Tabi Egészségfejlesztési Központ .

ADATVÉDELMI INCIDENSKEZELÉSI SZABÁLYZATA

Verzió: 1.0.

Tab, 2023. augusztus 24

Az Európai Parlament és a Tanács (EU) 2016/679 számú (2016. április 27.), a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, a 95/46/EK rendelet hatályon kívül helyezéséről szóló általános adatvédelmi rendelet (a továbbiakban: **GDPR**), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény rendelkezései alapján a Koppány-Völgye KEK Egészségügyi és Szolgáltató Nonprofit Kft. (a továbbiakban: **Adatkezelő**) adatvédelmi incidenskezelési tevékenységét az alábbiak szerint szabályozom.

1. A SZABÁLYZAT CÉLJA, HATÁLYA

1. §

(1) A jelen Adatvédelmi Incidenskezelési Szabályzat (a továbbiakban: **Szabályzat**) célja, hogy az Adatkezelő vonatkozásában meghatározza azokat a belső szabályokat és intézkedéseket, amelyek az Adatkezelő által a bekövetkezett adatvédelmi incidensek esetén végrehajtandók. A szabályok és intézkedések az adatvédelmi incidensek hatásainak csökkentésére, bekövetkezésük okának feltárására és további incidensek elkerülésére, valamint az incidensek által leállított folyamatok minél előbbi újraindítására irányulnak.

(2) Jelen Szabályzat személyi hatálya kiterjed:
a) az Adatkezelő vezető tisztségviselőire;
b) az Adatkezelőnél egészségügyi szolgálati jogviszonyban foglalkoztatott alkalmazottakra;
(az a) és b) pontban meghatározott személyi kör a továbbiakban együttesen: **Foglalkoztatottak**);
c) az Adatkezelő adatvédelemért felelős vezetőjére, vagy felelős személyére az incidenskezelési folyamatban meghatározott feladatok végrehajtása vonatkozásában;
d) az incidenskezelés szakmai elemzésére, megoldására, kezelésére kijelölt természetes személyekre, feladataik végrehajtása vonatkozásában.

(3) Jelen Szabályzat tárgyi hatálya kiterjed
a) az adatvédelmi incidenssel érintett személyes adatokra;
b) az incidens kezelése során tett intézkedésekre;
c) az adatvédelmi incidenssel érintett adathordozókra és rendszerekre.

2. FOGALOMMEGHATÁROZÁSOK:

2. §

(1) Jelen szabályzat alkalmazásában az adatkezelő, az adatfeldolgozó, az adatvédelmi incidens, az adatkezelés, az érintett, a harmadik fél és a személyes adat fogalommeghatározásainál a GDPR 4. cikk *„Fogalommeghatározások”* körében megfogalmazottak az irányadóak.

(2) A jelen Szabályzat vonatkozásában az adatvédelmi incidenssel érintett személyes adatok lehetnek:

a) olyan személyes adatok, melyeknek az Adatkezelő az adatkezelője;
b) olyan személyes adatok, melyeknek az Adatkezelő az adatfeldolgozója;
c) olyan személyes adatok, melyek vonatkozásában az Adatkezelő a GDPR szerinti közös adatkezelői pozícióban áll.

(3) Jelen Szabályzat alkalmazásában adatfeldolgozó lehet:
a) az Adatkezelő által megbízott harmadik személy adatfeldolgozó;
c) általa kötött és őt terhelő adatfeldolgozói szerződés alapján az Adatkezelő.

3. ADATVÉDELMI INCIDENS ÉSZLELÉSE, ELHÁRÍTÁSA

3. §

(1) Az adatvédelmi incidensről az Adatkezelő jellemzően három módon szerezhet tudomást:
a) Foglalkoztatottak által észlelt incidens;
b) érintett által bejelentett incidens;
c) harmadik fél által bejelentett incidens.

(2) Jellemző események, amelyek adatvédelmi incidenst okozhatnak:
a) adathordozó eszközök elvesztése vagy azok megsemmisülése;
b) adatállomány véletlen vagy szándékos törlése, megsemmisítése, megváltoztatása;
c) jogosulatlan (idegen vagy fel nem hatalmazott) személy hozzáférése az adatokhoz, adatmásolás, támadás, szándékos visszaélés megvalósítása;
d) adatok jogosulatlan átadása, hozzáférés biztosítása jogosulatlan személynek;
e) vírus vagy hacker támadás a számítógépen vagy a szerveren tárolt adatok esetében.

