



Ügyszám: NAIH/2018/788/2/K

[...] részére

[...]

[...]

Tisztelt [...]!

A Nemzeti Adatvédelmi és Információszabadság Hatóságnak elektronikus úton küldött levelében a GDPR-nak való megfeleléssel kapcsolatban több kérdésben is tájékoztatást kér, amellyel összefüggésben az alábbiakat hozom szíves tudomására.

1./ Az első kérdése az adatvédelmi rendeletnek való megfelelés első lépéseként említett ún. adattérkép elkészítésével kapcsolatban arra irányul, hogy mely adatkezeléseket szükséges összefoglalni benne.

a) Először is szeretném előre bocsátani, hogy a GDPR az „adattérkép” kifejezést nem használja, ezért erre a fogalomra először azt az értelmezést tekintem irányadónak, hogy az adattérkép elkészítése a kezelt adatok milyenségének, mennyiségének, típusának felmérésére vonatkozó tevékenység, amely által jobban meghatározhatók az adatkezelő kötelezettségei.

Ez alapján azt, hogy a már megkezdett adatkezelések közül melyeket érdemes áttekinteni a GDPR-nak való megfelelés érdekében, elsősorban a GDPR hatálya határozza meg. Ki kell emelnem, hogy e tekintetben a rendelet igen széles körben rendeli alkalmazandónak a szabályait: a 2. cikk (1) bekezdése szerint a rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak az adatoknak a nem automatizált kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni. E rendelkezés tehát nem tesz különbséget az adatkezelés jogalapja szerint, a GDPR egyaránt vonatkozik – egyebek mellett – a jogszabályon és a hozzájáruláson alapuló adatkezelésekre. Erre figyelemmel feltehetőleg érdemes lesz minél teljesebb terjedelemben felmérni az önkormányzati hivatal adatkezelési tevékenységeit, amely által adatkezelésenként beazonosítható és ellenőrizhetővé válik, hogy melyik adatkezelés milyen jogalapon történik.

Megjegyzem, hogy kifejezetten olyan kötelezettséget a GDPR nem ír elő, hogy az adatkezelő a rendeletnek való megfelelés érdekében a folyamatban lévő adatkezelések tekintetében végezze el a fenti helyzetelemzést, azonban a felkészülés érdekében hatékony módszer.

b) Az előzőhöz hasonló, ám attól tartalmában eltér az adatkezelési tevékenységek nyilvántartása. Az adatkezelési nyilvántartásról a GDPR 30. cikke rendelkezik, amelynek értelmezését a (82) preambulumbekkezdés segíti. Ezek alapján – figyelemmel a (79) preambulumbekkezdésre is – minden adatkezelő a saját felelősségi körébe tartozóan köteles az adatkezelési tevékenységek nyilvántartására a rendeletben meghatározott tartalommal. A GDPR e tekintetben sem tartalmaz eltérő szabályozást a jogszabályon alapuló kötelező adatkezelésekre vonatkozóan. A nyilvántartás-vezetési kötelezettség alól a rendelet egyedül a 250 főnél kevesebb személyt foglalkoztató vállalkozásokat és szervezeteket mentesíti, ha az adatkezelési tevékenységük nem esik az ott írt esetek közé [ld. 30. cikk (5) bekezdése]. Megjegyzem, hogy a GDPR 4. cikk 9. pontja alapján azok a közhatalmi szervek, amelyek egyedi vizsgálat keretében az uniós vagy tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, a rendelet alkalmazásában nem minősülnek címzetteknek, így az ennek megfelelő közhatalmi személyi kört a nyilvántartásban a címzettek között nem kell feltüntetni.

2./ A levél második pontjában azzal kapcsolatban érdeklődik, hogy a GDPR szempontjából van-e teendő a városi facebook oldallal, illetve a városi hírlevélre való feliratkozással kapcsolatban.

A GDPR-nak megfelelő adatkezelés kialakítása az adatkezelő kötelezettsége és felelőssége, így az említett esetekben azt kell megvizsgálni, hogy ki minősül adatkezelőnek. A GDPR 4. cikk 7. pontjának meghatározása szerint adatkezelő az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.

