Adatkezelési tájékoztató
LongiKid® Vizsgálószoftverhez

Az adatkezelő megnevezése: TSMT-HRG College Korlátolt felelősségű társaság
Az adatkezelő adatai
Székhely: 1027 Budapest, Frankel Leó út 13. félemelet 1.
Cégjegyzékszám: 01-09-293510
Adószám: 25868452-2-41
Képviseli: Fenyősi Fanni ügyvezető

I. Bevezetés:

A jelen adatkezelési szabályzat a TSMT-HRG College Kft., továbbiakban: **Adatkezelő** által használt LongiKid® Vizsgálószoftver adatkezelési folyamatait írja le. A szabályzat az adatok bevitelétől azok archiválásáig, vagy adott esetben a törlésig írja le az adatkezelés folyamatát. Az adatkezelő az adatkezelés teljes folyamata során a GDPR, és más vonatkozó jogszabályi rendelkezések alapján jár el.

II. A szabályzat hatálya:

Jelen adatkezelési szabályzat hatálya kiterjed az adatkezelővel szerződéses kapcsolatban álló valamennyi terapeutára, illetve azokra a szülőkre/gyámokra, akiknek gyermekeiről vizsgálati adatok keletkeznek, és az adatokat az őt vizsgáló terapeuta feltölti a LongiKid® vizsgálószoftver rendszerébe.

III. Alapfogalmak:

Jelen adatkezelési szabályzat vonatkozásában:

Adatok típusai

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 egy, vagy több tényező alapján azonosítható.

Genetikai adat: Egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

Biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását. Ilyen például az arckép vagy a daktiloszkópiai adat.

Egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

Adatkezelő személyek

Adatkezelő: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki/amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. Ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Adatfeldolgozó: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki/amely az adatkezelő nevében személyes adatokat kezel.

Az adatfeldolgozó korlátai:

- az adatkezelést érintő érdemi döntést nem hozhat,
- a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel,
- saját céljára adatfeldolgozást nem végezhet, továbbá
- a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni.

Kizárt adatkezelő: Olyan adatkezelő nem bízható meg, aki/amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységében érdekelt.

Írásbeli szerződés: Az adatkezelő és adatfeldolgozó között írásbeli szerződésnek kell fennállnia az adatfeldolgozásról, amelyben a fentieket szabályozni kell.

Címzett: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik félnek minősül-e.

Harmadik fél: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, aki/amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

Vállalkozás: Gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is.

Adatkezelési tevékenységek

Adatkezelés: A személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Az adatkezelés korlátozása: A tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

Profilalkotás: Személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

Álnevesítés: A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

Az érintett hozzájárulása: Az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

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.

Adatvédelmi hatásvizsgálat: Amennyiben az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

Adatvédelmi tisztviselő: Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor: a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat; b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél, ill. céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé; c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok különleges kategóriáinak (pl. faji vagy etnikai származásra, politikai véleményre, vallási meggyőződésre, stb.) és a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

Személyes adatok határokon átnyúló adatkezelése: a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint, vagy valószínűsíthetően jelentős mértékben érint érintetteket.

Kötelező erejű vállalati szabályok: A személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ.

Az információs társadalommal összefüggő szolgáltatás: szolgáltatás, amely az információs társadalom bármely szolgáltatása, azaz bármely, általában térítés ellenében, távolról (a felek egyidejű jelenléte nélkül), elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatás.

Adatfeldolgozás: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adaton végzik.

Adattovábbítás: Az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Nyilvánosságra hozatal: Az adat bárki számára történő hozzáférhetővé tétele.

Adattörlés: Az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.

Az anonimizálás, és álnevesítés folyamatát, az adatkezelés sajátosságaira tekintettel a dokumentum az alábbiakban részletezi.

Anonimizálás

A fentiek alapján az anonimizált adatok tekintetében már nem kell alkalmaznia a személyes adatok védelmére vonatkozó szabályokat. Ahogy a GDPR is rögzíti a Preambulumában (26):

Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható. Ez a rendelet ezért nem vonatkozik az ilyen anonim információk kezelésére, a statisztikai vagy kutatási célú adatkezelést is ideértve.

Fontos szempont és elvárás az anonimizációval kapcsolatban, hogy a kapcsolat ne legyen többé helyreállítható, azaz a természetes személy már nem azonosítható.