(3) Az Adatkezelő vagy az Adatkezelő nevében és utasításai alapján személyes adatokat kezelő adatfeldolgozó kezelésében lévő személyes adatokat érintő adatvédelmi incidens bekövetkezése esetén az Adatkezelő az adatvédelmi incidensről való tudomásszerzését követően haladéktalanul megtesz minden olyan intézkedést, amely szükséges:
a) az adatvédelmi incidensből eredő további adatszivárgás, vagy adatvesztés meggátolásához;
b) az adatbiztonság sérülésének helyreállításához és;
c) az adatvédelmi incidensből eredő károk mérsékléséhez.
(a fentiek a továbbiakban együttesen: **Beavatkozás**).

(4) Adatvédelmi incidens bekövetkezése esetén a Beavatkozás szervezésében és lebonyolításában az Adatkezelő nevében az Adatkezelő mindenkori intézményvezetője (a továbbiakban: intézményvezető) jár el.

(5) A Beavatkozás során az Intézményvezetőnek az informatikai szakterületért felelős Foglalkoztatott közreműködésével minden szükséges intézkedést meg kell tennie az incidens elhárítása és annak kivizsgálása érdekében, de különösen a következő cselekményeket:
a) meg kell állapítani az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) fel kell mérni az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
c) ki kell vizsgálni az incidens valószínű okát és fennállásának elhárítására azonnali intézkedéseket kell hozni;
d) hosszabb távú intézkedési tervet kell kidolgozni az incidens hatásainak csökkentésére, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

(6) A Beavatkozás végrehajtása során az Intézményvezető utasításai alapján a Beavatkozás lebonyolításában részt vevőknek különösen az alábbi részfeladatokat szükséges elvégezniük:
a) a további adatszivárgás megelőzése érdekében az incidenssel érintett infrastruktúra működésének fizikai vagy elektronikus úton történő felfüggesztése;
b) érintettség esetén a nyílt internet hozzáférésének blokkolása;
c) incidenssel érintett infrastruktúra hozzáférésének zárolása;
d) körülmények rögzítése a későbbi kivizsgálás érdekében;
e) logfájlok kinyerése;
f) incidens bekövetkezésében érintett személyek, valamint az incidenssel kapcsolatosan releváns információkkal bíró Foglalkoztatottak által elmondott információk jegyzőkönyv formájában történő rögzítése.

(7) Papír alapon történő adatkezelés esetén a Beavatkozásnak ki kell terjednie továbbá az alábbi lépések megtételére:
a) a dokumentumokat a tároló hely sérülésének elhárítása idejéig szükség esetén biztonságos helyre kell szállítani,
b) az adatok védelmének és integritásának biztonságát veszélyeztető állapot elhárítását azonnal meg kell kezdeni, az elhárítás idejére folyamatos felügyeletet kell biztosítani, vagy a dokumentumokat zárható helyre kell szállítani.

(8) Amennyiben az adatvédelmi incidens elektronikus adat nyilvántartó rendszert érint, a rendszer működésképtelensége alatt az adatokat papír alapon kell rögzíteni, és az elektronikus rendszer helyreállítását követően azokat a rendszerbe pótlólagosan fel kell venni. Az elektronikusan tárolt adatok sérülése esetén az Intézmény informatikai szabályzataiban foglaltak szerint kell eljárni és az incidenst jelenteni

(9) A sérült adat pótlásáért annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett.

(10) Az egészségügyi adatpótlásba be kell vonni azon betegellátó szervezeti egységek vezetőit, ahol a beteget kezelték és az adatok megsérültek. A pótolt adatokon a pótlás tényét fel kell tüntetni. Az egészségügyi adat sérüléséről és pótlásáról/visszaállításáról az egészségügyi ellátásért felelős szervezeti egység vezetője értesíti az Intézményvezetőt, továbbá jegyzőkönyvet vesz fel.

