ADATVÉDELMI INCIDENSEK KEZELÉSÉNEK ÉS BEJELENTÉSÉNEK SZABÁLYZATA

		Aláírás:
Jóváhagyta:	Börzsei Tibor Vince vezérigazgató	
Felelős:	dr. Fullajtár Gergely jogi igazgató	
Készítette:	dr. Fullajtár Gergely jogi igazgató	
Jogi megfelelőséget ellenőrizte:	dr. Fullajtár Gergely jogi igazgató	
Összhangvizsgálatot elvégezte:	Sebestény Enikő folyamatszabályozási és ellenőrzési osztályvezető	

TARTALOMJEGYZÉK

1. Általános rendelkezések 3
1.1 A szabályozás célja 3
1.2 Személyi hatály 3
1.3 Tárgyi hatály 3
2. Adatvédelmi incidensek esetkörei, tudomásszerzés és az előzetes vizsgálat 3
2.1 Adatvédelmi incidensek esetkörei, tudomásszerzés 3
2.2 Előzetes vizsgálat 5
3. Az adatvédelmi incidens bejelentésének mellőzése 5
4. Adatkezelés felfüggesztése adatvédelmi incidens esetén 6
5. Az adatvédelmi incidens kivizsgálása 6
6. Érintettek tájékoztatása 7
7. Az incidensjelentés és az incidens-nyilvántartás 8
8. Kapcsolódó szabályozások 8
9. Mellékletek 8

1. Általános rendelkezések

1.1 A szabályozás célja

Jelen szabályozás célja, hogy gyakorlati útmutatót nyújtson a NÚSZ Zrt. azon munkatársainak, akiket 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" vagy „GDPR") előírásai alapján a személyes adatok kezelése során felmerülő incidens esetén az incidens orvoslásával és a GDPR által előírt bejelentésével, dokumentálásával kapcsolatosan valamely kötelezettség terhel. Adatvédelmi incidens alatt értjük, az adatbiztonság olyan sérülését, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

1.2 Személyi hatály

Jelen szabályzat kiterjed a NÚSZ Zrt. Információbiztonsági Osztályának, Service Desk Osztályának személyes adatkezelésben érintett munkatársaira, az adatvédelmi tisztviselőre és mindazokra a NÚSZ munkavállalókra, akiknek munkáját, kötelezettségeit és felelősségét közvetlenül vagy közvetve érinti az adatvédelmi incidens.

1.3 Tárgyi hatály

Jelen szabályzat előírásai alkalmazandók az adatvédelmi incidens észlelése, bejelentése, kivizsgálása, elhárítása, dokumentálása és ezzel kapcsolatosan szükség esetén az érintettek tájékoztatása vonatkozásában.

2. Adatvédelmi incidensek esetkörei, tudomásszerzés és az előzetes vizsgálat

2.1 Adatvédelmi incidensek esetkörei, tudomásszerzés

Adatvédelmi incidens a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

A Nemzeti Útdíjfizetési Szolgáltató Zrt. (továbbiakban NÚSZ Zrt.) esetében adatvédelmi incidens különösen:

a) a személyes adatokat tároló szerver feltörése,
b) a személyes adatok jogosulatlan titkosítása, amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy a NÚSZ Zrt. adatkezelései során felhasználni,
c) ha a NÚSZ Zrt. valamely munkavállalója jogosulatlanul hozzáfér személyes adatokhoz, vagy a jogosultsági szintjét meghaladóan fér hozzá a személyes adatokhoz, vagy a munkavállaló által jogosulatlanul végrehajtott adatkezelési művelet (például a személyes adatokat tartalmazó adatbázis kimentése külső adathordozóra),

d) személyes adatok vétlen vagy szándékos, felhatalmazás nélküli nyilvánosságra hozatala,
e) személyes adatokat tartalmazó dokumentum más számára történő hozzáférhetővé tétele,
f) személyes adatokat tartalmazó postai küldemény téves címzetthez történő elpostázása,
g) személyes adatokat tartalmazó e-mail téves címzettnek történő kiküldése,
h) személyes adatokat tartalmazó adathordozó vagy informatikai eszköz elvesztése,
i) a személyes adatokat tároló informatikai eszköz vagy az ilyen adatokat tartalmazó dokumentumok sérülése, megsemmisülése (ideértve a tűzesetet vagy a vízkár által okozott sérülést vagy megsemmisülést), amelynek következtében a személyes adatokhoz - akár átmenetileg - nem lehet hozzáférni vagy a NÚSZ Zrt. adatkezelései során felhasználni.

