3. melléklet a 25/2019. (XII. 17.) NSZKK főigazgatói intézkedéshez

NEMZETI SZAKÉRTŐI ÉS KUTATÓ KÖZPONT
(SZERVEZETI EGYSÉG)

ADATVÉDELMI INCIDENSKEZELÉS ÉS NYILVÁNTARTÁS ELJÁRÁSI RENDJE

1. Adatvédelmi incidens észlelése esetére vonatkozó értesítési és bejelentési kötelezettség

Ha az NSZKK bármely alkalmazottja, vagy közreműködője adatvédelmi incidenst vagy arra utaló jelet észlel, vagy arra gyanakszik, azt azonnal jeleznie kell a szervezeti egysége vezetőjének.

Az adatvédelmi incidensről a Hivatalvezetőnek haladéktalanul tájékoztatnia kell az NSZKK főigazgatóját és az Adatvédelmi Tisztviselőt. A Hivatalvezető esetleges elérhetetlensége esetén a tájékoztatást az illetékes Adatgazdának kell megtennie.

Az Adatvédelmi Tisztviselőnek a Hivatalvezetővel együttműködve indokolatlan késedelem nélkül, legkésőbb 72 órán belül be kell jelentenie az adatvédelmi incidenst a felügyeleti hatóság (NAIH) részére. Ha ez nem lehetséges, akkor meg kell indokolni a késedelmet a felügyeleti hatóságnak. Mellőzhető a bejelentés, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira nézve. Az incidens bejelentésének mellőzése kizárólag az Adatvédelmi Tisztviselő ilyen tartalmú állásfoglalása alapján lehetséges.

A bejelentést a http://naih.hu/adatvedelmi-incidensbejelent--rendszer.html oldalon online, vagy papír alapon a NAIH adatvédelmi incidens bejelentő űrlapjával azonos tartalommal kell megtenni.

2. Adatvédelmi incidens minősítése és szintjei

Adatvédelmi incidensnek számít minden esemény, amelynek során az NSZKK által kezelt vagy feldolgozott személyes adattal az alábbiak valamelyike történik (*adatkezelési adatvédelmi incidens*)

- illetéktelenek férnek hozzá (az adat kompromittálódik)
- nem a munkafolyamatokban előírt módon módosul (pl. jogosulatlanok megváltoztatják vagy törlik)
- elérhetősége megváltozik (nem úgy, vagy nem akkor férnek hozzá, ahogy, vagy amikor arra a munkafolyamathoz szükséges)

Az NSZKK az adatvédelmi incidensek felmerülése esetén az adott incidenst az alábbiak szerint sorolja szintekbe:

- ***Alacsony szintű adatvédelmi incidens***: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy az azokhoz való jogosulatlan hozzáférés. Ilyen eset különösen az, ha az adat nem köthető természetes személyhez.

- ***Magas szintű adatvédelmi incidens***:
    - a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy az azokhoz való jogosulatlan hozzáférés,
    - az adatok körétől függetlenül minden olyan eset, amikor az incidensnek az érintettre súlyosan hátrányos hatása valószínűsíthető, vagy a hátrányos következmény bekövetkezése biztos.
- Adatvédelmi incidens kivizsgálása és az ok megszüntetése

Az adatvédelmi incidenst haladéktalanul ki kell vizsgálni, és soron kívül meg kell tenni a szükséges lépéseket az adatvédelmi incidenst előidéző ok megszüntetésére. Az adatvédelmi incidenst az illetékes Adatgazda végzi az Adatvédelmi Tisztviselő, a Hivatalvezető, valamint, ha az adatvédelmi incidens informatikai jellegű, az Informatikai Csoport vezetőjének bevonásával, továbbá a kivizsgálásba ugyancsak be kell vonni az esetlegesen érintett Adatfeldolgozókat is.

Ha a gyanú szerint magas szintű adatvédelmi incidensre került sor, azonnal, de legkésőbb 24 órán belül szükséges elvégezni az ahhoz szükséges vizsgálatokat, hogy megállapítható legyen, hogy az incidens oka az NSZKK-nak, vagy valamely Adatfeldolgozónak róható fel és a vizsgálat eredményéről tájékoztatni kell a vizsgálatba bevontakat.