(11) A papír alapon kezelt adatok esetén:
a) a hagyományos adathordozók tárolásakor az adatok visszakereshetőségének érdekében a megőrzés biztosítására az Adatkezelő iratkezelési szabályzatának előírásai szerint kell eljárni;

b) a következmények felszámolásakor, a visszaállítás érdekében, minden lehető és észszerű intézkedést meg kell tenni, felhasználva a bármely szervezeti egységben, vagy a betegnél fennmaradt hiteles dokumentumot;
c) a visszaállítást és annak mértékét az Intézményvezető egyetértésével a szervezeti egység vezetője írásban rendeli el.

4. AZ ADATVÉDELMI INCIDENS ÉRTÉKELÉSE

4. §

(1) A Beavatkozás során, illetve azt követően az Intézményvezető vagy az erre általa írásban kijelölt Foglalkoztatott felméri és a jelen Szabályzat 1. mellékletét képező adatvédelmi incidenskezelési nyilvántartásban, valamint az adatkezelői nyilvántartásában is rögzíti az adatvédelmi incidens körülményeit.

(2) Amennyiben az (1) bekezdésben rögzített felmérés során az Intézményvezető megállapítja, hogy az adatvédelmi incidens kockázattal jár az Érintettek jogainak érvényesülésére vonatkozóan, az adatvédelmi incidenst legfeljebb az arról való tudomásszerzését követő **72 órán belül** bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: **Felügyeleti Hatóság**) részére, a Felügyeleti Hatóság által működtetett internet alapú bejelentőrendszeren keresztül. Amennyiben az Intézményvezető a bejelentést a fenti határidőben nem tudja kivitelezni, úgy a bejelentéshez a késedelem igazolására szolgáló releváns, az incidens tárgykörével konkrétan összefüggő dokumentumok gyűjti, rendszerezi és a bejelentéshez mellékeli.

(3) Amennyiben az adatvédelmi incidens jellegéből fakadóan az (1) bekezdésben rögzített felmérést megelőzően is vélelmezhető, hogy az adatvédelmi incidens kockázattal jár az Érintettek jogainak érvényesülésére nézve, az Intézményvezető a (2) bekezdésben meghatározott bejelentést **haladéktalanul** megteszi.

(4) Amennyiben az (1) bekezdésben rögzített felmérés alapján valószínűsíthető, hogy az adatvédelmi incidens nem jár kockázattal az Érintettek jogainak érvényesülésére vonatkozóan, az Intézményvezető a jelen a (2) bekezdésben rögzített bejelentést **nem teszi meg**.

(5) Amennyiben az (1) bekezdésben rögzített felmérés alapján valószínűsíthető, hogy az adatvédelmi incidens az Érintetett megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következményekkel járhat, az Intézményvezető az adatvédelmi incidensről **haladéktalanul** tájékoztatja az Érintettet.

A tájékoztatás módja tekintetében meghatározó körülmény az, hogy az Adatkezelő az Érintett mely személyes adatát tartja nyilván e tárgykörben (pl.: postacímét, elektronikus levelezési címét). Amennyiben az érintetti tájékoztatás aránytalan erőfeszítést tenne szükségessé, úgy az Érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az Érintettek hasonlóan hatékony tájékoztatását.

Az Érintetti tájékoztatásnak legalább az alábbi információkat kell tartalmaznia:

a) az Adatkezelőnek az adatvédelmi incidensről további tájékoztatást nyújtó kapcsolattartójának neve és elérhetősége;
b) az adatvédelmi incidensből eredő, valószínűsíthető következmények;
c) az Intézményvezető által az adatvédelmi incidens orvoslására tett intézkedések, az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések.

Az Érintetti tájékoztatás tényének megtörténtét az Intézményvezető vagy az általa kijelölt Foglalkoztatott a jelen Szabályzat 1. mellékletét képező adatvédelmi incidenskezelési nyilvántartásban is rögzíti.

(6) Az Intézményvezető az (5) bekezdésben részletezett tájékoztatást abban az esetben mellőzheti, ha:

a) a Beavatkozás során megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre az adatvédelmi incidenssel érintett adatok vonatkozásában annak érdekében, hogy azok illetéktelenek számára értelmezhetetlenek legyenek;
b) a Beavatkozás során olyan további intézkedéseket tett, melyek biztosítják, hogy az Érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
c) az Érintettek tájékoztatása aránytalan erőfeszítést tenne szükségessé, például azok nagy száma vagy elérhetőségük ismeretlensége miatt. Ebben az esetben az Intézményvezető az Érintetteket az Adatkezelő https://tabjaro.hu elérési című honlapján nyilvánosan közzétett információk útján tájékoztatja.

Az Érintetti tájékoztatás mellőzésének tényét és jogalapját az Intézményvezető vagy az általa kijelölt Foglalkoztatott a jelen Szabályzat 1. mellékletét képező adatvédelmi incidenskezelési nyilvántartásban is rögzíti.

5. FELELŐSSÉGI KÉRDÉSEK, TOVÁBBI ADATVÉDELMI INCIDENSEK MEGELŐZÉSE

5. §

(1) A jelen Szabályzat 4. § (1) bekezdésében rögzített felmérésnek a szervezeti és személyi felelősségi kérdésekre is ki kell terjednie, a kivizsgálás során az egyes bizonyítékokat úgy kell gyűjteni, hogy azokat esetleges későbbi fegyelmi, illetve hatósági eljárásban hiteles bizonyítékként figyelembe lehessen venni.

(2) Amennyiben a jelen Szabályzat 4. § (1) bekezdésében rögzített felmérés az adatvédelmi incidens bekövetkezésében személyi felelősséget tár fel, úgy az Intézményvezető a felelősségre vonáshoz kapcsolódó intézkedések megtételéről gondoskodik.

(3) A jelen Szabályzat 4. § (1) bekezdésében rögzített felmérés eredményei alapján az Adatkezelőnek át kell tekintenie az adatkezelésre vonatkozó gyakorlatát, ennek körében különösen a szervezeti és személyi jogosultságok rendszerét, valamint az alkalmazott technológiákat. Az áttekintés során levont következtetések alapján az Intézményvezető

intézkedési terv összeállítására köteles, mely legalább a következő utánkövetési műveletek részletes meghatározását tartalmazza:

a) az adatkezeléshez alkalmazott technológiai eszközök fizikai és logikai védelmi képességeinek fejlesztésére vonatkozó felmérés elvégzése, fejlesztési ütemek meghatározása;
b) az adatokhoz történő személyi hozzáférés felülvizsgálata és szükség szerinti megváltoztatására irányuló javaslatok összeállítása;
c) az adatkezelésben érintett Foglalkoztatottak adatvédelmi tudatosításának elvégzése.

(5) Az intézkedési terv végrehajtását az Intézményvezető koordinálja.

6. ZÁRÓ ÉS HATÁLYBA LÉPTETŐ RENDELKEZÉSEK

6. §

(1) Jelen Szabályzat 2024. augusztus 24 napján lép hatályba.

(2) Jelen Szabályzatot jogszabályváltozás, belső szervezeti változás vagy feladatváltozás esetén a változás hatályba lépésétől számított 30 napon belül és legalább évente felül kell vizsgálni és megfelelően módosítani kell.

(3) Jelen Szabályzat megismerése az Adatkezelő közös hálózati meghajtóján keresztül minden Foglalkoztatott számára biztosított.
A szervezeti egységek vezetői vagy a kijelölt Foglalkoztatottak kötelesek gondoskodni arról, hogy a jelen Szabályzatban foglalt előírásokat a szervezeti egységek foglalkoztatottjai megismerjék, annak tényét a jelen szabályzat 1. függeléke szerinti papíralapú Megismerési nyilatkozaton aláírásukkal igazolják.

Tab, 2024. augusztus 24

…….……..…..……
Faragóné Magyarósi Krisztina
intézményvezető

MELLÉKLETEK JEGYZÉKE

1. melléklet: Adatvédelmi incidenskezelési nyilvántartás

1. függelék

Megismerési nyilatkozat

A 2023. augusztus 24. –tól hatályos, **Adatvédelmi Incidenskezelési Szabályzatban** foglaltakat megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartani és betartatni.

Név	Beosztás	Dátum	Aláírás