Álnevesítés

Az anonim adatra tehát már nem alkalmazandók a személyes adatok védelmére vonatkozó szabályok. Ezzel szemben az álnevesített adatok továbbra is a személyes adatok védelmére vonatkozó szabályok hatókörében maradnak. Az álnevesítés lényege, hogy a személyes adatok védelme során ez az adatok magas szintű védelmének egyik eszköze. A GDPR maga is ismeri és meghatározza az álnevesítés fogalmát és számos ponton ajánlja az adatkezelőknek az álnevesítés alkalmazását.

A Rendelet Preambuluma (28) szerint:

A személyes adatok álnevesítése csökkentheti az érintettek számára a kockázatokat, valamint segíthet az adatkezelőknek és az adatfeldolgozóknak abban, hogy az adatvédelmi kötelezettségeiknek megfeleljenek.

A GDPR alapján az álnevesítés (pszeudonimizáció) a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

A Rendelet az adatkezelők figyelmébe ajánlja az álnevesítést például:

- a beépített adatvédelem (25. cikk),
- az adatkezelés biztonsága (32. cikk),
- a magatartási kódexek (40. cikk)

IV. Az adatkezelés alapelvei.

A személyes adatok:

a.) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);

b.) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”);

c.) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”);

d) pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);

e.) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság”);

f.) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

Az adatkezelő felelős a fentiek megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

V. Az adatkezelés folyamata

A LongiKid® Vizsgálószoftverbe adatokat felvinni kizárólag a hozzáféréssel rendelkező terapeuták tudnak. A szülők a hozzájárulás megadásával ezen adatkezeléshez járulnak hozzá. Fontos, hogy a rendszer több ponton is biztosított.

- Invalid e-mail címről nem fogad regisztrációt, ellenőrzésre kerül az e-mail cím. Invalid e-mail címről történő regisztrációra nincs lehetőség, mert a terapeutákat meghívó admin minden email címet egyedileg ellenőriz, és kizárólag valós, ellenőrzött e-mail címről fogad el regisztrációt.
- Amennyiben nem valós regisztrációról történik belépési kísérlet, úgy azt a rendszer regisztrálja, és haladéktalanul értesítést küld a rendszer üzemeltetőjének. A terapeutákat minden esetben az admin(ok) hívja meg, így a terapeuta a nem valós e-mail címről érkező kéréseket, automatikusan elutasítja.
- Minden terapeuta kizárólag a saját maga által vizsgált gyermekek adatait látja, ezzel is erősítve az adatkezelés integritását, illetve bizalmas jellegét.
- A rendszer minden megkezdett vizsgálati folyamatot tárol. A megkezdett vizsgálatot a terapeutának a vizsgálat megkezdése után harminc nappal le kell zárnia. Minden folyamatban lévő, de még le nem zárt vizsgálatról a rendszer 20 nap elteltével értesítést küld a vizsgálatot felvevő terapeutának. Amennyiben a terapeuta a vizsgálatot az első figyelmeztetés után nem zárja le úgy a rendszer 25 nap elteltével újabb értesítést küld, a 28. napon ezen értesítést szükség esetén a rendszer megismétli. 30 nap elteltével a le nem zárt vizsgálatokhoz már kizárólag az admin férhet hozzá.

- Érintetti jogait a kiskorú képviselője (szülő, gyám) az adatkezelés teljes folyamata során gyakorolhatja.
- Adatok módosítására, javítására a vizsgálati adatokat a rendszerbe rögzítő terapeuta, valamint az admin jogosult, az érintetti joggyakorlás keretében megtett, előzetes kérés alapján, kizárólag indokolt esetben.

VI. Adatrögzítési, adattárolási időszak és cél a LongiKid® Vizsgálószoftverben

Adattulajdonos	**Adattípus**	**Adatkezelés, tárolás időtartama**	**Adatkezelés, tárolás célja**
Kiskorú	Beazonosításra szolgáló (pl. név)	A gyermek 18. életévének betöltéséig.	Operatív cél
Kiskorú	Demográfiai (pl. nem, életkor)	50 év	Statisztikai adatgyűjtés, folyamatfejlesztési célok
Kiskorú	Egészségügyi	50 év	Statisztikai adatgyűjtés, folyamatfejlesztési célok
Szülő	Beazonosításra szolgáló (pl. név)	A gyermek 18 éves koráig	Operatív cél
Szülő	Demográfiai (pl. nem, életkor)	50 év	Statisztikai adatgyűjtés, folyamatfejlesztési célok
Szülő	Egészségügyi	50 év	Statisztikai adatgyűjtés, folyamatfejlesztési célok

- Az elkészült vizsgálati eredmények a lezárás után PDF formátumban jelennek meg. A rendszer az elkészült vizsgálati dokumentációt a saját adatbázisában az egészségügyi jogszabályokban rögzítetteknek megfelelően 50 évig tárolja.
- Az adatkezelési időtartam befejeztével a LongiKid vizsgálószoftver rendszere automatikusan anonimizál, de az anonimizálást az adminok is meg tudják tenni az ő saját felületükről.

Az anonimizálás folyamata:

- A rendszer “anonimra” állítja a gyermek állapotát, Is anonim értéket true-ra állítja hogy tudjuk ki van anonimizálva.
- A rendszer archiválja a gyermeket, eltűnik a terapeuta felületéről (ugyanaz, mint a törlés gomb, terapeuta szempontból). Az archivált gyermek nem jelenik meg a terapeuta „gyermekek” menüjében, de a rendszerben továbbra is létezik
- A rendszer archiválja a gyermek vizsgálatait is, hogy ne jelenjen meg anonimizált gyermek vizsgálata a vizsgálatok fülön
- A rendszer átállítja a gyermek és a szülő nevét, valamint a gyermek születési helyét, tehát ezek a személyes adatok egy kóddá alakulnak, amiből nem visszafejthető az eredeti adat.
- A terapeuta az anonimizálást követően az anonimizált gyermekre vonatkozó adatokat beazonosítható módon már nem fogja látni.
- Az archivált gyermekekhez a terapeuta nem fér hozzá

VII. Adatvédelmi incidensek, illetve azok kezelése:

Az adatkezelő a LongiKid® Vizsgálószoftverében bekövetkezendő esetleges adatvédelmi incidensek során ugyanazon eljárásrendet követi, mint papír alapú, vagy egyéb más típusú elektronikus adatkezelési folyamatainak során.

Az adatvédelmi incidens fogalma és kezelésére vonatkozó előírások

Az adatvédelmi incidens a GDPR 4. cikk 12. pontja értelmében a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését (rendelkezésre állás sérülése), megváltoztatását (integritás sérülése), jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést (bizalmas jelleg sérülése) eredményezi.

Az adatvédelmi incidenst az adatkezelő köteles indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni az illetékes felügyeleti hatóságnak, 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. Amennyiben az incidens az adatfeldolgozó tevékenységi körén belül valósul meg, az adatfeldolgozó azt az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Ha az adatkezelő már észszerű mértékű bizonyossággal bír az incidens bekövetkeztéről, de még nem rendelkezik minden információval azzal kapcsolatban, érdemes – a 72 órás határidő betartása érdekében – a szakaszos bejelentés lehetőségével élni. Az ilyen jellegű bejelentések az annak pillanatában nem ismert információkkal később kiegészíthetők, helyesbíthetők, módosíthatók.

A Hatóság az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény (a továbbiakban: Eüsztv.) szerinti, elektronikus ügyintézésre kötelezett adatkezelők számára az adatvédelmi incidens bejelentéséhez formanyomtatványt biztosít (https://naih.hu/ugyinditas-formanyomtatvanyok), melyet az elektronikus ügyintézésre kötelezett adatkezelő, valamint az elektronikus ügyintézést önkéntesen vállaló adatkezelő, az Eüsztv.-ben meghatározott elektronikus úton pl. hivatali tárhelyen, vagy cégkapu, ügyfélkapu birtokában e-Papír szolgáltatáson keresztül nyújthat be.

Az ADATKEZELŐ az adatvédelmi incidenseiket a Hatóság Incidensbejelentő Rendszerén keresztül is bejelenthetik (https://naih.hu/adatvedelmi-incidensbejelento-rendszer).

Az incidensbejelentő portál célja kizárólag annak elősegítése, hogy az adatkezelők számára az incidensbejelentés folyamatát megkönnyítse, az panaszbenyújtásra nem szolgál.

Az elektronikus ügyintézésre nem kötelezett és azt önként sem vállaló adatkezelő postai úton a Hatóság levelezési címén (1363 Budapest, Pf. 9.), továbbá személyes átadással, személyazonosságának igazolását követően a Hatóság nyitvatartási idejében, előzetes időpont egyeztetése nélkül jelentheti be az adatvédelmi incidenst.

A Hatóság a bejelentés vizsgálata során kiemelt figyelmet fordít arra, hogy az tartalmazza-e legalább a GDPR 33. cikk (3) bekezdésében foglaltakat:

a.) az adatvédelmi incidens jellege, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b.) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó 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.

