Erste Önkéntes Nyugdíjpénztár

Adatvédelmi Incidens Kezelési Szabályzata

Az Erste Önkéntes Nyugdíjpénztár
adatvédelmi incidens kezelési szabályzata

Az Adatkezelő, az (Erste Önkéntes Nyugdíjpénztár, székhely: 1138 Budapest, Népfürdő utca 24-26.), a tényleges adatkezelés címe: 1138 Budapest, Népfürdő utca 24-26., internetes elérhetősége: www.erstenyugdijpenztar.hu, összhangban az Adatvédelmi és Adatbiztonsági Szabályzattal, megalkotta a jelen adatvédelmi incidens szabályzatát.

I. Fogalommagyarázat

1. A jelen Szabályzatban használt fogalmak tartalma megegyezik az Adatvédelmi és Adatbiztonsági Szabályzatban meghatározott fogalmak tartalmával.

II. A Szabályzat célja

1. A jelen Szabályzat elsődleges célja, hogy a szabályokat hozzon az esetlegesen bekövetkező adatvédelmi incidensek kezelésére, elhárítására, károk enyhítésére, és megelőzésére.

III. A Szabályzat Hatálya

1. Időbeli hatály: Jelen Szabályzat a hatályba léptetés napjától további rendelkezésig vagy visszavonásig hatályos.

2. Személyi hatály kiterjed a Munkatársakra, és mindazon személyekre, akik jogait vagy jogos érdekeit az adatvédelmi incidens érinti.

3. Tárgyi hatály: Jelen Szabályzat hatálya kiterjed az Adatkezelő bármely szervezeti egységében bekövetkezett adatvédelmi incidensre.

IV. Megelőző és felderítő intézkedések

1. Adatkezelő az adatvédelmi incidensek megelőzése és felderítése érdekében a következő technikai és szervezési intézkedéseket tette meg és ezen intézkedések megtételét rendszeresen ellenőrzi:

    a) Adatvédelmi szabályozási rendszert hozott létre és tart naprakészen;
    b) Az Adatvédelmi és Adatkezelési Szabályzatban meghatározta az adatvédelem szervezetét;
    c) Belső adatvédelmi felelőst/adatvédelmi tisztviselőt nevezett ki;
    d) Munkatársakat informálta és folyamatosan informálja, oktatja az adatvédelmi szabályozásról, annak változásáról;
    e) A Munkatársak megismerik és nyilatkozatokban fogadják el az adatvédelmi szabályozási rendszer rendelkezéseit;
    f) Munkatársak a személyes adatokkal kizárólag az adatvédelmi szabályozási rendszerben meghatározott jogosultságok alapján, célból és

módon kerülhetnek kapcsolatban, azokat csak a meghatározott módon kezelhetik;
g) Adatkezelő az adatvédelmi incidensek megelőzése és felderítése céljából az IBSZ-ben meghatározott naplózási rendet vezet be és folyamatosan ellenőriz;
h) Adatkezelő egyéb, az IBSZ-ben meghatározott informatikai eszközök segítségével akadályozza meg az adatok jogellenes kezelését, vagy azokhoz történő jogellenes hozzáférést.

V. Előzetes értékelési minta adatvédelmi incidens esetében

1. Adatkezelő az alábbi értékelési minta alapján végzi el az adatvédelmi incidens értékelését:

2. Az adatvédelmi incidens **jelentős mértékűnek** tekintendő a következő bármely esetben:
   a) adatvédelmi incidenssel érintett adatok köre: **Különleges adat vagy személyes adat;**
   b) adatvédelmi incidenssel érintettek száma: személyes adat esetében 100 vagy ennél több érintett, adatvédelmi incidenssel érintett különleges adat esetében legalább 1 érintett;
   c) azonnali intézkedést igényel;
   d) partner adatát érinti, függetlenül attól, hogy hány partnerről vagy adatról van szó
   e) hatás: jelentős vagy visszafordíthatatlan következmények
   f) jelentős reakciót igényel a normális működésen túl
   g) büntetőjogi következményei lehetnek
   h) az adatvédelmi incidens és/vagy körülménye elektronikus vagy nyomtatott médiában elérhető

3. Az adatvédelmi incidens **közepes** mértékűnek tekintendő a következő esetekben:

   a) adatvédelmi incidenssel érintett adatok köre: **személyes adat**
   b) adatvédelmi incidenssel érintettek száma: 100 érintettnél kevesebb érintett
   c) hatás: közepes, érintettek kényelmetlenségeket tapasztalhatnak
   d) az észlelés napján igényel intézkedést, de azonnali intézkedést nem igényel (függetlenül attól, hogy az intézkedés az észlelést követően azonnal megtörténik)
   e) büntetőjogi következmény nem merülhet fel, de más jogi következmény felmerülhet (pl. polgári jogi)

