbiztonsági, a honvédelmi, és a bűnügyi célú adatkezelésekre.

Ki kell emelni, hogy a GDPR hatálya alá csak a természetes személyek adataira vonatkozó adatkezelések tartoznak, így az nem vonatkozik jogi személyek és egyéb vállalkozások adatainak kezelésére. A személyes adat fogalmát a rendelet 4. cikk 1. pontja így határozza meg: „azonosított vagy azonosítható természetes személyre vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható".

2./ A GDPR (13) preambulum-bekezdése a kis- és középvállalkozások tekintetében előírja, hogy a rendelet alkalmazása során az uniós intézményeket és szerveket, és a tagállamokat és azok felügyeleti hatóságait ösztönözni kell, hogy vegyék figyelembe a mikro-, kis- és középvállalkozások sajátos szükségleteit. E kötelezettséget teszi hangsúlyosabbá, hogy a magatartási kódex és a tanúsítási eljárások kidolgozásával kapcsolatban a szabályozás szintén kiemeli a mikro-, kis- és középvállalkozások sajátos igényeit [40. cikk (1) bekezdése és 42. cikk (1) bekezdése].

A 30. cikk (5) bekezdése továbbá a 250 főnél kevesebb személyt foglalkoztató szervezetek esetében a nyilvántartás vezetése tekintetében valóban eltérést tartalmaz. E rendelkezés szerint ezeknek az adatkezelőknek (adatfeldolgozóknak) akkor kell nyilvántartást vezetniük az adatkezelési tevékenységeikről, ha a végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

A 9. és 10. cikkek szerinti adatokat érintő adatkezelési tevékenység jól beazonosítható. A másik két esetkör (a „valószínűsíthetően magas kockázat" és az „alkalmi jelleg") meghatározása azonban feltehetőleg már értelmezési kérdéseket vethet fel, és ezzel kapcsolatban szeretném kiemelni, hogy a GDPR alkalmazásához kapcsolódóan gyakorlati tapasztalatok még nem állnak rendelkezésre.

a) A „valószínűsíthetően magas kockázat" megítéléséhez a GDPR-ban a (75) és (91) preambulum-bekezdések nyújtanak eligazítást. Az Adatvédelmi Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport elfogadott továbbá egy iránymutatást (248. számú iránymutatás) az adatvédelmi hatásvizsgálatról, amely részletesen foglalkozik az adatkezelés „valószínűsíthetően magas kockázatának" értékelésével összefüggő kérdésekkel is. Ez az iránymutatás megtalálható magyar nyelven is a Hatóság honlapján a http://www.naih.hu/29-es-munkacsoport-iranymutatasai.html linkről. A jogalkalmazás során tehát elsősorban e szabályok tekinthetők kiindulópontnak. Az Európai Unióban egyébként számos módszer, szoftver elérhető a kockázatértékelés elvégzéséhez (ilyen például az az adatvédelmi hatásvizsgálathoz készített szoftver, amelyet a francia adatvédelmi hatóság, a CNIL hivatalosan is elfogad; az ezzel kapcsolatos információk a CNIL honlapjáról elérhetők). Az azonban, hogy ezek közül alkalmazza-e bármelyiket és melyiket alkalmazza az adatkezelő, már a saját felelősségi körébe esik. Az adatkezelők segítése érdekében a közeljövőben várhatóan magunk is közzétesszük a Hatóság honlapján az ehhez szükséges információkat, így azt érdemes lesz figyelemmel kísérni.

b) Az adatkezelés „alkalmi jellegének" megítélésére a rendelet nem tartalmaz további eligazítást. Elképzelhető, hogy az egységes jogalkalmazás biztosítása érdekében a jövőben a 29-es Adatvédelmi Munkacsoportból felálló Európai Adatvédelmi Testület is foglalkozik majd a kérdéssel, iránymutatást vagy ajánlást bocsát ki, addig azonban a nyelvtani értelmezést lehet alapul venni. Továbbá figyelembe lehet venni azt is, hogy a GDPR 5. cikk (2) bekezdésében írt „elszámoltathatóság elve" alapján az adatkezelőnek képesnek kell lennie a megfelelés igazolására, amelyhez a nyilvántartás adatai megfelelő alapul szolgálnak. Mindezek alapján a Hatóság álláspontja szerint e mentesített körbe valóban csak az egyedi, egyszeri, kivételes adatkezeléseket folytató kis- és középvállalkozások tartozhatnak, más esetben nem lehet eltekinteni a nyilvántartás vezetésétől.