Az adatkezelő által vezetett adatvédelmi incidens-nyilvántartás szóban forgó incidensre vonatkozó részének másolata is a bejelentés (illetve adott esetben a tényállás tisztázó végzésre adott válasz) fontos eleme.

Az incidensekkel kapcsolatos kötelezettségek adatkezelő általi teljesítésének vizsgálatát a Hatóság az általános közigazgatási rendtartásról szóló 2016. évi CL. törvény (a továbbiakban: Ákr.) által szabályozott hatósági ellenőrzés keretében végzi. Ha a bejelentés, illetve annak kiegészítései nem tartalmaznak minden szükséges információt, a Hatóság a tényállás tisztázása érdekében felveszi a kapcsolatot az adatkezelővel. Amennyiben a Hatóság a hatósági ellenőrzés során a GDPR 33-34. cikkében foglalt kötelezettségek betartásával kapcsolatban jogsértést tár fel, hatósági eljárást indít; ellenkező esetben a hatósági ellenőrzést lezárja.

Az alábbiakban felsorolásra kerülnek a gyakorlatban tipikusan előforduló incidenstípusok, a Hatóság által az adatkezelőtől jellemzően elvárt kockázatcsökkentő intézkedésekkel együtt.

a.) A bejelentések legjelentősebb részét a **téves címzés miatti félrepostázások, illetve téves címzett részére küldött elektronikus levelek adták**. Az adatkezelőnek ilyenkor mindent meg kell tennie, hogy a téves címzett a birtokába jutott, személyes adatokat tartalmazó dokumentumot, üzenetet megsemmisítse/törölje. Postai küldemény esetén az adatkezelő válaszborítékkal együtt küldött újabb levélben is kérheti a téves címzettet a nem neki szóló küldemény visszaküldésére. Gondoskodnia kell továbbá az adatkezelőnek arról, hogy a tényleges címzett is megkapja az üzenetet, valamint, amennyiben például az érintett személyes adatok jellege alapján az incidens kockázatát valószínűsíthetően magasnak értékeli, tájékoztatnia kell az incidensről az érintettet. Az ilyen tájékoztatás másolatát is célszerű megküldeni a Hatóságnak. Hasonló magatartás várható el az adatkezelőtől akkor is, ha a címzettnek az egyébként neki szóló üzenettel együtt téves, személyes adatokat tartalmazó csatolmány is kiküldésre került, akár postán, akár elektronikus üzenetben.

b.) **E-mailek küldése több címzett részére olyan módon, hogy a címzettek nem a „Titkos másolat", hanem a „Másolatot kap" mezőben vannak felsorolva**, tehát a címzettek látják, jogosulatlanul megismerik egymás e-mail címeit. Ilyenkor az incidens által a személyes adatokra jelentett kockázat csökkentése érdekében mindenképpen elvárható az adatkezelőtől, hogy a címzettekkel ismét felvéve a kapcsolatot, őket felkérje az üzenet törlésére.

c.) **Az adatkezelőt ért hackertámadás következtében kiszivárgott adatok.** Ilyen esetben fontos az incidens által érintett adatok mihamarabbi azonosítása, az informatikai biztonsági rendszerek felülvizsgálata. Abban az esetben, ha az adatkezelőnek szakértelem hiányában nem sikerül azonosítani a támadás folyamatát, illetve részletesen feltárni az incidenshez vezető körülményeket, érdemes külső szakértőt felkérni. Amennyiben a támadás emberi tényező kihasználásával történt (pl. phising), az elhárítás folyamatából kihagyhatatlan a munkavállalók oktatása. Abban az esetben, ha informatikai hibából adódott a sérülékenység, a teljes rendszer felülvizsgálata lehet indokolt. Minden esetben elvárható az adatkezelő információbiztonsági szabályzatának felülvizsgálata.

d**.) Ellopott/elvesztett számítástechnikai eszközök, telefonok**. Ilyen esetekben kiemelt szereppel bír az is, hogy az adatkezelő az incidenst megelőzően megfelelő figyelmet biztosított-e eszközei védelmének (jelszó, titkosítás), mellyel megakadályozható, hogy az adott eszközön tárolt adatokat illetéktelen személyek megismerhessék. Távoli hozzáférés lehetősége esetén utólag is elképzelhető az adatok eszközről való törlése. Fontos, hogy az incidensről való tudomásszerzést követően az adatkezelő azonnal azonosítsa, hogy az adott kliens milyen adatokhoz, szerverekhez fért hozzá, és milyen jogosultság került kiosztásra számára, azok pedig azonnal kerüljenek megvonásra, az érintett szervereket, szolgáltatásokat vonják vissza, illetve változtassák meg azok hozzáféréseit.

