



Ügyszám: NAIH/2018/1310/2/K

[...] részére

[...]

Tisztelt [...]!

A Nemzeti Adatvédelmi és Információszabadság Hatóságnak elektronikus úton küldött levelében azzal kapcsolatban kér tájékoztatást, hogy vonatkozik-e Önre az Európai Unió általános adatvédelmi rendelete (a továbbiakban: GDPR), szükséges-e adatvédelmi auditor bevonása, illetve adatvédelmi szabályzat kidolgozása és bejelentése a Hatóságnak, továbbá milyen kötelezettségei vannak a rendelet alapján. Ezeket illetően az alábbiakat hozom szíves tudomására.

1./ Azt, hogy a GDPR-t mely adatkezelésekre kell alkalmazni, a rendelet tárgyi hatályáról rendelkező 2. cikke alapján lehet eldönteni, amelynek értelmezését a 4. cikkben írt fogalom-meghatározások és a (14)-(18) preambulum-bekezdések segítik. Ezek értelmében a rendeletet a személyes adatok olyan kezelésére kell alkalmazni, amely részben vagy egészben automatizált módon történik (ez jellemzően a számítógépes adatkezelést jelenti), valamint az olyan nem automatizált (azaz manuális, kézi) adatkezelésre is, amely esetében az adatok valamely nyilvántartási rendszer részét képezik, vagy ha az adatokat valamilyen nyilvántartási rendszer részévé kívánják tenni. A nyilvántartás fogalma tágan értelmezendő, annak minősülhet bármilyen jegyzék, lista, amelyben az adatok valamilyen szempont szerint kereshetők, csoportosíthatók.

Miután a leveléből arra lehet következtetni, hogy az adatkezeléseket szálláshely szolgáltatás nyújtása keretében végzi, azokra a fenti rendelkezések alapján a GDPR-t alkalmazni kell. Ugyan a GDPR 2. cikk (2) bekezdés c) pontja alapján a GDPR-t nem kell alkalmazni a személyes adatok kezelésére, ha azt természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik, ez a kivétel csak olyan tevékenységekre vonatkozik, amelyek semmilyen szakmai vagy üzleti tevékenységgel nem hozhatók összefüggésbe [ld. GDPR (18) preambulum-bekezdése].

A GDPR rendelkezéseinek értelmezéséhez hasznos segítséget jelentenek az Adatvédelmi Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport iránymutatásai, amelyek elérhetők – jórészt magyarul is – a Hatóság honlapjáról (<http://www.naih.hu/29-es-munkacsoport-iranymutatasai.html>). Ezen kívül feltehetőleg érdemes áttekinteni a témában az Európai Bizottság felkészítő anyagait is ezeken a hivatkozási címeken: http://europa.eu/rapid/press-release_IP-18-386_hu.htm és

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#library.

2./ Ha az adatvédelmi auditor igénybevételére irányuló kérdése az adatvédelmi tisztviselőre vonatkozik, úgy tájékoztatom, hogy a rendelet 37. cikk (1) bekezdése határozza meg, hogy mikor kötelező a kijelölése. 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, hatókörükénél 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 büncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

A levelében foglalt információk nem utalnak arra, hogy a fenti körülmények valamelyike fennállna az Ön esetében, így feltehetőleg adatvédelmi tisztviselő alkalmazására nem lesz köteles.

Tájékoztatom, hogy az itt írt esetkörök és az adatvédelmi tisztviselő jogállását, feladatait érintő kérdések értelmezésével foglalkozik a 29-es Adatvédelmi Munkacsoport 243. számú iránymutatása, amely szintén elérhető a Hatóság honlapjáról: <http://www.naih.hu/files/Iranymutatas-az-adatvedelmi-tisztvisel-kkel-kapcsolatban.pdf>

3./ Az adatvédelmi szabállyal kapcsolatban tájékoztatom, hogy a GDPR kifejezetten ilyen kötelezettséget nem ír elő az adatkezelők számára. A 24. cikk (2) bekezdése alapján az adatkezelőnek akkor kell belső adatvédelmi szabályokat is alkalmaznia – a személyes adatok védelmének biztosítása céljából megvalósított technikai és szervezési intézkedések részeként – ha az az adatkezelési tevékenység vonatkozásában arányos. Ennek a rendelkezésnek az értelmezését a (78) preambulumbekkezdés segíti. Ez alapján azt kell tehát az adatkezelőnek mérlegelnie, hogy a kezelt adatok mennyisége és köre alapján „arányosnak” mutatkozik-e adatvédelmi szabályzat vagy más szabályrendszer (pl. utasítás, folyamatleírás, biztonsági szabályzat) elkészítése. Ha az adatkezelő az adatvédelmi szabályzat elkészítése mellett dönt, azt külön nem szükséges bejelentenie a Hatóságnak.

4./ 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. Elmondható, 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 felülvizsgálatát, az adathordozhatósághoz való jog biztosítását, az adatkezelési tevékenységekről nyilvántartás vezetését, 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 a szükséges információk nála állnak rendelkezésre. Ezen intézkedések tekintetében a (78) preambulumbekzdés példálózó felsorolást nyújt (belső szabályzat, álnevesítés, adatkezelések szükségességének időszakos felülvizsgálata stb.) A rendeletnek megfelelő adatkezelési tevékenység kialakítása az adatkezelő felelőssége.

Felhívom a figyelmét arra, hogy a Hatóság – eljárási kereteket nélkülöző, konzultációs válaszként kiadott – jelen tájékoztatása sem jogszabálynak, sem egyéb jogi eszköznek nem tekinthető, az normatív jelleggel, jogi erővel, illetve kötelező tartalommal nem rendelkezik. A Hatóság jelen ügyben rendelkezésre bocsátott információk alapján kialakított jogértelmezése más hatóságot, a bíróságot és az adatkezelőt nem köti, annak csak iránymutató jellege van. Az állásfoglalás, tájékoztatás kiadása tehát nem mentesíti annak címzettjét, illetve az adatkezelőt saját jogi álláspontja kialakításának szükségessége, illetve az adatkezelésért fennálló felelősség alól.

Budapest, 2018. április „ .”

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár