ADATVÉDELMI INCIDENSKEZELÉS ELJÁRÁSRENDJE

1. A Szabályzat célja

1. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (a továbbiakban: Rendelet) 5. cikk (2) bekezdése minden adatkezelőtől elvárja, a Rendeletnek való megfelelést és a megfelelés igazolás képességét („elszámoltathatóság”).

2. Az adatkezelőre vonatkozó adatok (továbbiakban: Intézmény):

   Név: Felsőpakonyi Herman Ottó Általános Iskola
   cím: 2363 Felsőpakony, Iskola utca 20.
   Törzskönyvi azonosító szám: K10870 (nyilvántartási szám)
   OM azonosító: 032477
   Adószám: 15835310-2-13
   honlap: http://iskola.felsopakony.hu/
   e-mail: iskola@felsopakony.hu
   telefon: 06 (29) 517-080
   intézményvezető: Matisz Zsolt

3. Az Intézmény, mint adatkezelő a Rendelet 25. cikk (1) bekezdésében meghatározott szervezési intézkedések részeként, az adatvédelmi incidens gyors azonosítása, bizonyítékok gyűjtése, megőrzése, az incidens következményeinek csökkentése, szükség esetén az adatvédelmi incidens határidőben történő bejelentése, az érintettek tájékoztatása, és az incidens következményeinek orvoslása érdekében a következő szabályzatot (továbbiakban: Szabályzat) alkotja:

2. A Szabályzat hatálya

4. A Szabályzat az alkalmazottakkal való közléstől, visszavonásáig hatályos.
5. Jelen szabályzat kötelezően felülvizsgálandó:
   a) jelentős szervezeti, vagy jogszabályi változásokat követően,
   b) a hatályossá válását követő minden harmadik évben, így a következő kötelező felülvizsgálat időpontja: 2025.;
   c) az adatkezelések változása, új adatkezelés bevezetése esetén haladéktalanul.
6. A Szabályzat személyi hatálya kiterjed az Intézmény alkalmazottaira, adatfeldolgozóira akik részére folyamatosan elérhetővé kell tenni.

3. Fogalmak

7. Az eljárásrend alkalmazásában:

   a) 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;
   b) adat megsemmisítése: az adat nem létezik többé, vagy nem létezik olyan formában, hogy azt az adatkezelő bármire használhassa;
   c) adat elvesztése: az adat még létezik, de az adatkezelő már elvesztette a felette lévő rendelkezést vagy a hozzáférést vagy már nincs a birtokában;
   d) adat megváltoztatása: az adatot megváltoztatták, meghibásodott vagy már nem teljes;
   e) adat jogosulatlan közlése, hozzáférése: adattovábbítás vagy nyilvánosságra hozatal olyan személyek részére, akiknek nincs felhatalmazása a hozzáférésre vagy az adatok fogadására;
   f) személyes adat: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

8. Az adatvédelmi incidensekre (a továbbiakban: incidens) történő gyors reagálás érdekében az Intézmény incidenskezelési csoportot (a továbbiakban: csoport) hozhat létre. Egyszerűbb megítélésű adatvédelmi incidens kivizsgálását, dokumentálását, értékelését az intézményvezető, az adatvédelmi tisztviselő bevonásával végzi.

9. A csoportban állandó tagként az adatvédelmi tisztviselő, az intézményvezető, az intézményvezető által megbízott személy, akadályoztatásuk esetén a helyettesítésükre kijelölt személy vesz részt.

10. Amennyiben nem saját fejlesztésű rendszert érintett az incidens, az intézményvezető intézkedik a fejlesztést végző értesítéséről a fejlesztési javaslatok megküldésével egyidejűleg.

11. Amennyiben az incidenskezeléssel érintett adatkezelésben adatfeldolgozó is részt vesz, az incidenskezelésbe az adatfeldolgozó képviselőjét is be kell vonni.

12. Aki a tevékenységének ellátása során az Intézmény által végzett adatkezeléssel kapcsolatban adatvédelmi incidens gyanúját, vagyis olyan esemény bekövetkezését észleli – ideértve azt is, ha az eseményt ő maga okozta – amelynek eredményeként személyes adatok véletlen vagy jogellenes megsemmisülésére, elveszésére, megváltoztatására kerülhetett sor, továbbá arra vonatkozó gyanúja áll fenn, hogy az adatok tekintetében arra nem jogosult személy adattovábbítást végezhetett vagy azokhoz illetéktelen személy szándékosan vagy véletlenül hozzáférhetett, az intézményvezető részére jelzi az eseményt.