4. Az adatvédelmi incidens **jelentéktelen** mértékűnek tekintendő a következő esetekben:

   a) adatvédelmi incidenssel érintett adatok köre: **olyan adat, amely segítségével nem azonosítható be érintett**
   b) adatvédelmi incidenssel érintettek száma: nem értelmezhető, mert érintett nem beazonosítható
   c) hatás: minimális (pl.: informatikai leállás tapasztalható)

d) az adatok visszaállítása egyszerűen kivitelezhető

VI. Munkatársak kötelezettségei az adatvédelmi incidenssel kapcsolatban

1. Adatvédelmi incidenssel kapcsolatban a Munkatársak kötelezettségei az alábbiakben meghatározottak, függetlenül attól, hogy a Munkatárs az adatvédelmi incidenst mekkora mértékűnek is gondolja: Munkatárs köteles az észlelését követően azonnal, késedelem nélkül

    a) értesíteni az adatvédelmi incidensről vagy feltételezett adatvédelmi incidensről valamint a körülményekről az adatvédelmi szervezet szerinti vezetőjét és a belső adatvédelmi felelőst/adatvédelmi tisztviselőt;
    b) feljegyezni a körülményeket, így
        a. az észlelés napját és időpontját, valamint, ha megállapítható
        b. a (feltételezett) adatvédelmi incidens bekövetkezésének napját és időpontját;
        c. azoknak a személyes adatoknak a körét, amelyet az adatvédelmi incidens érint;
        d. a jogsértés okát és terjedelmét, valamint az érintett adatok és a jogsértés közötti összefüggést

2. A vezető az értesítést követően, azonnal, késedelem nélkül köteles

    a) értesíteni a belső adatvédelmi felelőst/adatvédelmi tisztviselőt, ha az ő értesítése valamely okból elmaradt;
    b) megtenni minden intézkedést a (feltételezett) adatvédelmi incidens (jogsértés) megszüntetése és a kárenyhítés érdekében, és
    c) e megtett intézkedésekről, továbbá az intézkedések kimeneteléről, hatásairól, beleértve azt az álláspontot és annak alapját is kifejtve, hogy van-e további intézkedésre szükség, valamint az intézkedések megtételének dokumentálásának megtörténtéről, annak elküldésével értesíteni a belső adatvédelmi felelőst/adatvédelmi tisztviselőt.

3. A belső adatvédelmi felelős/adatvédelmi tisztviselő az értesítést követően, azonnal, késedelem nélkül köteles

    a) felülvizsgálni a már megtett intézkedéseket, azokról és hatásaikról további részletes tájékoztatást kérni;
    b) megtenni minden további intézkedést a (feltételezett) adatvédelmi incidens megszüntetése és kárenyhítés érdekében, szükség esetén, példálózó felsorolással élve Munkatársak jogosultságait átmenetileg megvonni vagy módosítani, jelszavakat módosítani, adathordozókat zárolni, elérhetetlenné tenni, kommunikációs csatornákat lezárni;
    c) elvégezni az adatvédelmi incidens értékelését:
        a. felmérni az adatvédelmi incidenssel érintett adatok számát;
        b. felmérni az adatvédelmi incidenssel érintett érintettek körét és számát;
        c. felmérni az adatvédelmi incidens hatásait az érintettekre és az Adatkezelőre nézve;
        d. az értékelésről írásos összefoglalást készíteni;

d) amennyiben az adatvédelmi incidens **közepes vagy jelentős** mértékű, tájékoztatni az érintetteket az adatvédelmi incidens körülményeiről, hatásairól, elhárítására tett intézkedésekről, megelőző intézkedésekről;
e) az újabb adatvédelmi incidens bekövetkezésének megelőzése céljából intézkedéseket, valamint, ha szükséges, javaslatokat is tenni az Adatkezelő mindenkori vezetője felé;
f) amennyiben szükséges, egyéb informatikai vonatkozású intézkedéseket tenni az adatvédelmi incidens körülményeire tekintettel, példálózó felsorolással élve adatmentést, adat visszaállítást végezni;
g) amennyiben a jogszabályi feltételek fennállnak, a feljelentés alapjául szolgáló dokumentációt összeállítani és a feljelentést megfogalmazni;
h) a fentiekről és minden egyéb körülményről jelentést létrehozni és megküldeni az Adatkezelő mindenkori vezetője számára;
i) a belső nyilvántartást vezetni az adatvédelmi incidensről.

4. A belső adatvédelmi felelős/adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

5. A belső adatvédelmi felelős/adatvédelmi tisztviselő az adatvédelmi incidens nyilvántartást az I. sz. melléklet mintáját felhasználva vezeti.