Tudomásszerzésnek minősül az, ha

a) az adatvédelmi incidensre bekövetkezésre utaló körülményt a NÚSZ Zrt. munkavállaló fedezi fel,
b) a NÚSZ Zrt.- nek e-mailen, postai levélben vagy más kommunikációs eszköz útján küldött üzenet, amely adatvédelmi incidens bekövetkezésre utaló körülményt tartalmaz (abban az esetben is, ha az üzenet névtelen),
c) a NÚSZ Zrt.-t telefonon keresztül adatvédelmi incidens bekövetkezésre utaló körülményről értesítik (abban az esetben is, ha a hívó fél ismeretlen vagy névtelen),
d) a sajtóban vagy más honlapon megjelent, adatvédelmi incidens bekövetkezésre utaló körülmény, amelyről a NÚSZ Zrt. értesül vagy arról értesítik
e) az adatfeldolgozó értesíti a cégnevet az adatvédelmi incidens bekövetkezéséről.

Amennyiben egy eseményről a tudomásszerzés időpontjában nem lehet eldönteni, hogy adatvédelmi incidensnek tekinthető-e, akkor haladéktalanul előzetes vizsgálatot kell indítani annak tisztázása érdekében, hogy az esemény megfeleltethető-e a szabályzatban szereplő fogalomnak. Az előzetes vizsgálat célja, hogy meg lehessen állapítani,

a) az adott esemény személyes adatokkal összefüggésben következett be,
b) ki lehet-e zárni annak lehetőségét, hogy az adott esemény személyes adatokat érintett.

Amennyiben az esemény személyes adatokkal összefüggésben következett be, vagy nem lehet kizárni annak lehetőségét, hogy az adott esemény személyes adatokat érintett, akkor az esemény adatvédelmi incidensnek minősül.

2.2 Előzetes vizsgálat

Amennyiben az előzetes vizsgálat alapján egyértelműen megállapítható, hogy az adott esemény nem érintett személyes adatokat, akkor az eseményt nem kell adatvédelmi incidensként kezelni. Ebben az esetben is az előzetes vizsgálatban fel kell térképezni, hogy

a) mi volt az adott esemény oka,
b) miért nem következett be adatvédelmi incidenst, illetve
c) - amennyiben az adott esemény kapcsán értelmezhető - hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló esemény.

Az előzetes vizsgálat lefolytatása az Adatvédelmi tisztviselő feladata. Távolléte esetén az előzetes vizsgálatot a vezérigazgató által kijelölt személy végzi. Informatikai eszközzel összefüggő incidens esetén az előzetes vizsgálatban az Adatvédelmi tisztviselő köteles kikérni az információbiztonsági osztályvezető véleményét. Távolléte esetén a műszaki igazgató jelöli ki azt a személyt, akinek a kivizsgálásban közreműködnie kell.

Az Adatvédelmi tisztviselő az előzetes vizsgálat megállapításait írásba kell foglalnia, kitérve abban a 2.2. pontban szereplő körülményekre, és - amennyiben szükséges - intézkedési tervet kell készíteni. A szükséges intézkedések meghozataláról és bevezetéséről a vezérigazgató dönt.

3. Az adatvédelmi incidens bejelentésének mellőzése

Abban az esetben, ha bizonyítottan adatvédelmi incidens történt, azonban az arról történő tudomásszerzés időpontjában vagy az előzetes vizsgálat alapján megállapítható, hogy az incidensnek valószínűsíthetően nincs kockázata az érintettekre nézve, akkor az incidensről nem kell bejelentést tenni a NAIH-nak.