13. Az incidenst észlelő az alábbi adatokat tünteti fel a jelzésben az intézményvezető részére:

a) az adatkezelés tárgyának rövid megjelölése, hogy az Intézmény mely nyilvántartásával, rendszerével vagy egyéb adatkezelésével kapcsolatban következett be az esemény;
b) az adatok kezeléséért felelős szervezet, vagy személy megjelölése;
c) az eseményt észlelő munkatárs neve, elérhetősége;
d) az esemény észlelőjén kívül az adott adatkezelés kapcsán érdemi információval szolgálni tudó személy neve, elérhetősége;
e) észlelés körülményei (az esemény rövid leírása);
f) az észlelés időpontja;
g) az eseménnyel érintett személyes adatok köre, valamint ha ez még nem állapítható meg teljes bizonyossággal, milyen személyes adatok lehetnek potenciálisan érintettek;
h) az esemény ismert következményei, illetve annak közvetlen veszélye.

14. Az intézményvezető akadályoztatása esetén az észlelő a vezető helyettesítésére kijelölt személyt tájékoztatja.

15. Amennyiben a vezető valamely okból az esemény adatvédelmi incidensként történő rögzítésével nem ért egyet, köteles arról feljegyzést készíteni.

16. Amennyiben az incidens az adatvédelmi tisztviselő tevékenységével áll összefüggésben, az észlelő a csoport bármely állandó tagja részére bejelentést tehet, ekkor az incidenst a csoport megkeresett tagja rögzíti a 13. pont szerint.

17. Az adatfeldolgozó igénybe vétele esetén, köteles az adatfeldolgozói szerződésben rendelkezni az adatfeldolgozó és az általa igénybe vett esetleges további adatfeldolgozó, incidensekkel kapcsolatos haladéktalan tájékoztatási kötelezettségéről és az incidenskezelésben történő kötelező közreműködéséről, továbbá ki kell kötni az adatfeldolgozó felelősségét azon esetekre, amikor az adatkezelő az incidensek kezelését az adatfeldolgozó mulasztása miatt nem képes a rendeletnek megfelelően ellátni.

18. A 17. pont szerinti szerződésben rendelkezni kell arról, hogy az adatfeldolgozó az incidensek bejelentését az erre szolgáló elektronikus levélcímen teheti meg az Intézmény felé, az **1. függelék** szerinti adattartalommal.

19. A csoport állandó tagjai a csoport valamely tagjától kapott értesítés alapján haladéktalanul megkezdik az észlelt esemény körülményeinek kivizsgálását.

20. A csoport a bejelentést követően az esemény kivizsgálása és az incidens kezelése érdekében tett intézkedéseit folyamatosan dokumentálja. A csoport az adatvédelmi incidens dokumentálása érdekében a **2. függelék** szerinti segédletet is kitölti, amely segítséget nyújt annak eldöntésében, hogy szükséges-e a NAIH, illetve az érintettek tájékoztatása.

21. Amennyiben a bejelentő általi észlelés időpontjában egyértelmű, hogy az esemény biztonsági eseménynek minősül és személyes adatok érintettsége ésszerűen nem zárható ki, tudomásra jutás időpontjaként az észlelés időpontját kell megjelölni.

22. A körülmények feltárása körében vizsgálni kell, hogy az esemény valóban biztonsági eseménynek minősül-e és személyes adatok érintettsége ésszerűen kizárható-e. Amennyiben a vizsgálat eredménye szerint az esemény biztonsági eseménynek minősül és személyes adatok érintettsége ésszerűen nem zárható ki, ezen megállapítás időpontját kell az adatvédelmi incidens adatkezelő tudomására jutási időpontjaként megjelölni.

23. Amennyiben a vizsgálat során megállapítható, hogy az intézkedés hiánya visszafordíthatatlan következményekkel járna vagy az eset azonnali intézkedést igényel, a csoport megteszi a szükséges intézkedéseket, és azok leírását és indokát rögzíti.

24. A vizsgálat során fel kell tárni a bizonyíthatóan vagy feltételezhetően érintett személyes adatok kategóriáit és számát, továbbá az érintettek számát.

25. A csoport az érintett kapcsolattartóval a következők szerint együttműködve megállapítja, hogy az előzetesen elkészített kockázatértékelési táblázatban szereplő mely következményekkel lehet számolni, értékelni kell azok további egymásra gyakorolt hatását, és ezek alapján fel kell mérni az érintettek jogaira és szabadságaira gyakorolt hatás mértékét:

