Ügyszám: NAIH/2018/2162/2/K

[…] részére

[…]

Tisztelt […]!

A Nemzeti Adatvédelmi és Információszabadság Hatóságnak elektronikus úton küldött levelében az Európai Unió általános adatvédelmi rendeletére (a továbbiakban: GDPR) való felkészülés érdekében, kkv-k és egyéni vállalkozók könyvelése kapcsán azzal kapcsolatban kér tájékoztatást, hogy kiknek kell adatvédelmi szabályzatot készíteniük, van-e ennek valamilyen határa (cégforma, méret), milyen formai követelményei vannak és ki fogja ezeket ellenőrizni.

Ezzel összefüggésben az alábbiakról tájékoztatom.

1. Először is szeretném kiemelni, hogy a GDPR kifejezetten adatvédelmi szabályzatalkotási kötelezettséget – sem mérettől, sem cégformától függően - nem ír elő az adatkezelők számára.

A GDPR 24. cikke az adatkezelő feladatává teszi, 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 történik.

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 ez az adatkezelési tevékenység vonatkozásában arányos. Ennek a rendelkezésnek az értelmezését a (78) preambulumbekezdés segíti.

A GDPR (78) preambulumbekezdés szerint ahhoz, hogy az adatkezelő igazolni tudja az e rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit. Az említett intézkedések magukban foglalhatják a személyes adatok kezelésének minimálisra csökkentését, a személyes adatok mihamarabbi álnevesítését, a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat, stb.

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. A rendeletnek megfelelő adatkezelési tevékenység kialakítása tehát, az adatkezelő felelősségi körébe tartozik.

Azt, hogy konkrét esetben milyen technikai és szervezési intézkedések lehetnek szükségesek, csak az adatkezelés valamennyi körülményének ismeretében lehet eldönteni, amelynek megítélésére ezért elsősorban az adatkezelő képes, miután a szükséges információk nála állnak rendelkezésre. Ezzel kapcsolatban tehát nem lehet általános álláspontot kialakítani.

Amennyiben az adatkezelő az adatvédelmi szabályzat elkészítése mellett dönt, úgy a rendelet nem tartalmaz speciális előírást arra vonatkozóan, hogy a szabályzatnak milyen kötelező tartalmi, formai elemei legyenek. Azonban az, hogy a szabályzat alapján kialakított adatkezelési gyakorlat a GDPR-ral összhangban van-e, az adatkezelő (adatfeldolgozó) felelőssége.

Az Adatvédelmi Irányelv 29. cikke alapján létrejött 29-es Adatvédelmi Munkacsoport 253. számú iránymutatásának III. d) pontja (iránymutatás 13. oldala) - amely egyébként a többi iránymutatással együtt elérhető a honlapunkról - az adatkezelőt (adatfeldolgozót) terhelő felelősség mértékének értékelésével összefüggésben alábbi kérdések vizsgálatát vetette fel, melyek szintén támpontot jelentenek a szabályzat elkészítése szükségességének megítéléséhez:

- Az adatkezelő végrehajtotta-e a beépített vagy alapértelmezett adatvédelem elveinek megfelelő technikai intézkedéseket (25. cikk)?
- Az adatkezelő a szervezet minden szintjén végrehajtotta-e a beépített és alapértelmezett adatvédelem elveinek (25. cikk) érvényesítésére szolgáló szervezési intézkedéseket?
- Gondoskodott-e az adatkezelő/adatfeldolgozó a megfelelő szintű biztonságról (32. cikk)?
- A releváns adatvédelmi eljárások/szabályzatok ismertek-e és alkalmazásra kerültek-e a szervezet megfelelő vezetési szintjein (24. cikk)?

A fentieket összefoglalva: önmagában a szabályzat megírásának elmaradása nem von maga után szankciót, hiszen külön szabályzatalkotási kötelezettséget nem is ír elő a GDPR, azonban valamely jogsértés elbírálásakor a megfelelő korrekciós intézkedés alkalmazásával összefüggésben a Hatóság mérlegeli – többek között – az adatvédelmi szabályok ismeretével és alkalmazásával kapcsolatos információkat is.

2. A GDPR 51. cikk (1) bekezdése értelmében tagállami szinten kerül sor a rendelet alkalmazásának ellenőrzéséért felelős (egy vagy több) független közhatalmi szerv (azaz a felügyeleti hatóság) kijelölésére.

Ezt hazánkban az Infotv. módosításáról szóló tervezet tartalmazza, mely már elkészült, és az várhatóan hamarosan benyújtásra kerül az Országgyűlés elé. A tervezet szerint e kijelölt szerv Hatóságunk lesz.

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. május „ „.

Üdvözlettel:

Dr. Péterfalvi Attila
elnök
c. egyetemi tanár