Ilyen adatvédelmi incidensnek tekinthető különösen az, ha a személyes adatokat tartalmazó, az érintett téves lakcímére küldött postai küldemény felbontás nélkül visszaérkezik a NÚSZ Zrt.-hez.

Az adatvédelmi incidens bejelentésének mellőzéséről az Adatvédelmi tisztviselő javaslata alapján a vezérigazgató dönt. A javaslatban ki kell térni arra, hogy

a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
b) miért nem következett be az érintettekre nézve kockázatot jelentő adatvédelmi incidens,
c) - amennyiben az adott adatvédelmi incidens kapcsán értelmezhető - hogyan lehet megelőzni azt, hogy a jövőben ne következzen be hasonló adatvédelmi incidens,
d) miért javasolja azt, hogy erről a NÚSZ Zrt. ne tegyen bejelentést a NAIH-nak.

Amennyiben a vezérigazgató a javaslatot elfogadja, akkor az adatvédelmi incidenst fel kell vezetni az incidens-nyilvántartásba.

4. Adatkezelés felfüggesztése adatvédelmi incidens esetén

Az adatvédelmi incidenst felfedező vagy arról (telefonon, e-mailben, postai úton) tudomást szerző munkavállaló köteles értesítenie az Adatvédelmi tisztviselőt, távolléte esetén a vezérigazgató által kijelöl személyt. A munkavállaló a munkakörének ellátása során igénybe vett informatikai eszközzel összefüggő incidens esetén kötelező értesítenie az információbiztonsági osztályvezetőt, távolléte esetén a műszaki igazgatót.

Adatvédelmi incidensre vonatkozó értesítést követően haladéktalanul fel kell függeszteni azt az adatkezelést, amit az adatvédelmi incidens érintett.

Abban az esetben, ha

a) a rendelkezésre álló információk alapján az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei, vagy
b) a felfüggesztést követően a NÚSZ Zrt. olyan intézkedéseket hozott, amelyek biztosítják, hogy az adatvédelmi incidensnek nincsenek és nem is várhatóak súlyos következményei

a felfüggesztés megszüntethető.

A felfüggesztés megszüntetéséről az Adatvédelmi tisztviselő írásbeli javaslatára a vezérigazgató dönt. A javaslatban ki kell térni arra, hogy

a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
b) miért javasolja a felfüggesztés megszüntetését.

5. Az adatvédelmi incidens kivizsgálása

Az adatvédelmi incidenst az Adatvédelmi tisztviselőnek a tudomásszerzést vagy az előzetes vizsgálat lezárultát követő 72 órán belül be kell jelentenie a NAIH honlapján, függetlenül attól, hogy mennyi információ áll a NÚSZ Zrt. rendelkezésére az adatvédelmi incidenssel összefüggésben.

Az adatkezelés felfüggesztését követően haladéktalanul meg kell kezdeni az adatvédelmi incidens kivizsgálását. A kivizsgálás során az alábbi körülményeket kell tisztázni:

a) az adatvédelmi incidens bekövetkezése előtt alkalmazott intézkedések,
b) az adatvédelmi incidens okát (valószínűsíthető okát),
c) az adatvédelmi incidenssel érintett személyes adatok típusa és mennyisége (legalább becsléssel),
d) az érintettek száma (legalább becsléssel),
e) az érintettek kategóriái, így különösen, hogy az adatvédelmi incidensben van-e sérülékeny érintetti kör (például gyerekek, idős emberek, vagy más ország állampolgárai),
f) mennyire egyszerű az érintettek azonosítása azon adatkör alapján, amelyet az adatvédelmi incidens érintett,

g) az adatvédelmi incidens lehetséges vagy már megtörtént következményei, illetve azok súlyossága az érintettekre nézve,
h) szükséges-e az érintetteket tájékoztatni az adatvédelmi incidensről, és amennyiben nem, akkor ennek indoka.