3./ A megkeresésében azzal kapcsolatban is érdeklődik, hogy milyen konkrét intézkedéseket kell tenni a jogszabályi megfelelés érdekében. Ennek meghatározása igen sokrétű feladat, azt csak a végzett adatkezelési tevékenységek valamennyi részletének birtokában lehetne eldönteni, amelyre a Hatóságnak nincs módja, és ilyen tevékenység folytatására hatáskörrel sem rendelkezik. Az az előzőekből is látható, hogy a GDPR a jelenleginél hangsúlyosabban kívánja meg az adatkezelés jogszerűségének bizonyítását, így erre feltehetőleg kiemelt gondot kell fordítani. De említeni lehet még az érintettek részére nyújtott tájékoztatások

nyújtásának felülvizsgálatát, az adathordozhatósághoz való jog biztosítását, az adatvédelmi hatásvizsgálat elvégzését vagy az adatkezelés biztonságát veszélyeztető helyzetek (incidensek) Hatóságnak történő bejelentését stb. A GDPR 24. cikke az adatkezelő feladatává teszi azt, hogy – 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 hajtson végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a rendelettel összhangban történjen. Annak megítélésére azonban, hogy konkrét esetben milyen technikai és szervezési intézkedések lehetnek szükségesek, elsősorban az adatkezelő képes, miután – ahogy fentebb is említettem – a szükséges információk nála állnak rendelkezésre. Ezen intézkedések tekintetében a (78) preambulumbekezdés példálózó felsorolást nyújt (belső szabályzat, álnevesítés, adatkezelések szükségességének időszakos felülvizsgálata stb.)

4./ A beadványában érinti az adatkezelői nyilvántartás kérdését, amelyet a Hatóság az adatkezelők bejelentései alapján a hatályos szabályozás szerint vezet az érintettek tájékozódásának elősegítése érdekében. Ebben a nyilvántartásban fel kell tüntetni az adatkezelésre vonatkozó minden lényeges körülményt, így például az adatkezelés célját, jogalapját, időtartamát.

Tájékoztatom, hogy az adatkezelők ezen bejelentési kötelezettsége a Hatóság felé május 25. napjától megszűnik, a GDPR ugyanis nem tartalmaz a tagállami felügyeleti hatóságok által vezetendő országos adatvédelmi nyilvántartásra vonatkozó szabályozást.

5./ Azt, hogy kinek kell adatvédelmi tisztviselőt alkalmazni, a rendelet 37. cikke határozza meg. Ez alapján az adatkezelőnek (adatfeldolgozónak) adatvédelmi tisztviselőt kell kijelölnie minden olyan esetben, amikor:
a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;
b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;
c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Az itt írt esetkörök és az adatvédelmi tisztviselő jogállását, feladatait érintő kérdések értelmezéséhez a 29-es Adatvédelmi Munkacsoport 243. számú iránymutatása áll rendelkezésre, amely szintén elérhető a Hatóság honlapjáról.

6./ A levelében azzal kapcsolatban is érdeklődik, hogy ki ellenőrzi majd a GDPR betartását, mit ellenőriznek, és hogy van-e reális esély a 20 millió eurós büntetésre.

A GDPR alkalmazásának ellenőrzése Magyarországon a Hatóságunk feladata. A GDPR egyébként e tekintetben előírja, hogy minden tagállamban egy (vagy több) független közhatalmi szerv kerüljön kijelölésre, amelyek több tagállami érintettség esetén a

rendeletben szabályozott módon együttműködnek egymással. A 29-es Adatvédelmi Munkacsoportból továbbá május 25. napjától feláll az Európai Adatvédelmi Testület, amelyik bizonyos esetekben részt vesz a felügyeleti hatóságok együttműködési eljárásaiban, és az ő feladata lesz a rendelet egységes alkalmazásának biztosítása, amelynek érdekében iránymutatást, ajánlást és legjobb gyakorlatokat is kibocsáthat.

A NAIH eljárása indulhat kérelemre és hivatalból is, az ellenőrzés menetére már a nemzeti jog szabályai irányadók, a GDPR csak kevés alkalmazandó szabályt tartalmaz. Az eljárások kialakítása okán egyébként az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) módosítása is szükségessé vált, az erről szóló tervezet várhatóan hamarosan benyújtásra kerül az Országgyűléshez.

A GDPR megsértése esetén alkalmazandó szankciókat maga a GDPR határozza meg. A 83. cikk (2) bekezdése alapján a Hatóság alkalmazhat meghatározott intézkedéseket (pl. figyelmeztetés vagy utasítás a rendeletnek megfelelő adatkezelés kialakítására), és ezek mellett vagy helyett közigazgatási bírságot kell kiszabnia. A rendelet meghatározza azt is, hogy melyek a bírság kiszabása során figyelembe veendő tényezők, és azt is, hogy a GDPR mely rendelkezéseinek megsértése milyen mértékű bírság kiszabását vonhatja maga után. Ez azonban nem jelenti, hogy automatikusan bírság kiszabására kerülne sor; a szankció meghatározása előtt a Hatóságnak az eset körülményeinek széleskörű mérlegelését kell elvégeznie. Az értékelési szempontok tekintetében az Unióban egységes megközelítés kialakítása a cél, ennek érdekében a 29-es Adatvédelmi Munkacsoport iránymutatást bocsátott ki (253. számú iránymutatás), amely a többi iránymutatással együtt szintén elérhető a honlapunkról.

Bízom benne, hogy a fentiek elégséges választ tartalmaznak a kérdéseire, amely alapján megfelelő tájékoztatást lehet nyújtani a nyilvánosság számára. Amennyiben a rendelet valamely rendelkezésével kapcsolatban bizonytalanság merülne fel, úgy természetesen a jövőben is forduljon bizalommal a Hatósághoz.

Budapest, 2018. április „ .”

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár