A DÉLI ASZC KISKUNFÉLEGYHÁZI MEZŐGAZDASÁGI ÉS ÉLELMISZERIPARI TECHNIKUM, SZAKKÉPZŐ ISKOLA ÉS KOLLÉGIUM

ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZATA

Székhely: 6100 Kiskunfélegyháza, Petőfi S. u. 2/A

Készült: 2023.01.31.

adatvédelmi tisztviselő

igazgató

PREAMBULUM

Jogszabályi háttér

- Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Adatkezelés biztonsága

Az adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatvédelmi incidens kockázatát.

Az adatkezelő intézkedéseket hoz annak biztosítására, hogy az adatkezelő irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat.

Intézkedések:

- az adatkezelő rendszer jogosultalan személyek általi hozzáférésének megtagadása,
- az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozása,
- az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint a tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozása,
- az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozása,
- annak biztosítása, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férhetnek hozzá,
- annak ellenőrizhetővé tétele, hogy a személyes adatokat adatátviteli berendezés útján mely címzettek továbbíthatják, bocsájthatják rendelkezésre,
- annak ellenőrizhetővé tétele, hogy mely személyes adatokat mely időpontban és ki vitt be az adatkezelő rendszerbe,
- a személyes adatok továbbítása vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, módosításának vagy törlésének megakadályozása,
- annak biztosítása, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen,
- annak biztosítása, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.

1. A szabályzat hatálya, érvényessége

A szabályzat területi hatálya: kiterjed az adatkezelő teljes működési területére, valamennyi alkalmazott informatikai eszközre és szoftverre.

A szabályzat személyi hatálya: kiterjed az adatkezelővel munkaviszonyban vagy munkavégzésre irányuló jogviszonyban álló valamennyi természetes és jogi személyre.

A szabályzat időbeli hatálya: a kiadás napjától visszavonásig érvényes.

A szabályzat érvényesítése és a megismerési kötelezettség: a szabályzat kidolgozása, elkészítése és szükség szerinti módosítása az adatvédelmi incidens-kezelési csoport feladata.

A szabályzatban előírtak betartatásáért hatás- és jogosultsági körére vonatkozóan minden érintett alkalmazott felelős.

A szabályzatban előírtak betartásának ellenőrzése az érintett szervezeti egység vezetőjének feladata.

A szabályzat előírásait az adatkezelőnél dolgozó minden személy a szakmai feladatköréhez szükséges mértékben köteles megismerni, a vonatkozó előírásokat betartani és betartatni.

A szabályzat egyes előírásait a munkavégzéséhez szükséges mértékben minden, az adatkezelővel munkaviszonyban, illetve egyéb szerződéses jogviszonyban álló foglalkoztatottal ismertetni kell.

A szabályzat előírásait megszegőkkel, illetve a jelentési kötelezettséget elmulasztókkal szemben a hatályos törvényeknek, rendeleteknek és belső szabályzatnak megfelelő, jogszerű felelősségre vonást kell alkalmazni.

2. Az adatvédelmi incidens-kezelő csoport

A csoport döntést hozó vezetője az intézmény igazgatója.

Az adatvédelmi incidenst vizsgáló csoport tagjai:

- igazgató,
- adatvédelmi tisztviselő,
- rendszergazdai feladatokat ellátó személy,
- az érintett terület vezetője, ahol az incidens bekövetkezett.

3. Az incidens kezelésével összefüggő feladatok

- az incidens azonosítása,
- az incidens minősítését bizonyító adatok, dokumentumok vizsgálata,
- az incidens által bekövetkezett kockázat, kár, veszélyhelyzet maghatározása,
- az elhárítás érdekében teendő intézkedések meghatározása,
- az incidens bejelentésére vonatkozó döntés meghozatala,
- az incidens okainak feltárása,
- az érintettek tájékoztatása,

- a teljes vizsgálat megindítása,
- kapcsolattartás a NAIH-val.

