ADATVÉDELMI INCIDENSEK BEJELENTÉSÉNEK ÉS KEZELÉSÉNEK SZABÁLYZATA

Aláírás:

Jóváhagyta:	Dr. Bartal Tamás vezérigazgató	
Készítésért felelős:	Dr. Mórocz Aliz jogi igazgató	
Megfelelősségi vizsgálatot elvégezte:	Dr. Lemesánszky Zoltán megfelelést támogató csoportvezető	
Jogi megfelelőséget ellenőrizte:	Dr. Mórocz Aliz jogi igazgató	
Összhangvizsgálatot elvégezte:	Sebestény Enikő folyamatszabályozási osztályvezető	
Készítette:	dr. Strich-Szekeres Krisztina jogtanácsos	

Hatálybalépés dátuma: 2021.09.07.

TARTALOMJEGYZÉK

1. Általános rendelkezések

1.1 A szabályozás célja

Jelen szabályozás célja, hogy gyakorlati útmutatóul szolgáljon a Nemzeti Útdíjfizetési Szolgáltató Zrt. (a továbbiakban: NÚSZ, vagy Társaság) által végzett személyes adatkezelések során bekövetkező incidensek (adatvédelmi incidensek) esetére a NÚSZ munkatársainak annak érdekében, hogy az incidensek bejelentésére és kezelésére 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”) előírásainak megfelelően, gyorsan és hatékonyan kerüljön sor.

1.2 Személyi hatály

Jelen szabályzat kiterjed mindazokra a NÚSZ munkavállalókra (ide értve a NÚSZ munkavégzésre irányuló egyéb jogviszonyban álló személyeket is), akiket munkavégzésük során, illetve azzal összefüggésben közvetlenül vagy közvetve érint az adatvédelmi incidens.

1.3 Tárgyi hatály

Jelen szabályzat előírásai alkalmazandók az adatvédelmi incidens észlelése, jelentése, kivizsgálása, hatósági bejelentése, elhárítása, dokumentálása és ezzel kapcsolatosan szükség esetén az érintettek tájékoztatása vonatkozásában. Az adatvédelmi incidensek bejelentésének és kezelésének folyamatát az 1. sz. mellékletet képező folyamatábra mutatja be.

2. Adatvédelmi incidensek esetkörei, tudomásszerzés, vizsgálat és nyilvántartás

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 NÚSZ 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 adatkezelései során felhasználni,
c) ha a NÚSZ 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, elhagyása, feltörése, adatlopás,
i) személyes adatokat tartalmazó mobil telekommunikációs eszköz (pl. mobiltelefon) elvesztése, elhagyása, feltörése, adatlopás,
j) 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 adatkezelései során felhasználni.

Tudomásszerzésnek minősül az, ha:

a) az adatvédelmi incidens bekövetkezésére utaló körülményt a NÚSZ munkavállalója fedezi fel,
b) a NÚSZ-nak 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-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 értesül vagy arról értesítik,
e) az adatfeldolgozó értesíti a NÚSZ-t az adatvédelmi incidens bekövetkezéséről.

2.2 Előzetes vizsgálat

Az incidens bekövetkezésére utaló körülményeket haladéktalanul meg kell vizsgálni annak megállapítása érdekében, hogy történt-e adatvédelmi incidens.

Az adatvédelmi incidens-gyanús eset előzetes vizsgálatának kezdeményezése az esetet észlelő munkatárs feladata. A munkatárs az észlelést követően haladéktalanul e-mailben értesíti közvetlen felettesét és a dpo@nemzetiutdij.hu email címen a Társaság adatvédelmi tisztviselőjét az adatvédelmi incidens gyanúját felvető esetről.

Az eset előzetes kivizsgálását az adatvédelmi tisztviselő – távolléte esetén az adatvédelmi tisztviselő helyettesítésére kijelölt munkavállaló - végzi, aki ennek során tisztázó kérdéseket tehet fel. A kérdésekre az érintett munkatárs vagy közvetlen felettese a lehető legrövidebb – legfeljebb 48 órás – időtartamon belül válaszolni köteles.

Mobil telekommunikációs eszközt érintő incidens-gyanús esemény kapcsán a munkavállaló a Mobil telekommunikációs eszközök igénybevételéről szóló szabályzat rendkívüli esemény bejelentésével kapcsolatos előírásainak megfelelően köteles eljárni.