6. Az Adatkezelő mindenkori vezetője köteles

a) megismerni az adatvédelmi incidens minden körülményét (a számára tett jelentést);
b) informálódni az adatvédelmi incidensről, amennyiben annak minden körülménye számára nem érthető;
c) azonnal elrendelni minden olyan intézkedést, amelyet a belső adatvédelmi felelős/adatvédelmi tisztviselő nem rendelhet el, de az intézkedés a kárenyhítést vagy a jövőbeni újabb adatvédelmi incidens megelőzését szolgálja;
d) amennyiben a jogszabályi feltételek fennállnak, feljelentést tenni az illetékes rendőrkapitányságon/hatóságnál.

VII. Adatvédelmi incidenssel kapcsolatos rendelkezések 2018. május hó 25. napját követően

1. A Szabályzat előző fejezeteiben meghatározott rendelkezéseket kell alkalmazni 2018. május hó 25. napját követően az adatvédelmi incidensek kezelésekor a következő módosító rendelkezések betartásával:

2. A személyes adat, valamint az adatvédelmi incidens fogalmára az 1. fejezetben külön a 2018. május hó 25. napján hatályba lépő definíciókat kell használni.

3. Adatkezelő az Előzetes értékelési minta c. fejezet (V. fejezet) teljes szövegét hatályon kívül helyezi 2018. május hó 25 napjával és helyette a következőket lépteti hatályba e naptól:

Előzetes értékelési minta adatvédelmi incidens esetében

1. Adatvédelmi tisztviselő a lenti linken elérhető értékelési sémát köteles használni a következő megjegyzéssel:

2. Az adatvédelmi incidens súlyossága értékelésének fő kritériumai a következők:
   a) Az **Adatkezelési Környezet (AK) és annak vizsgálata**
   b) Az **Azonosíthatóság Mértékének** (**AM**) meghatározása: azt tárja fel, hogy az adatvédelmi incidenssel érintett adatokból mennyire könnyen lehet az érintettek azonosítását elvégezni
   c) A **Sérülés Körülményeinek (SK**) leírása: a sérülés körülményeit vizsgálja, elsősorban a megsérült adat biztonságának csökkenését, illetve a rosszindulatú támadásra és a szándékosságra utaló valamennyi jelet

3. Az értékelési séma segítséget nyújt az adatvédelmi incidensben érintett adatok típusának meghatározásában (egyszerű adat, pénzügyi adat, viselkedésre vonatkozó adat, érzékeny adat), az eset körülményeinek feltérképezésében (a veszélyességet csökkentő, illetve növelő faktorok), és végül a veszély súlyosságának (VS) objektív mérők szerinti megállapításában.

4. A séma képlete: **VS = AK x AM + SK**

5. A vizsgálat eredményeként az adatvédelmi incidens súlyosságának alacsony, közepes, magas vagy nagyon magas fokozatát állapíthatja meg az adatvédelmi tisztviselő.

6. Amennyiben a Nemzeti Adatvédelmi és Információszabadság Hatóság létrehozta saját értékelési módszertanát, azt kell megfelelően alkalmazni.

7. A módszertan elérhetősége: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn-severity/at_download/fullReport

4. Adatkezelő (adatvédelmi tisztviselőjének feladatvégzésén keresztül) indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles a Nemzeti Adatvédelmi és Információszabadság Hatóság számára, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

5. Tekintettel az előző pontból származó kötelezettségre, az adatvédelmi tisztviselő az értékelést, mint hatásvizsgálatot az észlelést követően késedelem nélkül, haladéktalanul elvégezni, és az eredményről tájékoztatni köteles az Adatkezelő mindenkori vezetőjét.

6. Amennyiben a hatásvizsgálat alapján az adatvédelmi incidens a hatóság felé be kell jelenteni, úgy az adatvédelmi tisztviselő előkészíti és az Adatkezelő mindenkori vezetője számára megküldi a bejelentést.

7. Adatkezelő a bejelentésben köteles

    a) ismertetni az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
    b) közölni az adatvédelmi tisztviselő nevét és elérhetőségeit;
    c) ismertetni az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
    d) ismertetni az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

8. Adatkezelő 2018. május hó 25. napjával következőket lépteti hatályba:

    d) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell a GDPR-ban foglaltnak megfelelő információkat. Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:
        a. Az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
        b. az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg
        c. a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását

9. Adatkezelő a 2. sz. melléklet szerinti minta alapján tesz adatvédelmi incidens bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság felé, kivéve, ha a hatóság az adatvédelmi incidensek bejelentésére szolgáló felületet, és/vagy formanyomtatványt hoz létre, mert ebben az esetben azt használja.

