Szabályzat megnevezése	**Adatvédelmi Incidenskezelési szabályzat**	
Verzió	**2023/ 01**	
Hatályba lépés dátuma:	2023. JANUÁR 01. NAPJA	
Készítő	Hierotheosz Egyesület	
Felülvizsgálat gyakorisága:	évente	

Verzió kontroll		
Hatályba lépés	**Verzió**	**Módosítás részletei**
	2023/01	Dokumentum keletkezése

ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZAT

Máriapócs, 2023. január 01.

Tartalomjegyzék

1. Adatvédelmi incidens

1.1. Adatvédelmi incidens típusai

Az adatvédelmi incidens egyfajta biztonsági incidens. Minden adatvédelmi incidens biztonsági incidens, de nem minden biztonsági incidens adatvédelmi incidens. Ez azt jelenti, hogy a biztonság megsértése akkor minősül személyes adatok megsértésének, amikor a megsértett adatok személyes adatok.

Az adatvédelmi incidens típusai:

- titoksértés,
- hozzáférhetőségi adatsértés,
- sértetlenségi adatsértés.

A körülményektől függően a személyes adatok megsértése a titkossággal, az adatok hozzáférhetőségével, valamint sértetlenségével is kapcsolatos lehet egyidejűleg, illetve előfordulhat ezek bármelyikének kombinációja.

1.2. Adatvédelmi incidens lehetséges következményei

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában

- fizikai,
- vagyoni, vagy
- nem vagyoni károkat

okozhat a természetes személyeknek, többek között

- a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,
- a hátrányos megkülönböztetést,
- a személyazonosság-lopást vagy a személyazonossággal való visszaélést,
- a pénzügyi veszteséget,
- az álnevesítés engedély nélküli feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve
- a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Következésképpen, amint az Egyesület, mint adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles a Hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az érintettet az Egyesület, mint adatkezelő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. A tájékoztatásnak tartalmaznia kell

- annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint
- az érintett a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatokat.

Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a Hatósággal, és betartva az általa vagy más érintett hatóságok, például bűnüldöző hatóságok által adott útmutatást. Például, ha az érintettek sürgős tájékoztatása a kár közvetlen veszélyének mérsékléséhez szükséges.

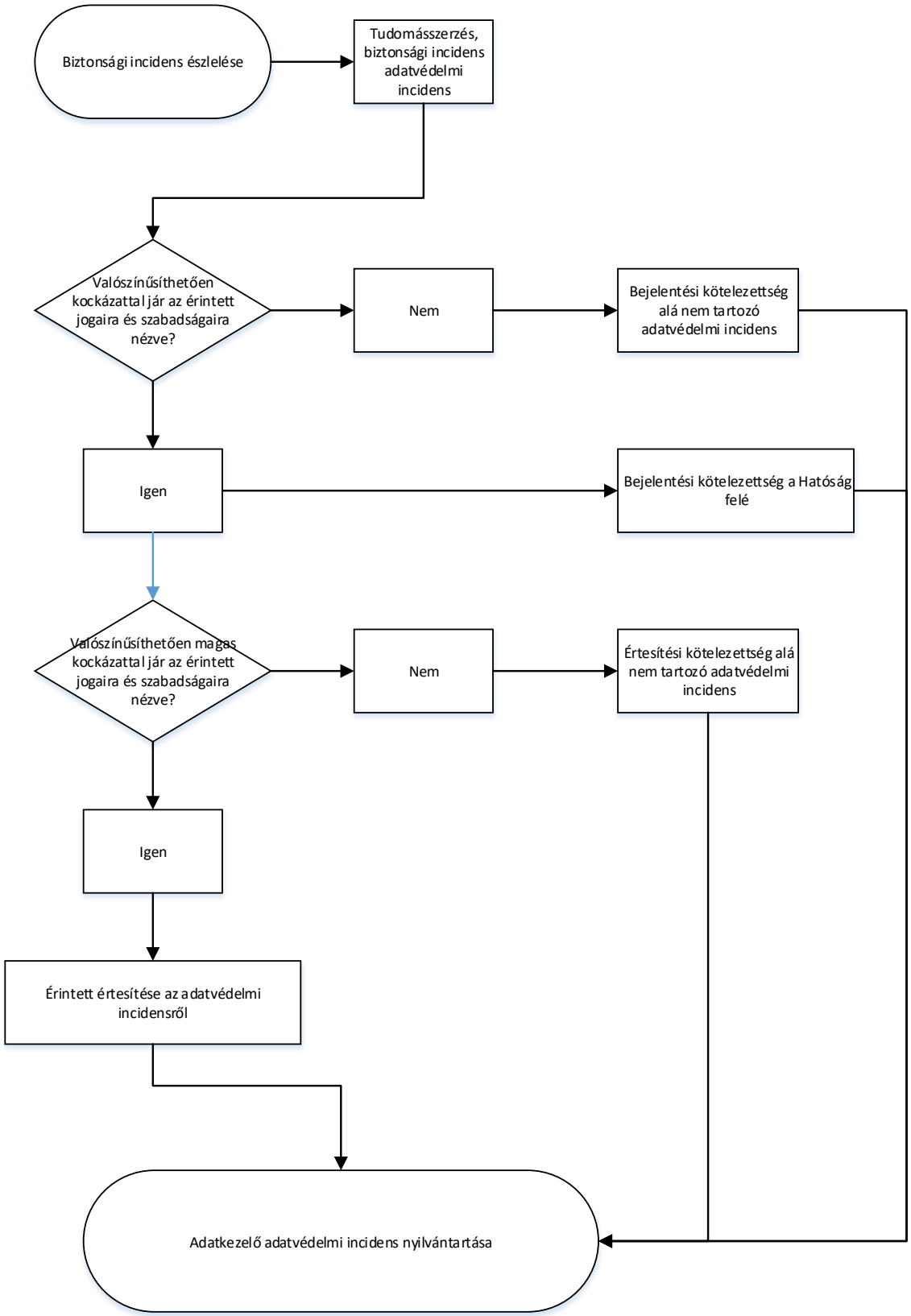
Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen

- az adatvédelmi incidens jellegére és súlyosságára, valamint
- annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira

figyelemmel kell megállapítani.

A Hatóságnak történt bejelentés a Hatóságnak az Általános Adatvédelmi Rendeletben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti.

1.3. Az adatvédelmi incidenskezelés folyamatábrája



A Hatóság adatvédelmi incidens bejelentő rendszerébe az Egyesületet az adatvédelmi tisztviselő vagy az Egyesület részéről eljáró személy regisztrálja.

Adatvédelmi incidens gyanúja esetén haladéktalanul értesíteni kell az adatvédelmi tisztviselőt (amennyiben van) vagy az Egyesület vezetőjét és az elektronikus információs rendszer biztonságáért felelős személyt. Ha az adatvédelmi incidens az adatfeldolgozót is érinti, az adatvédelmi tisztviselő egyeztet az adatfeldolgozó képviselőjével a felmerülő kockázatokról és azok esélyeiről.

Az adatvédelmi tisztviselő (vagy az Egyesület vezetője) és az elektronikus információs rendszer biztonságáért felelős személy haladéktalanul megvizsgálja, hogy

- a biztonság sérülése érinti-e a személyes adatok biztonságát,
- kockázatos-e a biztonság sérülése az érintettek jogaira és szabadságaira nézve, különös tekintettel az incidenssel érintett adatok típusára, mennyiségére,
- milyen intézkedések tehetők a kockázatok csökkentésére,
- szükséges-e az adatvédelmi incidens bejelentése a Hatóság felé, és
- szükséges-e az érintettek értesítése.

Az adatvédelmi tisztviselő (vagy az Egyesület vezetője) és az elektronikus információs rendszer biztonságáért felelős személy az elvégzett elemzés alapján dönt

- az esemény adatvédelmi incidensnek nyilvánításáról vagy
- az adatvédelmi incidensnek nyilvánítás mellőzéséről.

Amennyiben az adatvédelmi tisztviselő (vagy az Egyesület vezetője) és az elektronikus információs rendszer biztonságáért felelős személy az eseményt adatvédelmi incidensként értékeli, úgy dönt annak alacsony, közepes vagy magas kockázatáról. E személyek a döntésről az adatvédelmi incidens bekövetkeztéről való tudomásszerzést követő 24 órán belül értesítik az Egyesület vezető tisztségviselőjét.

Az adatvédelmi incidens kockázata

- alacsony, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve,
- közepes, ha az adatvédelmi incidens kockázata nem magas, de valószínűsíthetően kockázattal jár az érintettek jogaira és szabadságaira nézve, és a negatív következményeket nem lehet intézkedésekkel hatékonyan elhárítani,

- magas, ha az adatvédelmi incidens az érintettek jogaira és szabadságaira nézve jelentős vagy akár visszafordíthatatlan következményekkel vagy komoly nehézségekkel jár vagy járhat.

Alacsony kockázatú adatvédelmi incidenst kizárólag az adatvédelmi incidens nyilvántartásban szükséges rögzíteni.

Ha az adatvédelmi incidens közepes vagy magas kockázatú, az adatvédelmi tisztviselő és az elektronikus információs rendszer biztonságáért felelős személy javaslatot tesz az Egyesület részére az adatvédelmi incidens következményeinek mérséklését célzó intézkedésekre. Ezekben az esetekben az adatvédelmi incidenst az adatvédelmi tisztviselő az Egyesület tudomásszerzésétől számított 72 órán belül bejelenti a Hatóság részére annak incidensbejelentő rendszerén keresztül. Magas kockázatú adatvédelmi incidens bekövetkeztéről az érintetteket - a megfelelő intézkedés megtétele céljából - tájékoztatni kell. A tájékoztatás megtételéről az adatvédelmi tisztviselő (vagy az Egyesület vezetője) gondoskodik.

Ha a közvetlen tájékoztatás lehetetlen, vagy aránytalan nehézségbe ütközik, a tájékoztatást egyéb módon kell megtenni, különösen az adatkezelő honlapján vagy a helyben szokásos hirdetményi úton.

Az adatkezelő (vagy az Egyesület vezetője) a tevékenységéről dokumentációt vezet, amelyben részletesen rögzíti a döntések alapjait, körülményeit.

Az Egyesület az adatvédelmi incidensekről az 1. sz. melléklet szerinti formában nyilvántartást vezet.