    a) amennyiben az incidens több adatkezelést is érintett, a vizsgálatot adatkezelésenként kell elvégezni azzal, hogy azok egymásra gyakorolt hatását is értékelni kell,
    b) amennyiben az incidens egy, más adatkezelésekkel összeköttetésben álló rendszerben következett be, a vizsgálatot minden rendszerre el kell végezni,
    c) amennyiben a vizsgálat eredményeként kiderül, hogy az észlelt esemény nem adatvédelmi incidens, annak indokolását dokumentálni kell,
    d) amennyiben a vizsgálat eredményeként a csoport megállapítja, hogy az incidens valószínűsíthetően nem jár kockázattal az érintettek jogaira és szabadságaira nézve, azt indokolással dokumentálni kell, kitérve az incidens kezelésére és a további hasonló incidensek elkerülése érdekében javasolt intézkedésekre,
    e) amennyiben a vizsgálat eredményeként a csoport megállapítja, hogy az incidens valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve, azt indokolással dokumentálni kell, kitérve az incidens kezelésére és a további hasonló incidensek elkerülése érdekében javasolt intézkedésekre, ideértve a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: NAIH) felé történő jelentést is,
    f) amennyiben a vizsgálat eredményeként a csoport megállapítja, hogy az incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, azt indokolással dokumentálni kell, kitérve az incidens kezelésére és a további hasonló incidensek elkerülése érdekében javasolt intézkedésekre, ideértve a NAIH felé történő jelentést és az érintettek tájékoztatását is, kitérve a tájékoztatás javasolt módjára.
    g) a csoport rögzíti és megőrzi a kivizsgálás során tudomására jutó bizonyítékokat.

26. Amennyiben az érintettek tájékoztatása kapcsán a rendelet 34. cikk (3) bekezdésében felsorolt kivételek valamelyike fennáll, és erre tekintettel a csoport a tájékoztatást nem javasolja, ahhoz az alábbi indokolást kell fűzni:

a) meg kell jelölni az adatkezelő által végrehajtott, az adatvédelmi incidens által érintett adatok tekintetében alkalmazott olyan megfelelő technikai és szervezési védelmi intézkedéseket, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
b) az adatkezelő által az adatvédelmi incidenst követően tett olyan további intézkedéseket, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) amennyiben az érintettek személyes tájékoztatása aránytalan erőfeszítést tenne szükségessé, meg kell jelölni ennek indokát és az érintettek nyilvánosan közzétett információk vagy hasonlóan hatékony intézkedés útján történő tájékoztatásának javasolt módját.

27. A csoport az adatvédelmi incidensről a következményekre tekintettel az intézményvezető részére írásbeli összefoglalót készít, amely a következőket tartalmazza:

a) az esemény rövid ismertetését,
b) az esemény kivizsgálását végző személyek megnevezését,
c) az adatvédelmi incidens jellegét, vagyis, hogy bizalmasság, sértetlenség vagy rendelkezésre állás sérült-e,
d) az érintettek kategóriáit,
e) az érintettek hozzávetőleges számát,
f) az incidenssel érintett adatok kategóriáit,
g) az incidenssel érintett adatok hozzávetőleges számát,
h) az incidens valószínűsíthető kockázatait vagy következményeit (elsődleges és másodlagos következményeket, figyelemmel azok valószínűségére és súlyosságára) vagy azok hiányát,
i) a haladéktalanul szükségessé vált és elvégzett intézkedések ismertetését.

28. Az összefoglalóban az előző pontban foglaltakon túl az intézményvezetőn kívül a csoport indokolással ellátott javaslatot tesz az intézményvezető részére az incidens kezelésére, amely tartalmazza, hogy:
a) szükséges-e a NAIH felé jelentés küldése,
b) szükséges-e az érintettek értesítése,
c) javasolt intézkedések az incidens orvoslása érdekében, határidővel, ideértve a már bekövetkezett következmények enyhítését is.

29. Az adatvédelmi tisztviselő a javaslatot haladéktalanul közvetlenül az intézményvezető részére megküldi, amelyet a csoport valamennyi tagja aláír.

30. Az intézményvezető, mint döntésre jogosult, a javaslatban foglaltak alapján dönt a javasolt intézkedés elfogadásáról. A javaslatban szereplő intézkedések alatt a csoport szövegszerűen feltünteti, hogy a „Döntésre jogosult vezető, a bizottság által a jelen jelentésben foglaltakkal maradéktalanul egyetért, melyet aláír”. A döntésre jogosult vezető egyetértése esetén, a hozzá felterjesztett javaslat elfogadásaként aláírja az iratot, vagy a javasolt intézkedés megváltoztatása érdekében visszautasítja azt, és megindokolja a döntését.

31. Az előző pont szerinti Intézményvezetői döntés tartalmáról feljegyzést kell készíteni, amelyben rögzíteni kell, ha a csoport javaslatához képest eltérő döntés született, amennyiben ismert, annak indokát is megjelölve.

32. A kivizsgálás során rögzített adatokat, az azokkal összefüggésben tett intézkedéseket a vizsgálat lezárását követően külön nyilvántartásba kell venni.

33. Amennyiben az incidensről való tudomásszerzést követő 48 órán belül nem kerül sor a 26-27. pontok szerinti teljes összefoglaló összeállítására, a csoport részösszefoglalót készít.