A városi facebook oldal létrehozója álláspontom szerint előre meghatározott adatkezelési szabályokhoz csatlakozik, a beállítási opciók közötti választásra csak korlátozott lehetősége van, így az adatkezelés felülvizsgálatára, módosítására nincs valódi ráhatása. A facebook oldal látogatóinak adataival tervezett további adatkezelés, valamint a városi hírlevélre való feliratkozás tekintetében már felmerülhet a további tennivalók szükségessége (pl. az érintettek tájékoztatásának, hozzájárulásainak áttekintése), azonban az adatkezelés részleteit illető egyéb információ hiányában (pl. adatfeldolgozó bevonására sor kerül-e) azzal kapcsolatban konkrét álláspontot nem lehet kialakítani.

3./ A beadványa 3. és 4. pontja az adatvédelmi hatásvizsgálattal kapcsolatos kérdéseket tartalmaz: egy hivatal tekintetében milyen esetben kell adatvédelmi hatásvizsgálatot lefolytatni, és mi alapján lehet megállapítani, hogy az adatkezelési művelet magas kockázattal jár-e vagy sem?

A GDPR 35. cikk (1) bekezdése határozza meg, hogy az adatvédelmi hatásvizsgálatot mikor kell elvégezni, a (3) bekezdés pedig példalózó felsorolást ad ezekre az esetekre, illetve további eligazítást nyújt a (91) preambulumbekkezdés. Ha a kérdéses tervezett adatkezelés nem esik a megadott példák közé, akkor valóban az adatkezelés valószínűsíthetően magas kockázatának megítélése a meghatározó. A személyek jogait és szabadságait érintő kockázatok feltérképezéséhez és értelmezéséhez a (75) preambulumbekkezdésben foglaltak szolgálnak irányzékkul.

Tájékoztatom, hogy a GDPR 35. cikk (4) bekezdése értelmében Hatóságunk összeállít és nyilvánosságra hoz majd egy jegyzéket, amely azon adatkezelési műveletek típusait tartalmazza, amelyekre vonatkozóan az adatvédelmi hatásvizsgálatot el kell végezni. Megjegyzem, hogy miután a 35. cikk (6) bekezdése értelmében e lista elfogadását megelőzően a Hatóságnak még egységességi mechanizmust is igénybe kell vennie, amelyre csak a GDPR alkalmazandóvá válását követően van lehetőség, e jegyzék elfogadása szintén csak ezen időpontot követően történhet meg.

A GDPR 35. cikk (1) bekezdése azonban az adatkezelőkre nézve olyan kötelezettséget fogalmaz meg, amely az említett listától függetlenül írja elő az adatvédelmi hatásvizsgálat elkészítését, ha a meghatározott feltételek fennállnak. Ebből következően amennyiben az adatkezelés az e bekezdésben foglaltakat teljesíti, úgy az adatvédelmi hatásvizsgálat elkészítésétől nem lehet eltekinteni. A 35. cikk (4) bekezdés szerinti lista az adatkezelő mérlegelési tevékenységét segíti azzal, hogy a listán szereplő adatkezelési műveletek tekintetében nem kell feltérképeznie, számba vennie és értékelnie az érintettre vonatkozó hatásokat, azonban maga a kötelezettség a listától függetlenül fennáll.

Szeretném még felhívni a figyelmét az Adatvédelmi Irányelv 29. cikke alapján létrehozott Adatvédelmi Munkacsoport 248. számú iránymutatására, amely kifejezetten az adatvédelmi hatásvizsgálattal kapcsolatos kérdésekkel foglalkozik részletesen. Ez az iránymutatás magyarul is elérhető a Hatóság honlapjáról (<http://www.naih.hu/29-es-munkacsoport-iranymutasai.html>).

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. március „ .”

Üdvözlettel:

Dr. Péterfalvi Attila  
elnök  
c. egyetemi tanár