FŐVÁROSI ÁLLAT- ÉS NÖVÉNYKERT

ADATVÉDELMI INCIDENS KEZELÉSÉNEK SZABÁLYZATA

Hatályba lépésének napja:

2019. Március 12.

Alkalmazását kötelezően elrendelem:

Prof. Dr. Persányi Miklós főigazgató

TARTALOMJEGYZÉK

1. A szabályzat célja, hatálya

2. Adatvédelmi incidens fogalma

3. Adatvédelmi incidens észlelése, kezelése

4. Az érintettek tájékoztatása adatvédelmi incidensről

5. Adatvédelmi incidensek nyilvántartása

6. Záró rendelkezések

7. Intézkedések a szabályzat megismertetésére

8. Záradék

9. Mellékletek:

- 3 sz. melléklet: Érintettek tájékoztatása adatvédelmi incidensről

- 4 sz. melléklet: Nyilvántartás adatvédelmi incidensről

1. A SZABÁLYZAT CÉLJA, HATÁLYA

A szabályzat célja, hogy meghatározza az Adatfelelősnél, jelen esetben a Fővárosi Állat- és Növénykert-nél, - továbbiakban FÁNK - az adatvédelmi incidens során követendő eljárásrendet, az adatvédelmi incidens kezelését, nyilvántartását.

A szabályzat tárgyi hatálya az adatvédelmi incidensekre terjed ki.

2. ADATVÉDELMI INCIDENS FOGALMA

Adatvédelmi incidens fogalma: 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; (Rendelet 4. cikk 12.)

A leggyakoribb jelentett incidensek lehetnek például: a laptop vagy mobil telefon elvesztése, adatok nem biztonságos továbbítása, partnerlisták illetéktelen másolása, továbbítása, szerver elleni támadások, honlap feltörése. Papíralapon tárolt adatok elvesztése, megsemmisítése.

3. ADATVÉDELMI INCIDENS ÉSZLELÉSE, KEZELÉSE

A FÁNK minden közalkalmazottja – beleértve az egyéb jogviszonyban foglalkoztatott személyeket is – köteles a FÁNK-on belül történt adatvédelmi incidenst haladéktalanul jelenteni a szervezeti egység vezetőjének, az IT vezetőnek, valamint az adatvédelmi tisztviselőnek. A bejelentés tartalmazza a bejelentő nevét, telefonszámát, beosztását, szervezeti egységének megnevezését.

A bejelentés adatvédelmi tisztviselőhöz érkezését követően az adatvédelmi tisztviselő haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését.

Adatvédelmi incidens estén az informatikai csoportvezető és az adatvédelmi tisztségviselő haladéktalanul megvizsgálja a bejelentést, ennek során azonosítani kell az incidenst, el kell dönteni, hogy valódi incidensről, vagy téves riasztásról van szó. Meg kell vizsgálni és meg kell állapítani:

a) az incidens bekövetkezésének helyét és időpontját,

b) az incidens leírását, körülményeit, hatásait,

c) az incidens során érintett adatok körét, számosságát,

d) az incidenssel érintett személyek körét,

e) az incidens elhárítása érdekében megtett intézkedések leírását,

f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

g) az adatvédelmi incidenst az informatikai csoportvezető vagy az adatvédelmi tisztviselő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak a www.naih.hu honlapon keresztül, 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.

(6)A természetes személyek jogait és szabadságait érintő – változó valószínűségű és súlyosságú – kockázatok származhatnak:

A személyes adatok kezeléséből, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek, különösen, ha az adatkezelésből hátrányos megkülönböztetés, személyazonosság-lopás vagy személyazonossággal való visszaélés, pénzügyi veszteség, a jó hírnév sérelme, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése, az álnevesítés engedély nélkül történő feloldása, vagy bármilyen egyéb jelentős gazdasági vagy szociális hátrány fakadhat; vagy ha az érintettek nem gyakorolhatják jogaikat és szabadságaikat, vagy nem rendelkezhetnek saját személyes adataik felett; vagy ha olyan személyes adatok kezelése történik, amelyek faji vagy etnikai származásra, vagy politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utalnak, valamint ha a kezelt adatok genetikai adatok, egészségügyi adatok vagy a szexuális életre, büntetőjogi felelősség megállapítására, illetve bűncselekményekre, vagy ezekhez kapcsolódó biztonsági intézkedésekre vonatkoznak; vagy ha személyes jellemzők értékelésére, így különösen munkahelyi teljesítménnyel kapcsolatos jellemzők, gazdasági helyzet, egészségi állapot, személyes preferenciák vagy érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére vagy előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából; vagy ha kiszolgáltatott személyek – különösen, ha gyermekek – személyes adatainak a kezelésére kerül sor; vagy ha az adatkezelés nagy mennyiségű személyes adat alapján zajlik, és nagyszámú érintettre terjed ki. (Rendelet preambulum 75. pontja)

Adatvédelmi incidens észlelésekor az informatikai csoportvezető és az adatvédelmi tisztviselő, haladéktalanul tájékoztatást ad a FÁNK Főigazgatójának.

Adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása az informatika valamint az adatvédelmi tisztviselő feladata.

Az informatikai rendszereken naplózni kell a hozzáféréseket és hozzáférési kísérleteket, és ezeket folyamatosan elemezni kell.

4. AZ ÉRINTETTEK TÁJÉKOZTATÁSA AZ ADATVÉDELMI INCIDENSRŐL

Ha a vizsgálat eredményeként megállapítást nyert, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az érintettek tájékoztatása szükséges, az adatvédelmi tisztviselő haladéktalanul értesíti az érintetteket, valamint a FÁNK Főigazgatóját.

Nem kell az érintetteket tájékoztatni:

- ha a FÁNK olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét; - ha az adatvédelmi incidens bekövetkezését követően a FÁNK olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg; - ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

5. ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA

Az adatvédelmi incidensekről nyilvántartást kell vezetni, amely tartalmazza:

a) az érintett személyes adatok körét,

b) az adatvédelmi incidenssel érintettek körét és számát,

c) az adatvédelmi incidens időpontját,

d) az adatvédelmi incidens körülményeit, hatásait,

e) az adatvédelmi incidens orvoslására megtett intézkedéseket,

f) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatvédelmi incidensekre vonatkozó nyilvántartást 5 évig meg kell őrizni.

6. ZÁRÓ RENDELKEZÉSEK

Jelen Szabályzat 2019. március 12-én lép hatályba.

7. INTÉZKEDÉSEK A SZABÁLYZAT MEGISMERTETÉSÉRE

E Szabályzat rendelkezéseit meg kell ismertetni a FÁNK valamennyi közalkalmazottjával valamint az egyéb jogviszonyban foglalkoztatott személyekkel.

8. ZÁRADÉK

A Szabályzatban nem szabályozott kérdésekben a mindenkor hatályos jogszabályok az irányadók.

A Szabályzat elválaszthatatlan részét képezik a felsorolt mellékletek.

9. MELLÉKLETEK

- I. sz. melléklet: Érintettek tájékoztatása adatvédelmi incidensről

- II. sz. melléklet: Nyilvántartás adatvédelmi incidensről