Belső adatvédelmi szabályzat

CINE-MIS Nonprofit Kft

elfogadva az 5. számú ügyvezetői utasítással

2021.07.01.

1 Általános rendelkezések

1.1 Személyi Hatály

A jelen szabályzat hatálya kiterjed a **CINE-MIS Nonprofit Kft** (3525 Miskolc, Kossuth Lajos utca 11; *cjsz:* 05-09-016617; a továbbiakban: „**adatkezelő**") valamennyi munkavállalójára, valamint az adatkezelővel munkavégzésre irányuló egyéb jogviszonyban álló – személyes adatok kezelésével kapcsolatos tevékenységet végző – személyre (a továbbiakban: „**Munkatársak**"). A Munkatársak munkájuk végzése során szükségszerűen találkoznak a CINE-MIS Nonprofit Kft; mint adatkezelő által kezelt személyes adatokkal. A személyes adatokat a feladataik teljesítéséhez kapcsolódóan rögzítik, tárolják, módosítják, továbbítják, azaz adatkezelési műveleteket végeznek az adatkezelő nevében. Az adatkezelő Munkatársai kötelesek a jelen adatvédelmi szabályzat rendelkezéseinek betartására és betartatására.

1.2 Tárgyi hatály

A jelen szabályzat tárgya az Európai Parlament és a Tanács (EU) 2016/679 számú általános adatvédelmi rendelete (General Data Protection Regulation; a továbbiakban: **GDPR**) és a vonatkozó egyéb jogszabályoknak való megfelelés érdekében a személyes adatoknak az adatkezelő által vagy az adatkezelő nevében végzett kezelése tekintetében az adatkezelői hatáskörök és felelősség szabályozása, ehhez kapcsolódóan megfelelő és hatékony technikai és szervezési intézkedések rögzítése, melyek által igazolható, hogy az adatkezelési tevékenységek jogszerűek, és az alkalmazott intézkedések hatékonysága az előírásoknak megfelelő szintű.

A jelen szabályzat célja a személyes adatok jogszerű és szakszerű kezelésének biztosításához szükséges információk rendelkezésre bocsátása és az ezzel összefüggő belső eljárási szabályok meghatározása.

1.3 Időbeli hatály

A szabályzat [2021]. év [07] hó [01] napjától annak visszavonásig hatályos.

1.4 A szabályzat karbantartása, közzététele

A szabályzat kidolgozásáért, karbantartásáért és közzétételéért a belső adatvédelmi felelős és az adatkezelő vezetősége felelős, végrehajtásáért a szabályzat egyes rendelkezéseinek címzettjei felelősek.

A szabályzat felülvizsgálata, karbantartása minden naptári év december 31. napjáig esedékes, valamint soron kívül olyan jogszabályváltozás vagy felügyeleti hatóság ellenőrzése esetén, mely a szabályzatban foglalt rendelkezéseket érinti.

1.5 Szankciók

A GDPR előírásainak megsértése esetén az adatkezelőre pénzbírság szabható ki, amelynek maximális mértéke 20 millió Euró, vagy az adatkezelő éves bevételének 4%-a. Ezen túlmenően szabálysértés esetén az érintett kártérítési és sérelemdíj iránti igényt is érvényesíthet az adatkezelővel szemben.

Adatvédelmi incidens - például adatvesztés, adatokkal való bármely visszaélés vagy hacker támadás esetén - a jogsértést, amennyiben az kockázattal jár az érintettekre nézve, nyilvánosságra kell hozni, valamint a NAIH-nak és – amennyiben a kockázat mértéke magas – az érintetteknek jelenteni kell. Tekintettel kell lenni tehát arra, hogy minden adatvédelmi jogsértés nyilvánosságra kerülhet, és az adatkezelő jó hírnevének jelentős csorbulásához vezethet.

Az adatkezelő fenntartja a jogot arra, hogy a jelen Adatvédelmi belső szabályzat megsértése esetén munka-, polgári- vagy büntetőjogi lépéseket tegyen, ideértve a jogviszony azonnali hatályú felmondását és kártérítés vagy - az adatkezelő jó hírnevének sérülése esetén - sérelemdíj érvényesítését a jelen szabályzat megszegőjével szemben.

