NEMZETI SZAKÉRTŐI ÉS KUTATÓ KÖZPONT
(SZERVEZETI EGYSÉG)

Informatikai rendszerekre, rendszerelemekre és tevékenységekre vonatkozó kiemelt adatkezelési követelmények[1]

1. Az NSZKK informatikai rendszereinek és rendszerelemeinek tervezése, beszerzése, fejlesztése, bevezetése, migrációja, használata, üzemeltetése, karbantartása, üzemi állapotból kivezetése, leállítása, selejtezése, megsemmisítése során a funkcionális és felhasználói elvárások mellett az adatvédelmi elvárásokat azonos prioritással kell kezelni.
2. Az adatvédelmi elvárásokat az informatikai rendszerek és rendszerelemek NSZKK szerinti életciklusának tervezésének kezdetén dokumentáltan meg kell határozni a rendszerek és rendszerelemek teljes életciklusára vonatkozóan („privacy by design") és azt következetesen alkalmazni kell, az elvárásokat enyhíteni nem megengedett.
3. Az adatvédelmi elvárások az informatikai rendszer, rendszerelem tulajdoni viszonyaitól (saját tulajdonú, bérelt, lízingelt, ingyenesen használatba vett stb.), üzemeltetői jellegétől (belső üzemeltetésű, külső partner által üzemeltetett, vegyes üzemeltetésű stb.), kialakításától (telepítés nélkül futtatható, telepített vastagklienses, telepített köztesréteg megoldású, telepített böngészőből elérhető, SaaS, IaaS, PaaS, magánfelhő szolgáltatás, publikus felhőszolgáltatás stb.), felhasználói céljától (üzemi rendszer, felhasználói tesztrendszer, fejlesztői tesztrendszer stb.) függetlenül egyaránt betartandóak.
4. Az informatikai rendszer, rendszerelem tervezésének és üzemeltetésének előkészítésébe, valamint bármilyen, ezek működését illetve adatkezelését érintő adminisztratív, logikai, műszaki vagy egyéb módosításba a tervezés előkészületi szakaszában be kell vonni az Informatikai Csoport vezetőjét, az elektronikus információ biztonságért felelős személyt, a biztonsági vezetőt, az adatvédelmi tisztviselőt és a rendszert használni kívánó szervezeti egységek képviselőit, akik előzetes, írásos jóváhagyása feltétele az informatikai rendszerre, rendszerelemre vonatkozó beruházás, módosítás, változtatás pénzügyi jóváhagyásra előterjesztésének és a későbbi megvalósításnak, üzembe állításnak.
5. Az informatikai rendszerre, rendszerelemre tervezésének előkészítése során, a beruházás pénzügyi jóváhagyásra előterjesztését megelőzően a telepítést kezdeményező szervezeti egység vezetője köteles elkészíteni a Nemzeti Szakértői és Kutató Központ adatkezelési és adatvédelmi szabályzatáról szóló 25/2019. (XII. 17) NSZKK főigazgatói intézkedésben előírt adatvédelmi kockázatelemzést és hatásvizsgálatot. Pénzügyi jóváhagyásra előterjesztés, és azt követő döntés, beszerzés, telepítés, üzemeltetés csak olyan informatikai rendszer, rendszerelem esetében megengedett, amelynél az adatvédelmi hatásvizsgálat előzetesen igazolta, hogy az adatkezelés nem jár magas kockázattal.
6. Az NSZKK-ban kizárólag olyan informatikai rendszer, rendszerelem alkalmazható, amely esetében
    a) rendelkezésre áll
        i. az NSZKK számára fejlesztett termék esetében

[1] Az eredeti normát az M8. melléklettel kiegészítette a 6/2020. (IV.28.) NSZKK főigazgatói intézkedés, hatályba lépett 2020. április 29-én vagy 2020. április 30-án.

1. a felhasználói és informatikai specifikáció,
2. az adatvédelmi kockázatelemzés és hatásvizsgálat,
3. az üzemeltetési leírás (beleértve az üzemeltetéshez szükséges feladatok részletes leírásával és a hibaüzenetek, valamint kezelésük leírásával),
4. a felhasználók és jogosultságaik karbantartási lehetőségének leírásával,
5. a naplóállományok felépítésének és tartalmának leírása,

ii. kereskedelmi forgalomban beszerezhető termék esetében

1. az adatvédelmi kockázatelemzés és hatásvizsgálat,
2. az üzemeltetési leírás (beleértve az üzemeltetéshez szükséges feladatok részletes leírásával és a hibaüzenetek, valamint kezelésük leírásával),
3. a felhasználók és jogosultságaik karbantartási lehetőségének leírásával,
4. a naplóállományok felépítésének és tartalmának leírása;

b) az informatikai rendszert, rendszerelemet használók (továbbiakban: felhasználók) egyértelműen azonosíthatóak és azonosításra is kerülnek;

c) a felhasználók jogosultságai megfelelő jogosultsággal informatikai közreműködés nélkül, felhasználói felületről is állíthatók;

