



Ügyszám: NAIH-13119-2/2024.
Ügyintéző: dr. Berei Szonja
E-mail: berei.szonja@naih.hu
Tel.: 391-1412

Dr. Rédey Krisztina részére
közigazgatási államtitkár
Miniszterelnöki Kabinetiroda

kat@mk.gov.hu

Tisztelt Államtitkár Asszony!

Magyarország kiberbiztonságáról szóló törvény tervezetére a személyes adatok védelme és a közérdekű adatok nyilvánossága szempontjából a következő észrevételt teszem.

1. A tervezet több új, személyes adatokat is tartalmazó nyilvántartás létrehozásáról rendelkezik. Ilyen: a 11. § (13) bekezdése, a 20. § (legfelső szintű doménnév-nyilvántartás), 28. § (hatósági nyilvántartás), 29. § (SZTFH által vezetett nyilvántartás). Ezekről a nyilvántartásokról egységesen elmondható, hogy a szabályozásuk hiányos. Erre vonatkozó információk hiányában nem világos, hogy elkészültek-e az előzetes adatvédelmi hatásvizsgálatok, amelyekről az általános adatvédelmi rendelet 35. cikke és az információs önrendelkezési jogról és az információbiztonságról szóló 2011. évi CXII. törvény 25/G. §-a rendelkezik.

A 11. § (13) bekezdésében szabályozott nyilvántartással kapcsolatban nem rendelkezik arról a tervezet, hogy kik és hogyan kerülnek be, és főleg milyen személyes adataikkal a nyilvántartásba, valamint hogyan lehet onnan kikerülni, meddig tart az adatkezelés, lehetséges-e adattovábbítás a rendszerből. A legfelső szintű doménnév-nyilvántartás esetében hiányzik az adatkezelési cél megjelölése (a személyes adatok kezelésének célját kell megjelölni), továbbá itt is az adatkezelés ideje, arról való rendelkezés, hogy ki férhet hozzá ezekhez az adatokhoz (lehetséges-e adattovábbítás), meddig tart az adatkezelés.

A 28. § (1) bekezdésével kapcsolatban felhívom rá a figyelmet, hogy nem megfelelő adatkezelési cél az: „e törvényben meghatározott feladatainak végrehajtása céljából” fordulat, és az Alkotmánybíróság is ezt az álláspontot képviseli gyakorlatában. Ebből a fordulatból hiányzik az a konkrétum, amely alapján megítélhető lenne az érintett, a jogalkalmazó és az adatkezelés felügyeletét ellátó szerv számára is az, hogy az adatkezelés valóban eleget tesz az általános adatvédelmi rendeletben meghatározott alapelveknek, és az adatkezelési cél eléréséhez szükséges, azzal arányos, annak elérésére alkalmas.

A 29. § szerinti nyilvántartás esetében szintén az adatkezelési cél megjelölés hiányzik.

A tervezet 76. §-ában található adatkezelési szabályok további átgondolást tesznek szükségessé. A nyilvántartások és a különböző adatkezelések összevonása miatt egyáltalán nem derül ki, hogy miért van szükség és miért ilyen hosszú adatmegőrzési időre az egyes esetekben. A normaszövegből ki kell derülnie, hogy miért szükséges pl. egy szervezet tevékenységének

megszűnése után még öt évig nyilvántartani az adatait, mi ennek az adatkezelésnek a célja? Kiemelt tekintettel arra az esetre, ha a szervezet nyilvántartásba vétele, és a vonatkozó személyes adatok nyilvántartásának célja a szervezet működéséhez kapcsolódott. Éppen ezért ennek a 76. §-nak a teljes átgondolását és a szabályok sokkal részletesebb kidolgozását javaslom.

2. A tervezet 65-67. §-ához a következő kiegészítést javaslom a kiberbiztonsági incidenskezelő központhoz bejelentett olyan incidensekre vonatkozóan, amelyek egyben személyes adatokat is érintenek, tehát a GDPR vagy Infotv. szerint egyben adatvédelmi incidensnek is minősülnek: a javaslatom, hogy ezekről az incidensekről a kiberbiztonsági incidenskezelő központ kéthavonta tájékoztassa az adatvédelmi hatóságot a bejelentő adatkezelő, az érintett személyes adatok kategóriája, a bejelentés dátuma és az incidens rövid leírásával. Így meg lehetne azt vizsgálni, hogy a kiberbiztonsági incidenskezelő központhoz és NAIH-hoz is bejelentett, személyes adatokat is érintő incidensek között milyen összefüggések vannak, azok mennyire vannak átfedésben és szükséges-e az esetleges eltérések miatt vizsgálatot indítani.

Budapest, *az elektronikus aláírás és időbélyegző szerint*

Üdvözlettel

Dr. habil. Péterfalvi Attila,
elnök, c. egyetemi tanár