1.6 Személyes adatokkal kapcsolatos fogalmak

- **Adatfeldolgozás:** az adatfeldolgozás során az adatkezelő (azaz a CINE-MIS Nonprofit Kft.) megbízásában eljáró valamely szerv (pl. szolgáltató) az adatkezelő (CINE-MIS Nonprofit Kft) személyes adatait kezeli. Az adatfeldolgozó az adatokat az adatkezelő utasításai alapján kezeli. Az adatok felett továbbra is az adatkezelő rendelkezik. Az adatfeldolgozás feltételezi, hogy a felek a jogszabályban előírt minimális tartalommal írásbeli adatfeldolgozási szerződést kötöttek.
- **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 adatok mindennapi kezelése során külön-külön ellenőrizni kell, hogy a konkrét adatkezelés – a jelen szabályzat rendelkezéseire is tekintettel – megengedett-e.
- **Adatkezelő:** az a természetes vagy jogi személy, aki a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. A jelen szabályzat alkalmazásában adatkezelő a CINE-MIS Nonprofit Kft.
- **Adatkezelés korlátozása**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.
- **Adattovábbítás**: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.
- **Adattörlés**: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.
- **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.
- **Érintett:** valamennyi azonosított vagy azonosítható természetes személy, akinek a személyes adatait az adatkezelő nevében a Munkatársak kezelik. Akkor tekinthető egy személy azonosíthatónak, ha pl. egyes adatok összekapcsolásával az adott személy beazonosítására valaki képes lenne. Érintettnek minősülnek például az adatkezelő üzleti partnereinek képviselői, vagy az alkalmazottak is; utóbbi fogalom magában foglalja az álláshirdetésre pályázókat, közfoglalkoztatottakat, gyakornokokat stb.
- **GDPR:** A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendelet (Általános Adatvédelmi Rendelet).
- **Harmadik fél:** harmadik félnek minősül az adatkezelésért felelős szerven kívül mindenki, aki nem azonos az érintettel. Nem minősülnek harmadik félnek az adatfeldolgozók (vállalkozók), akik jogszabály szerint az adatkezelőhöz tartoznak, valamint azok a személyek, akik az adatkezelő vagy az adatfeldolgozó közvetlen felelősségi körén belül jogosultak az adatok kezelésére. Harmadik félnek minősülnek rendszerint más vállalatok.
- **Honlap**: www.cinemis.hu
- **Infotv.:** az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény.
- **Jelölt:** akinek szándéka van az adatkezelővel bármilyen munkavégzésre irányuló jogviszonyt (munkaviszony, közalkalmazotti, közszolgálati tisztviselői, közfoglalkoztatotti jogviszony stb.) létesíteni. A Jelölt egyben érintettnek is minősül.
- **Különleges kategóriába tartozó személyes adatok:** minden olyan személyes adat, amely az egészségi állapotra (pl. orvosi diagnózis, szemüveges személyről készített kép), a faji vagy etnikai származásra (pl. állampolgárság, bőrszín), a vallási vagy világnézeti meggyőződésre utal, valamint a biometrikus adatok (pl. ujjlenyomat), a genetikai adatok, a politikai véleményre, a szakszervezeti tagságra, a szexuális életre vagy a szexuális beállítottságra utaló személyes adatok.
- **NAIH:** a Nemzeti Adatvédelmi és Információszabadság Hatóság, amely az adatkezelő tekintetében a GDPR szerinti érintett felügyeleti hatóságnak minősül.

- **Munkatársak:** az adatkezelő azon munkavállalói, megbízottai és mindazon, az adatkezelővel más jogviszonyban álló személyek, akik az adatkezelőnél végzett tevékenységük során az adatkezelő személyes adatokat tartalmazó adatbázisaihoz hozzáféréssel rendelkeznek, vagy bármely egyéb okból kifolyólag az adatkezelőnél kifejtett tevékenységükkel kapcsolatban személyes adatok birtokába jutnak.
- **Személyes adatok:** az Érintettre vonatkozó bármely információ, amennyiben az érintett azonosított vagy azonosítható. A személyes adatok vonatkozhatnak személyes körülményekre (pl. név, cím, családi állapot, gyerekek, hobbik, bizonyítványok, foglalkozás stb) vagy tárgyi körülményekre (pl. bevétel, vagyon, tulajdon, autó, biztosítások, e-mailek írása, bankszámlaszám stb).
- **Tiltakozás:** az Érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