d) a felhasználók jogosultság-állítása keretében beállítható, hogy adott kezelt adatot a felhasználó adott művelet során hogyan érhet el (létrehozhatja, olvashatja, módosíthatja, másik adattal összekapcsolhatja vagy a kapcsolatot megszüntetheti, törölheti);

e) a felhasználók tevékenysége a bejelentkezési kísérlettől a használat befejezéséig egyértelműen és teljes körűen naplózásra kerül (beleértve a sikertelenül és sikeresen megkísérelt műveleteket, továbbá az olvasási, létrehozási, módosítási, törlési és exportálási műveleteket), kiemelten az adatkezelési műveletek esetében; a műveletet végző felhasználó azonosításra alkalmas adatával és a művelet legalább ezredmásodperc pontosságú időadatával együtt;

f) az informatikai rendszer és rendszerelem ideje (belső órája) rendszeresen (de legalább naponta) szinkronizálásra kerül az NSZKK által meghatározott referencia időforráshoz;

g) a naplóállomány módosítás és törlés ellen védett;

h) a naplózás a naplóállományra vonatkozó módosítási és törlési kísérleteket is naplózza és arról automatikus, azonnali üzenetet küld az Informatikai Csoport vezetőjének, az elektronikus információ biztonságért felelős személynek, az adatvédelmi tisztviselőnek és a biztonsági vezetőnek;

i) a naplóállományok tárolási ideje paraméterezhető, de legalább

i. a rendszerek és rendszerelemek működési jellemzői esetében legalább 90 nap;

ii. a felhasználókra és jogosultságaikra vonatkozó műveletek esetében legalább 8 évig terjed;

iii. az adatok olvasása és exportálása esetén legalább egy évig terjed;

iv. az adatok létrehozása, módosítása és törlése esetében az adatokra meghatározott irattárazási idő végéig terjed;

v. a naplózásra vonatkozó műveletek, továbbá a naplózási paraméterek változtatása esetén időben korlátlan;

j) a naplóállományok megfelelő jogosultsággal informatikai közreműködés nélkül, felhasználói felületről is értékelhető módon lekérdezhetők;

k) a naplózási hiba esetén (kiemelten beleértve a naplózásra szolgáló tárhely megtelését vagy elérhetetlenné válását) leállítja az informatikai rendszer, rendszerelem használatát (beleértve az olvasási lehetőséget is) és erről automatikus, azonnali üzenetet küld az Informatikai Csoport vezetőjének, az elektronikus információ biztonságért felelős személynek, az adatvédelmi tisztviselőnek és a biztonsági vezetőnek;

l) az egyes adatok tárolási ideje meghatározható;

m) a tárolási idő határát elérő adatok egyértelműen azonosíthatók;

n) a tárolási idő határát elérő adatok az informatikai rendszer, rendszerelem működését nem veszélyeztető, naplózott és dokumentált módon eltávolíthatók vagy felismerhetetlenné módosíthatóak, melynek során és utána az informatikai rendszer, rendszerelem adatainak konzisztenciája, integritása, sértetlensége, kapcsolatai változatlanok maradnak;

7. Az adatkezelési elvárásoknak meg nem felelő informatikai rendszer, rendszerelem az NSZKK-ban nem használható

8. A szabályzat kiadásakor üzemben levő informatikai rendszerről, rendszerelemről az azok üzembe állítását kezdeményező, valamint az azokat üzemeltető szervezeti egység a szabályzat kiadását követő 30 napon belül köteles tájékoztatni az NSZKK Informatikai Csoportját, amely az informatikai rendszerekről, rendszerelemekről a szabályzat kiadását követő 90 napon belül nyilvántartást készít, amelyet a későbbiekben naprakészen tart.

9. A szabályzat kiadásakor üzemben levő, de az elvárásoknak nem megfelelő informatikai rendszer, rendszerelemet megfelelővé tételéről vagy kiváltásáról az azokat üzemeltető szervezeti egység vezetőjének a szabályzat kiadását követő 180 napon tervet kell készítenie és azt elfogadásra elő kell terjesztenie a Főigazgató felé.

10. Az informatikai rendszerek és rendszerelemek ebben a mellékletben leírtaknak megfelelőségét az elektronikus információ biztonságért felelősnek rendszeresen, dokumentált módon legalább évente ellenőriznie szükséges és a nem-megfeleléseket jelenteni kell a Főigazgatónak.

11. Az ebben a mellékletben leírtaknak meg nem felelő informatikai rendszer, rendszerelem telepítésének és üzemeltetésének valamennyi kockázatáért és következményéért (beleértve a funkcionális nem-megfelelőségéért, valamint az adatkezelés nem-megfelelése miatti hatósági elmarasztalásokért, büntetésekért, kártérítésekért és sérelemdíjakért, valamint további pénzügyi szankciókért) az előírásokat be nem tartó szervezeti egység vezetője felelős.