Az IT eszközök elvesztése, eltulajdonítása esetén az IT eszközök és szolgáltatások igénylési és használati rendje tárgyú vezérigazgatói utasítás „Feljegyzés IT eszközzel kapcsolatos lehetséges adatvédelmi incidens esetén" elnevezésű kitöltött mellékletét kell megküldeni az adatvédelmi tisztviselő részére a jelen szabályzat rendelkezéseinek megfelelően.

a) Nem történt adatvédelmi incidens

Amennyiben az előzetes vizsgálat alapján egyértelműen megállapítható, hogy az adott esemény nem minősül adatvédelmi incidensnek, úgy erről az adatvédelmi tisztviselő egy munkanapon belül válasz emailben tájékoztatja a részére az esetről szóló jelzést megküldő munkatársat és a munkatárs közvetlen felettesét. Az adatvédelmi tisztviselő e tájékoztatásban megindokolja, miért nem tekinthető adatvédelmi incidensnek az esemény és – amennyiben az az eset jellegére tekintettel adatvédelmi szempontból indokolt lehet – javaslatot tesz a hasonló események bekövetkeztének elkerülése, illetve kockázatának mérséklése érdekében.

b) Adatvédelmi incidens történt

Az adatvédelmi tisztviselőnek az előzetes vizsgálat megállapításait írásba kell foglalnia, és - amennyiben szükséges - intézkedési javaslatot kell tennie. Az adatvédelmi tisztviselő a vizsgálat megállapításait és az esetleges intézkedési javaslato(ka)t feljegyzés (a továbbiakban: „incidensjelentés") formájában rögzíti, majd a Társaság vezérigazgatója elé terjeszti. Vezérigazgatói jóváhagyás esetén a szükséges intézkedések bevezetéséről és végrehajtásáról az érintett szakterület vezetője gondoskodik az adatvédelmi tisztviselő visszajelzése – így például a vezérigazgató által jóváhagyólag aláírt feljegyzés megküldése – alapján.

Abban az esetben, ha a vezérigazgató nem ért egyet a vizsgálat megállapításaival vagy a javasolt intézkedésekkel, a feljegyzésen utal a jóváhagyás hiányára, illetve a véleményeltérésre, egyidejű írásbeli indokolással.

c) Információbiztonsági sérelem gyanúja

Amennyiben felmerül az információbiztonság sérelmének gyanúja, az adatvédelmi tisztviselő az előzetes vizsgálatban köteles kikérni az információbiztonsági osztályvezető véleményét emailben, akinek távolléte esetén a műszaki igazgató jelöli ki a vizsgálatban közreműködő munkatársat. Az információbiztonsági osztályvezető (vagy más kijelölt munkatárs) az adatvédelmi tisztviselő emailjére 24 órán belül válaszol.

Amennyiben az információbiztonság sérelme megállapítható, az információbiztosági osztályvezető annak orvoslása iránt a szükséges intézkedéseket késedelem nélkül megteszi.

Abban az esetben, ha az információbiztonság sérelme mellett adatvédelmi incidens kerül megállapításra, az incidensjelentésben is utalni kell az információbiztonság sérelmére és a sérelem orvoslása érdekében tett (teendő) intézkedésekre.

2.3 Vizsgálat

2.3.1. Kockázattal nem járó adatvédelmi incidensek kezelése

Abban az esetben, ha az előzetes vizsgálat eredményeképpen az eset adatvédelmi incidensnek minősül, azonban megállapítható, hogy az incidensnek valószínűsíthetően nincs kockázata az érintettekre nézve, akkor az incidensről nem kell bejelentést tenni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (a továbbiakban: „NAIH).

Ilyen adatvédelmi incidensnek tekinthető különösen, ha a személyes adatokat tartalmazó, téves lakcímre küldött postai küldemény felbontás nélkül visszaérkezik a NÚSZ-hoz.

Az adatvédelmi incidens bejelentésének mellőzéséről az adatvédelmi tisztviselő által az incidensjelentésben tett javaslat alapján a vezérigazgató dönt. A javaslatban az adatvédelmi tisztviselőnek ki kell térnie 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) hogyan lehet megelőzni azt, hogy a jövőben bekövetkezzen hasonló adatvédelmi incidens (amennyiben az adott adatvédelmi incidens kapcsán ez értelmezhető),
d) miért javasolja azt, hogy erről a NÚSZ ne tegyen bejelentést a NAIH-nak.

Amennyiben a vezérigazgató a javaslatot elfogadja, az adatvédelmi tisztviselő felvezeti az adatvédelmi incidenst az incidens-nyilvántartásba.

Abban az esetben, ha a vezérigazgató a javaslatot nem fogadja el, a bejelentés szükségességére vonatkozó véleményeltérését és annak indokát a feljegyzésen rögzíti. Ekkor az adatvédelmi tisztviselő az 2.3.2. b) pontban foglaltak szerint jár el.

2.3.2. Kockázattal járó adatvédelmi incidensek kezelése

Az adatvédelmi incidens kockázatosnak tekinthető abban az esetben, ha az valószínűsíthető kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

a) Az adatkezelés felfüggesztése

Ha a rendelkezésre álló információk alapján az adatvédelmi incidensnek súlyos következményei vannak vagy ilyen következményekkel kell számolni, az adatvédelmi incidenssel érintett adatkezelést haladéktalanul fel kell függeszteni.

Az incidensjelentésben utalni kell a felfüggesztés tényére vagy annak mellőzésére - indokolással.