Határon átnyúló adatkezeléssel kapcsolatos incidensek

A GDPR 56. cikke értelmében az adatkezelő vagy az adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye szerinti felügyeleti hatóság jogosult fő felügyeleti hatóságként eljárni az említett adatkezelő vagy az adatfeldolgozó által végzett határokon átnyúló adatkezelés tekintetében, a 60. cikk szerinti eljárással összhangban („one-stop-shop” mechanizmus).

Tehát a Hatóság eljárása határon átnyúló adatkezeléssel kapcsolatos incidenseknél attól függ, hogy az adatkezelő vagy az adatfeldolgozó tevékenységi központja Magyarországon található-e, vagy sem.

VIII. Az érintetti joggyakorlás biztosítása az adatkezelés folyamata során:

Az általános adatvédelmi rendelet[1] 57. cikk (1) bekezdésének f) pontja és 77. cikk (1) bekezdése alapján minden érintett jogosult arra, hogy panaszt tegyen a Hatóságnál, ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti az általános adatvédelmi rendeletet. A Hatóság gyakorlati tapasztalatai szerint ugyanakkor az adatkezelők[2] az esetek nagy részében együttműködnének az érintettekkel és maguktól helyreállítanák a jogszerű állapotot, ha konkrét kérelem érkezne részükről az általuk kifogásolt adatkezelés vonatkozásában.

A Hatóság ezért azt javasolja az érintett számára, hogy az ügyek gyorsabb és hatékonyabb intézése érdekében a panasz benyújtása előtt közvetlenül az adatkezelőkkel vegye fel a kapcsolatot, és éljen az alábbi érintetti jogaival.

Főszabály szerin minden érintett kérelmezheti az adott adatkezelőnél:

- személyes adataihoz való hozzáférését,
- személyes adatainak helyesbítését,
- személyes adatainak törlését,
- az adott adatkezelés korlátozását,
- személyes adatainak hordozhatóságát,
- továbbá tiltakozhat személyes adatai kezelése ellen.

Bármely érintetti jog gyakorlására irányuló kérelemről is legyen szó, az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül köteles tájékoztatni érintettet a kérelem nyomán hozott intézkedéseiről. Szükség esetén – figyelembe véve a

kérelem összetettségét és a kérelmek számát – ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról azonban az adatkezelő köteles a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatni az érintettet.

Ha az adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül, akkor is köteles tájékoztatni érintettet az intézkedés elmaradásának okairól, valamint arról, hogy érintett panaszt nyújthat be a Hatósághoz és élhet bírósági jogorvoslati jogával, a lakó- vagy tartózkodási helye szerint illetékes törvényszék előtt (a törvényszékek elérhetőségéről az alábbi linken tájékozódhat: http://birosag.hu/torvenyszekek).

Ha az adatkezelőnek megalapozott kétségei vannak az érintett személyazonosságával kapcsolatban valamely érintetti jogának gyakorlására irányuló kérelme benyújtása során, az adatkezelő további, a személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti az érintettől. Amennyiben ugyanis az adatkezelő bizonyítja, hogy nem áll módjában az érintettet azonosítani, megtagadhatja az érintetti jog gyakorlására irányuló kérelem teljesítését.

Az érintetti kérelmekre vonatkozó tájékoztatás és intézkedés főszabály szerint díjmentes. Ha azonban a kérelem egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre észszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása azonban az adatkezelőt terheli.

Az általános adatvédelmi rendelet 37. cikke meghatározza, hogy mely esetekben jelöl ki az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt. A Hatóság javasolja, hogy ezeknél az adatkezelőknél vagy adatfeldolgozóknál érintett vegye igénybe az adatvédelmi tisztviselők közreműködését.

Amennyiben az adatkezelő a fenti határidőket is figyelembe véve igazolható módon nem teljesíti az érintett valamely kérelmét, a Hatóság – panasz alapján – kivizsgálja az ügyet.

A személyes adataihoz való hozzáférés joga

Ezen joga alapján érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adataihoz és az általános adatvédelmi rendeletben felsorolt információkhoz (például az adatkezelés célja, jogalapja, a személyes adatok címzettjei vagy a címzettek kategóriái, harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás esetén az azzal kapcsolatos tudnivalók; az adatkezelés időtartama, vagy annak szempontjai, az érintett jogai, jogorvoslati lehetőségei, az adatszolgáltatás elmaradásának következményei) hozzáférést kapjon.

Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát köteles az érintett rendelkezésére bocsátani. A Hatóság felhívja azonban a figyelmét arra, hogy a kért további másolatokért az adatkezelő adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel, továbbá a másolat igénylésére vonatkozó jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait.

A személyes adatai helyesbítéséhez való joga

A helyesbítéshez való joga alapján érintett egyrészt jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse az érintettre vonatkozó pontatlan személyes adatokat, másrészt jogosult arra, hogy kérje a hiányos személyes adatainak kiegészítését.

A személyes adatai törléséhez és „elfeledtetéshez” való joga

Főszabály szerint törléshez való joga alapján érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje az érintett személyes adatait, az adatkezelő pedig köteles arra, hogy indokolatlan késedelem nélkül törölje azokat, meghatározott feltételek esetén.

Az „elfeledtetéshez” való jog a törléshez való jog online környezetbe történő kiterjesztését jelenti, amely alapján, ha az adatkezelő nyilvánosságra hozta az érintett személyes adatát, és azt törölni köteles, köteles megtenni észszerűen elvárható lépéseket annak érdekében, hogy tájékoztassa az érintett személyes adatait kezelő adatkezelőket, hogy érintett kérelmezte a személyes adataira mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Ezen érintetti joggal kapcsolatban fontos azonban megjegyezni, hogy a személyes adatok törlésére és „elfeledtetésére” nincs lehetőség, amennyiben az általános adatvédelmi rendelet 17. cikk (3) bekezdésében meghatározott esetek valamelyike fennáll.

A személyes adatai kezelésének korlátozásához való joga

Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza, közismertebb nevén zárolja az adatkezelést, ha az alábbi feltételek valamelyike teljesül:

- Az érintett vitatja a személyes adatai pontosságát. Ebben az esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze ezen személyes adatai pontosságát;
- Az adatkezelés jogellenes, és érintett ellenzi a személyes adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- Az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- Az érintett tiltakozott az adatkezelés ellen. Ebben az esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

A személyes adatai hordozhatóságához való joga

Az érintett ezen joga alapján jogosult arra, hogy a rá vonatkozó, és egy adatkezelő rendelkezésére bocsátott személyes adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket a személyes adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta. Ezt a jogát akkor gyakorolhatja, ha az adatkezelés hozzájáruláson vagy szerződésen alapul és az adatkezelés automatizált módon történik.

A személyes adatai kezelése elleni tiltakozási joga

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen, ha a személyes adatai kezelésére az adatkezelő jogos érdeke, vagy a közhatalmi jellege miatt kerül sor. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha érintett tiltakozik a személyes adatai közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatai a továbbiakban e célból nem kezeli.

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet)

Az általános adatvédelmi rendelet 4. cikk 7. pontja alapján: „adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.”

Az általános adatvédelmi rendelet 23. cikke tartalmazza azokat a rendelkezéseket, amelyek alapján korlátozhatóak az egyes érintetti jogok.

Jogorvoslati záradék:

Az érintettnek amennyiben az adatkezeléssel kapcsolatos bármely folyamatot sérelmesnek érzi joga van a jogorvoslat igénybevételéhez. Vélt jogsérelem esetén az érintett az adatkezelőtől kérheti a sérelemmel érintett helyzet orvoslását. Amennyiben ilyen kérés érkezik, azt az adatkezelő minden esetben köteles megvizsgálni, és a vizsgálat eredményéről az érintettet minden esetben írásban tájékoztatni. Az írásban érkezett beadványok elbírálására minden esetben haladéktalanul, de legkésőbb a beadvány beérkezésétől számított harminc napon belül megtörténik.

Amennyiben az érintett a kapott tájékoztatással nem elégedett, azt jogilag nem tartja helytállónak, úgy panaszával a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (NAIH) fordulhat

Levelezési cím:

- ugyfelszolgalat@naih.hu
- 1363 Budapest, Pf.: 9.

Cím: 1055 Budapest, Falk Miksa utca 9-11

Amennyiben jónak látja, a területileg illetékes bírósághoz is fordulhat. Az adatkezelő esetében a területileg illetékes bíróság a Budapest, II. és III. kerületi Bíróság.

Elérhetőségek:

- Cím: 1036 Budapest, Lajos utca 48-66.
- Levelezési cím: 1300 Budapest Pf.: 22.
- Központi telefonszám: +36 (1) 430-6500
- E-mail: obuda@birosag.hu