VIII. Záró rendelkezések

1. Jelen Szabályzat rendelkezéseinek ismeretét a Munkatársak a 3. sz. melléklet aláírásával ismerik el.

2. A jelen Szabályzat tartalmára a 2011. évi CXII. törvény, valamint az EU 2016/679. sz. rendelete (GDPR) irányadó elsődlegesen.

3. Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán a hatályos jogszabály a jelen szabályzatban foglalt értelmező rendelkezéstől eltérően határoz meg valamely fogalmat, akkor ezen rendelkezés helyébe minden további rendelkezés nélkül a mindenkor hatályos jogszabályi rendelkezés lép.

4. Amennyiben jelen szabályzat hatálybalépését követően jogszabályváltozás folytán jelen szabályzat valamely rendelkezése a hatályos jogszabályok rendelkezéseivel nem áll többé összhangban, akkor az érintett rendelkezés helyébe minden külön rendelkezés nélkül a hatályos jogszabályi rendelkezés lép.

1. sz. melléklet

Adatvédelmi incidensek nyilvántartása

Adatkezelő: Erste Önkéntes Nyugdíjpénztár
székhely:
adószám:
telefonszám:
e-mail:
fax: -
képviseli:
belső adatvédelmi felelős/adatvédelmi tisztviselő:

Adatvédelmi incidens azonosítására szolgáló jelzés (pl. dátumból képzett azonosítószám):
Az adatvédelmi incidens jellege:
Az adatvédelmi incidenssel kapcsolatban az érintettek kategóriái:
Az adatvédelmi incidenssel érintett érintettek száma:
Az adatvédelmi incidenssel érintett személyes adatok köre:
Az adatvédelmi incidenssel érintett személyes adatok száma:
Incidenshez kapcsolódó tények:
Az adatvédelmi incidens időpontja:
Az adatvédelmi incidens időtartama:
Az adatvédelmi incidens körülményei:
Az adatvédelmi incidenssel érintett egység neve és elérhetőségi adatai:
Az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetését is:
Az adatvédelmi incidens hatásai, következményei:
Az adatvédelmi incidens elhárítására megtett intézkedések:
Az adatkezelést előíró jogszabályban meghatározott egyéb adatok (ha van):
Az adatvédelmi incidensre vonatkozó bejegyzés lezárásának időpontja és az azt lezáró neve, aláírása:

Adatvédelmi incidens azonosítására szolgáló jelzés (pl. dátumból képzett azonosítószám):
Az adatvédelmi incidens jellege:
Az adatvédelmi incidenssel kapcsolatban az érintettek kategóriái:
Az adatvédelmi incidenssel érintett érintettek száma:
Az adatvédelmi incidenssel érintett személyes adatok köre:
Az adatvédelmi incidenssel érintett személyes adatok száma:
Incidenshez kapcsolódó tények:
Az adatvédelmi incidens időpontja:
Az adatvédelmi incidens időtartama:
Az adatvédelmi incidens körülményei:
Az adatvédelmi incidenssel érintett egység neve és elérhetőségi adatai:

Az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetését is:
Az adatvédelmi incidens hatásai, következményei:
Az adatvédelmi incidens elhárítására megtett intézkedések:
Az adatkezelést előíró jogszabályban meghatározott egyéb adatok (ha van):
Az adatvédelmi incidensre vonatkozó bejegyzés lezárásának időpontja és az azt lezáró neve, aláírása:

2. sz. melléklet

Nyilatkozat
az adatvédelmi incidens bejelentéséről az
az EU 2016/679 Rendelet 33. cikk alapján

Címzett:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410
www: http://www.naih.hu
e-mail: ugyfelszolgalat@naih.hu

Alulírott Adatkezelő, a következőkben meghatározott adatvédelmi incidenssel kapcsolatban, az EU 2016/679 Rendeletének 33. cikke alapján az alábbi bejelentést teszem:

1. Adatkezelő neve és azonosító adatai:
   név: Erste Önkéntes Nyugdíjpénztár
   székhely:
   adószám:
   telefonszám:
   e-mail:
   fax: -
   képviseli:
   adatvédelmi tisztviselő:
2. Az adatvédelmi incidens jellegének ismertetése:
3. Az adatvédelmi incidenssel érintett egység neve és elérhetőségi adatai:
4. Az adatvédelmi incidens időpontja:
5. Ha a bejelentés nem történt meg az észlelést követő 72 órán belül, a késedelem igazolására szolgáló indokok:
6. Az érintettek kategóriái és hozzávetőleges száma:
7. Az incidenssel érintett adatok kategóriái és hozzávetőleges száma:
8. Az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetése:
9. Az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések ismertetése:
10. Az adatvédelmi tisztviselő (vagy a további tájékoztatást nyújtó egyéb kapcsolattartó) neve és elérhetősége:

Kelt, ...