Az adatvédelmi incidens kivizsgálása az Adatvédelmi tisztviselő feladata. Távolléte esetén a kivizsgálást a vezérigazgató által kijelölt személy végzi. Informatikai eszközzel összefüggő incidens esetén a kivizsgálásban köteles az információbiztonsági osztályvezetővel egyeztetnie. Távolléte esetén a műszaki igazgató jelöli ki azt a személyt, akinek a kivizsgálásban közreműködnie kell.

Amennyiben a kivizsgálás függetlensége vagy hatékonysága a NÚSZ Zrt.-n belül nem biztosítható, akkor az adatvédelmi incidens kivizsgálásával külső szakértőt kell megbízni.

Az adatvédelmi incidens kivizsgálása során feltárt új körülményeket az Adatvédelmi tisztviselő haladéktalanul köteles bejelenteni a NAIH-nak.

6. Érintettek tájékoztatása

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettekre nézve, a NÚSZ Zrt.-nek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről.

Az adatvédelmi incidens magas kockázattal jár, és az érintetteket tájékoztatni kell, ha az incidens az alábbi adatkategóriák egyikére vonatkozik:

a) a különleges adatok,
b) az érintett pénzügyi helyzetére vonatkozó adatok (például tartozás),
c) az érintett társadalmi megbecsülésére kiható adatok (például rossz iskolai eredmények),
d) felhasználónév, jelszó,
e) a személyiséglopásra alkalmas adatok (például okmánymásolat).

Az érintetteknek adott tájékoztatóban ismertetni kell

a) az adatvédelmi incidens jellegét,
b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
c) ismertetni kell az adatvédelmi incidens lehetséges vagy már megtörtént következményeit, illetve azok súlyosságát az érintettekre nézve,
d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az előzetes tájékoztatást az érintettek e-mail címére kell elküldeni. Ha nem áll rendelkezésre az érintettek e-mail címe, akkor a postai elérhetőségükre kell továbbítani a tájékoztatást. Amennyiben van olyan érintett, akit nem lehet az adatvédelmi incidensről tájékoztatni, holott az vagy az érintettek tájékoztatása aránytalan erőfeszítést tenne szükségessé, akkor a honlapon közlemény helyezhető el.

Az előzetes tájékoztatás mellőzhető, ha

a) a NÚSZ Zrt. megfelelő adatbiztonsági intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, így különösen olyan intézkedések jöhetnek szóba, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat (például titkosítás alkalmazása),
b) az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az adatvédelmi incidens valószínűsíthetően nem jár magas kockázattal az érintettekre nézve.

Az érintettek előzetes tájékoztatásának mellőzéséről az Adatvédelmi tisztviselő javaslata alapján a vezérigazgató dönt. A javaslatban ki kell térni arra, hogy

a) milyen adatvédelmi incidens történt (a személyes adatok típusa, mennyisége, érintettek száma, kategóriái, milyen következményei voltak vagy lehettek volna az érintettre),
b) miért javasolja azt, hogy a NÚSZ Zrt. ne tájékoztassa az érintetteket az adatvédelmi incidensről.

7. Az incidensjelentés és az incidens-nyilvántartás

Az adatvédelmi incidens kivizsgálását írásban kell rögzíteni (incidensjelentés). Az incidensjelentésben az Adatvédelmi tisztviselőnek - az információbiztonsági osztályvezetővel egyetértésben - javaslatot kell tenni az adatvédelmi incidens orvoslására és az okainak megszüntetésére. A szükséges intézkedések meghozataláról és bevezetéséről a vezérigazgató dönt.

A NÚSZ Zrt-nél történt valamennyi adatvédelmi incidensről az 1. számú melléklet szerinti nyilvántartást kell vezetni, függetlenül attól, hogy a NAIH-nak kellett-e bejelentést tenni vagy sem.

Az incidens-nyilvántartást adatvédelmi incidensenként külön-külön kell vezetni, úgy, hogy annak alapján a NAIH ellenőrizhesse az irányadó jognak való megfelelést.

8. Kapcsolódó szabályozások

- információ biztonsággal kapcsolatos szabályozó elemek
- Adatvédelmi szabályzat

9. Mellékletek

1. sz. melléklet: Adatvédelmi incidens nyilvántartás