34. A részösszefoglalót a 26-27. pontokban meghatározottak szerint kell megküldeni azzal, hogy a részösszefoglaló felterjesztésével egyidejűleg a vizsgálatot tovább kell folytatni, és annak lezárását követően a vizsgálatról teljes összefoglalót kell megküldeni.

35. Amennyiben az adatvédelmi incidens megítélése egyszerű, úgy a 13. pontban foglaltakról történő tudomás szerzés alapján, az adatvédelmi tisztviselővel való egyeztetést követően a **2. függelék** kitöltése alapján dokumentált intézményvezetői döntés hozható a NAIH felé történő bejelentés jóváhagyása érdekében.

36. Amennyiben az intézményvezető a NAIH felé történő bejelentést jóváhagyja, a NAIH részére történő bejelentést a hatóság internetes felületén az adatvédelmi tisztviselő, távollétében a helyettesítésére a csoportból kijelölt személy teszi meg, amelynek bejelentési időpontját a rendszerben rögzíteni kell. A beküldött bejelentés online rendszerből generált kivonatát az intézményvezető részére az adatvédelmi tisztviselő megküldi.

37. A NAIH-hal az incidens kezelése során az adatvédelmi tisztviselő tart kapcsolatot, amely együttműködésről folyamatosan tájékoztatja az intézményvezetőt, az eljárásba a csoport további tagjait szükség szerint bevonja.

38. Az érintettek gyors tájékoztathatósága érdekében minden adatkezelés kapcsán fel kell mérni a tájékoztatás elsődleges módját.

39. Az Intézményhez nem tartozó érintettekkel történő kapcsolattartást, értesítés esetén - az adatkezelés kapcsán, az érintett által megadott kapcsolattartási csatorna valamelyikén keresztül - az adatkezelő szakterület végzi.

40. A tájékoztató nem küldhető együtt más anyaggal, irattal, tájékoztatással.

41. Az érintettek részére küldendő tájékoztatót az intézményvezető és az adatvédelmi tisztviselő közösen készíti el a **3. függelék** alapján.

42. A tájékoztatóban világosan és közérthetően ismertetni kell:
    a) az adatvédelmi incidens jellegét,
    b) az adatvédelmi tisztviselő nevét és elérhetőségeit,
    c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
    d) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

43. A tájékoztatóban minden esetben meg kell határozni, ha az érintettek maguk milyen intézkedéseket tehetnek az incidens káros következményeinek elhárítása érdekében.

44. Amennyiben a közvetlen tájékoztatás lehetősége aránytalan erőfeszítéssel járna, és a csoport az érintettek körére figyelemmel az Intézmény média útján történő tájékoztatást javasolta, a csoport jelentésének Intézményvezetői jóváhagyását követően a megbízott alkalmazott intézkedik a csoport által elkészített tájékoztató közzététele érdekében.

45. Az alkalmazott személyes adatait érintő adatvédelmi incidens tekintetében a tájékoztatás elsődlegesen elektronikus levélcímre vagy ügyfélkapura küldött értesítés útján történik. Amennyiben az incidensről történő értesítés e módon nem lehetséges, az alkalmazottat szóban, dokumentált módon kell tájékoztatni.

46. Az érintettek tájékoztatási módját és idejét dokumentálni kell.

47. Az incidens orvoslására tett intézkedéseket az intézményvezető által jóváhagyott javaslat szerint kell végrehajtani.

48. Rögzíteni kell:
    a) a megtett intézkedéseket, valamint azok időpontját,
    b) a NAIH által tett megállapításokat, javaslatokat,
    c) a NAIH javaslatai alapján tett intézkedéseket és azok végrehajtási idejét.

49. Az incidenssel kapcsolatos vizsgálat lezárását követően az érintett adatkezelések kockázatértékelését ismételten el kell végezni, az annak során tett megállapításokat, javaslatokat és újfajta adatbiztonsági intézkedéseket rögzíteni kell.

50. Amennyiben az incidens bejelentése a tudomásszerzéstől számított 72 órán belül nem valósult meg, a késedelem tényéről és annak okáról az adatvédelmi tisztviselő feljegyzést készít és azt megküldi az intézményvezető részére.

51. Az adatkezelőt a vele kötött adatfeldolgozói szerződésben kijelölt kapcsolattartó haladéktalanul, az intézményvezető egyidejű tájékoztatása mellett értesíti. Az értesítést az adatkezelő által az adatfeldolgozói szerződésben meghatározott tartalommal kell megtenni. Amennyiben az adatkezelő ilyet nem határozott meg, az Intézmény a saját adatfeldolgozóitól elvárt adattartalmat bocsátja az adatkezelő rendelkezésére.

Kelt: Felsőpakony, 2022. október 1.

…….
Matisz Zsolt
intézményvezető
Felsőpakonyi Herman Ottó
Általános Iskola