Ha az incidens oka a valamely Adatfeldolgozó által nyújtott szolgáltatással függ össze, akkor közre kell működni az incidens kezelésével összefüggő intézkedések meghozatalában.

Az incidens okától függetlenül meg kell tenni minden elvárható lépést, az ésszerűen elvárható határidőn belül.

Ha a gyanú szerint alacsony szintű adatvédelmi incidensre került sor, 72 órán belül el kell végezni az ahhoz szükséges vizsgálatokat, hogy meg lehessen állapítani, az incidens oka az NSZKK-nak vagy valamely Adatfeldolgozónak róható fel és a vizsgálat eredményéről tájékoztatni kell a vizsgálatba bevontakat.

Ha az incidens oka valamely Adatfeldolgozó által nyújtott szolgáltatással függ össze, akkor közre kell működni az incidens kezelésével összefüggő intézkedések meghozatalában.

Az incidens okától függetlenül meg kell tenni minden elvárható lépést, az ésszerűen elvárható határidőn belül.

Az adatvédelmi incidens vizsgálata során

- elemezni kell az adatkezelés környezetét, a megsérült adatok fajtáját, beleértve az adatkezelés valamennyi körülményét,
- meg kell határozni az azonosíthatóság mértékét, azaz fel kell tárni, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehetséges az érintettek azonosítása,
- meg kell vizsgálni a sérülés körülményeit, elsősorban a megsérült adat biztonságának csökkenését, illetve a rosszindulatú támadásra és a szándékosságra utaló valamennyi jelet.

Ha az Adatfeldolgozó bármely, az NSZKK-tól érkező jelzés alapján megállapítja, hogy bármilyen szintű adatvédelmi incidens oka az ő szolgáltatásának működésével függ össze, akkor a szolgáltatás hibájának javítását

- ***magas szintű*** incidens esetén haladéktalanul,
- **alacsony szintű** incidens esetén 72 órán belül megkezdi,

a hibajavítást pedig

- ***magas szintű*** incidens esetén a lehetőségekhez képest, az ésszerűen elvárható határidőn belül legkorábban,
- **alacsony szintű** incidens esetén legfeljebb 30 napon belül befejezi, és a hibajavításról tájékoztatja a vizsgálatba bevontakat.

3. Az érintettek tájékoztatása

Ha az incidens valószínűsíthetően magas kockázattal jár, a Hivatalvezető gondoskodik arról, hogy az érintetteket indokolatlan késedelem nélkül tájékoztassák.

Az adatvédelmi incidensről az érintetteknek szóló tájékoztatásban az NSZKK-nak az alábbi adatokat kell megjelölnie:

- érintett személyes adatok körét és számosságát,
- incidenssel érintettek körét, számát,
- incidens időpontját,
- incidens körülményeit,
- incidens hatását, várható következményeit az érintettek és az NSZKK számára,
- incidens elhárítása érdekében az NSZKK által tett intézkedések, beleértve
- az incidens továbbterjedésének megakadályozása érdekében tett és tervezett intézkedéseket,
- az incidens hatásának csökkentése érdekében tett és tervezett intézkedéseket
- incidenssel kapcsolatos egyéb lényeges adatokat.

.

Az érintettek értesítése nem szükséges:

- ha az adat titkosítva volt és értelmezhetetlen a jogosulatlanul hozzáférő számára,
- vagy valószínűsíthetően nem jár magas kockázattal az érintettek jogaira és szabadságára nézve,
- vagy ha az értesítés aránytalanul nagy erőfeszítést igényelne az adatkezelő részéről - ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását (pl. sajtóközleményt kell kiadni).

4. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidenseket (vagy annak gyanúját) az Adatvédelmi Tisztviselőnek nyilvántartásba kell venni, az incidensek jellemzőivel együtt. A nyilvántartást az adott incidens vizsgálata során kapott információval frissíteni kell, annak érdekében, hogy az NSZKK az incidensek valamennyi jellegzetességét egy helyen, elemzésre és további jelentésre alkalmas állapotban tárolja.

Az incidensek nyilvántartására az M3A. számú *„Adatvédelmi incidens nyilvántartása"* mellékletében levő sablont kell használni.

Az incidenseket továbbá az Adatkezelési Nyilvántartásban is fel kell tüntetni az arra vonatkozó oszlopban történő jelzéssel.