A felfüggesztés megszüntethető, ha a meghozott és végrehajtott intézkedési javaslatnak megfelelően tett intézkedések következtében a súlyos következmények elhárultak.

A felfüggesztés megszüntetéséről az adatvédelmi tisztviselő – feljegyzés formájában rögzített – írásbeli javaslatára a vezérigazgató dönt.

b) Az adatvédelmi incidens bejelentése és további vizsgálata

A kockázattal járó incidenst az adatvédelmi tisztviselő köteles a tudomásszerzést követő 72 órán belül bejelenteni a NAIH részére, függetlenül attól, hogy azzal kapcsolatban mennyi információ áll a NÚSZ rendelkezésére. Ha a bejelentés nem történik meg 72 órán belül, a bejelentésben elő kell adni a késedelem igazolására szolgáló indokokat is.

Amennyiben sor kerül az adatkezelés felfüggesztésére mint azonnali intézkedésre, ezt követően haladéktalanul meg kell kezdeni az adatvédelmi incidens további kivizsgálását. A további kivizsgálás során az alábbi körülményeket kell tisztázni (amennyiben azok az előzetes vizsgálat során nem vagy nem kellő mértékben lettek tisztázva):

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 további kivizsgálása az adatvédelmi tisztviselő feladata. Távolléte esetén a kivizsgálást az adatvédelmi tisztviselő helyettesítésére kijelölt munkavállaló végzi. Az adatvédelmi tisztviselő ennek során az érintett szakterület vezetőjének vagy az általa kijelölt munkatársnak, illetve - információbiztonsági vonatkozás esetén - az információbiztonsági osztályvezetőnek (távolléte esetén a műszaki igazgató által kijelölt munkatársnak) kérdéseket tehet fel, melyek megválaszolására a címzettek a lehető legrövidebb - legfeljebb egy munkanapos – időtartamon belül kötelesek.

Amennyiben a kivizsgálás függetlensége vagy hatékonysága a NÚSZ-on 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.

2.3.3. Magas kockázattal járó incidensek kezelése

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettekre nézve, a NÚSZ adatvédelmi incidenssel érintett szervezeti egységének vezetője által a Társaság Szervezeti és Működési Szabályzatában és Kötelezettségvállalási Szabályzatban foglaltakkal összhangban kijelölt munkavállaló(k) indokolatlan késedelem nélkül tájékoztatnia/tájékoztatniuk kell az érintettet az adatvédelmi incidensről. Az adatvédelmi tisztviselő jelzi az érintettek tájékoztatásának szükségességét az adatvédelmi incidenssel

érintett szervezeti egység vezetője részére, egyúttal felkéri a tájékoztatást közlő munkavállaló(k) azonnali kijelölésére és a tájékoztatás haladéktalan megtételére. A tájékoztatás szövegét szükség esetén az adatvédelmi tisztviselővel előzetesen egyeztetni kell.

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

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 szóló tájékoztatóban ismertetni kell:

a) az adatvédelmi incidens jellegét,
b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
c) 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.

A 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, vagy az érintettek tájékoztatása aránytalan erőfeszítést tenne szükségessé, akkor a honlapon közlemény helyezhető el.

A tájékoztatás mellőzhető, ha:

a) a NÚSZ 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 tájékoztatásának mellőzéséről az adatvédelmi tisztviselő feljegyzés formájában tett 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 ne tájékoztassa az érintetteket az adatvédelmi incidensről.

Abban az esetben, ha a vezérigazgató a javaslatot nem fogadja el, az érintettek tájékoztatásának szükségességére vonatkozó álláspontját és annak indokolását a feljegyzésen rögzíti. Ekkor az adatvédelmi tisztviselő a jelen pontban foglaltaknak megfelelően intézkedik az érintettek tájékoztatása érdekében.

2.4 Az incidens-nyilvántartás

A NÚSZ-nál történt valamennyi adatvédelmi incidensről nyilvántartást kell vezetni, függetlenül attól, hogy a NAIH-nak kellett-e bejelentést tenni vagy sem. A nyilvántartás vezetéséhez segítséget nyújt a 2. sz. mellékletet képező minta.

3. Záró rendelkezések

Hatályát veszti a 2020. szeptember 15. napján hatályba lépett Adatvédelmi Incidensek Kezelésének és Bejelentésének Szabályzata.

Jelen szabályzat 2021.09.07. napján lép hatályba.

4. Kapcsolódó szabályozások

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”)

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Mobil telekommunikációs eszközök igénybevétele szabályzat

IT eszközök és szolgáltatások igénylési és használati rendje tárgyú vezérigazgatói utasítás

Információbiztonsági Szabályzat

Adatvédelmi Szabályzat

Adatvédelmi szabályzat a munkavállalói személyes adatok kezeléséről

5. Mellékletek

1. sz. melléklet: Adatvédelmi incidensek bejelentése és kezelése (folyamatábra)
2. sz. melléklet: Adatvédelmi incidens nyilvántartás minta