4. Adatvédelmi incidens azonosítása, minősítése, típusa

Adatvédelmi incidens fogalma:

A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok

- véletlen vagy jogellenes megsemmisítését, elvesztését,
- megváltozását,
- jogosulatlan közlését,
- vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az adatvédelmi incidens típusai:

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek:

- a személyes adatok feletti rendelkezés elvesztését,
- a jogok korlátozását,
- a hátrányos megkülönböztetést,
- a személyazonosság-lopást vagy a személyazonossággal való visszaélést,
- a pénzügyi veszteséget,
- az álnevesítés engedély nélküli feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését,
- a természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Az azonosítást követően a minősítés érdekében tisztázni kell az alábbiakat:

- Milyen kockázatot jelent az érintett természetes személy(ek) jogaira és szabadságaira tekintettel.
- Kiváltó okok, körülmények, amelyek az incidens bekövetkezéséhez vezettek. Az incidens bekövetkezésének körülményei.
- A személyes adatok érzékenységének meghatározása.
- Az incidensben érintett személyes adatok száma.
- Az érintett adatok fajtái, illetve az érintetti kör speciális tulajdonságai.

5. Adatvédelmi incidens bejelentése

Az adatvédelmi incidenst az érintett részleg, illetve az adatfeldolgozó a tudomására jutást követően köteles indokolatlan késedelem nélkül azonnal jelenteni az adatvédelmi incidens-kezelő csoport valamely állandó tagjának.

Az adatkezelő az adatvédelmi incidens-kezelő csoport döntése alapján az adatvédelmi incidenst a tudomásszerzést követően indokolatlan késedelem nélkül, de legkésőbb 72 órával bejelenti az illetékes felügyeleti hatóságnak, a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Ha a bejelentés nem tehető meg 72 órán belül, meg kell jelölni a késedelem okát, és további késedelem nélkül közölni kell a rendelkezésre álló és kért információkat részletekben.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell a késedelem igazolására szolgáló indokokat is.

A bejelentés a NAIH honlapján elérhető online felületen, postai levélben vagy e-mailben a NAIH által biztosított elektronikus formanyomtatvány kitöltésével történik meg.

A bejelentés tartalmazza:

- az adatvédelmi incidens jellegét, az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségét,
- az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetését,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetését.

A gyakorlatban tipikusan előforduló incidenstípusok:

- téves címzés miatti félrepostázások, téves címzett részére küldött elektronikus levelek,
- e-mailek küldése több címzett részére oly módon, hogy a címzettek nem a „Titkos másolat”, hanem a „Másolatot kap” mezőben vannak felsorolva,
- hackertámadás következtében kiszivárgott adatok,
- ellopott vagy elveszett számítástechnikai eszközök, telefonok esete.

6. Az érintettek tájékoztatása

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről, amely tartalmazza

- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens jellegét, következményeit,
- az orvoslásra tett vagy tervezett intézkedéseket.

Nem kell tájékoztatni az érintettet, ha

- az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták,
- a személyes adatok titkosítva voltak,
- az adatkezelő által tett intézkedések eredményeként a magas kockázat valószínűsíthetően nem valósul meg,
- aránytalan erőfeszítés lenne az érintettek tájékoztatása.

Amennyiben az adatkezelő nem értesítette az érintettet az adatvédelmi incidensről, de miután a felügyeleti hatóság mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását.

Az adatvédelmi incidens után, a feltárt hiányosságokat kiértékelve, az adatkezelő részéről indokolt lehet a belső folyamatok felülvizsgálata, további szűrők, ellenőrzések beiktatása a munkafolyamatba, illetve a munkatársak adatvédelmi tudatosságának növelése.

7. Az adatvédelmi incidensek nyilvántartása

Az adatvédelmi nyilvántartás a NAIH által ajánlott és kitöltött bejelentő lapok alapján, azok iktatásával és elektronikus másolatának tárolásával valósul meg, mely – a teljes felsorolás nélkül – az alábbiakat tartalmazza:

- az incidens jellege, az adatvédelmi incidenshez kapcsolódó tények, annak hatásai,
- érintettek kategóriái és száma,
- adatok kategóriái és száma,
- valószínűsíthető következmények,
- az incidens következményei elhárítására, következmények enyhítésére tett és tervezett intézkedések.

Az adatvédelmi incidensek nyilvántartását az adatvédelmi tisztviselő/felelős vezeti elektronikus dokumentumban, excel táblázatban.

A nyilvántartás része az incidenssel kapcsolatos vizsgálódás dokumentumának elektronikus másolata.

Az incidens vizsgálatát és kezelését – a NAIH honlapjáról letölthető – papíralapú incidens-bejelentő lap kitöltésével kell dokumentálni.