2 Beépített és alapértelmezett adatvédelem szabályai társaságunknál / intézményünknél

Az adatkezelő a GDPR-ban meghatározott tájékoztatások, nyilvántartások és szabályozások megalkotásán túl az alábbi technikai és szervezési intézkedéseket rendeli el a beépített és alapértelmezett adatvédelem elvének való megfelelés érdekében:

a) Adatvédelmi szervezet: Az adatkezelő a GDPR rendeletnek való megfelelés érdekében külön definiált, önálló adatvédelmi szervezetet működtet, mely az adatvédelmi tisztviselő, a belső adatvédelmi felelős, a szakterületi adatvédelmi felelősök, valamint a helyi adatvédelmi felelősökből áll. Az adatvédelmi szervezet élén az adatkezelő vezetője áll. Az adatvédelmi szervezettel kapcsolatos rendelkezéseket a 10. pont tartalmaz.

b) Rögzített adatvédelmi feladat- és hatáskörök: Az adatkezelő a GDPR-nak való megfelelés érdekében minden egyes adatvédelemmel kapcsolatos jogszabályi kötelezettség, illetve jelen szabályzatban rögzített adatvédelemmel kapcsolatos vállalati intézkedés tekintetében meghatározza és dedikálja a feladat- és hatásköröket mind a végrehajtás, mind pedig a végrehajtás ellenőrzése tekintetében.

c) Adatvédelmi tudatosságot erősítő oktatások: Az adatkezelő a GDPR-nak való megfelelés érdekében előre meghatározott rend (időbeli ütemezés, tematika) szerint az adatvédelmi tudatosságot erősítő belső oktatásokat szervez.

d) Titoktartási klauzulák és titoktartási nyilatkozatok: Az adatkezelő személyes adatok kezelését végző munkatársai tekintetében a munkaszerződés / kinevezés, vagy egyéb szerződés / okirat tartalmazza, hogy a titoktartási kötelezettség a jogviszonyból származó lényeges kötelezettség. A munkaköri leírás rögzíti, hogy a Munkatárs felelős az általa kezelt személyes adatok megfelelő biztonsága érdekében, az adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztésének elkerülése érdekében minden adott helyzetben általában elvárhatót megtenni, az adatokat bizalmasan kezelni.

e) Álnevesítés: [***]

f) Adatbiztonsági intézkedések: Informatikai biztonsági szabályzat szerint / [***].

g) Évenkénti felülvizsgálat: A belső adatvédelmi felelős évente felülvizsgálja az adatkezelési (jog) és adatbiztonsági (IT) tevékenységét. A felülvizsgálat lefolytatásával külső vállalkozás is megbízható. A vizsgálat eredménye egy jelentés, amely összegzi az adatvédelmi szempontból aggályos gyakorlatot és megoldási javaslatokat tartalmaz a GDPR előírásainak való megfelelés érdekében.

3 Adatvédelmi alapelvek érvényesülése a gyakorlatban

A GDPR és az Infotv; valamint a NAIH gyakorlata megkívánja az adatkezelőktől, hogy bizonyos alapelveket betartsanak. Ezek az alábbiak:

3.1 Jogszerűség: A személyes adatok kezelése csak abban az esetben megengedett, ha a GDPR-ban foglalt alábbi indokok (jogalapok) valamelyike fennáll:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek. Jogos érdeken alapuló adatkezelés megkezdését megelőzően érdekmérlegelési tesztet kell végezni. Az érdekmérlegelési tesztek elvégzése a belső adatvédelmi felelős feladata, aki, szükség esetén egyeztet az adatvédelmi tisztviselővel. A belső adatvédelmi felelőst segíti az érintett terület vezetője. A jogos érdek, mint jogalap nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre (!).

Biztosítani kell, hogy a fenti jogalapok valamelyike az adatkezelés teljes időtartama alatt fennálljon. Amennyiben a jogalap már nem áll fenn, mert például az érintett visszavonta a hozzájárulását, és az adatok kezelésére nincs más jogalap, úgy az adatok további kezelése jogellenes, ezért az adatokat törölni kell valamennyi nyilvántartásunkból, ideértve az adatok papír alapú, vagy elektronikus tárolását.

Példák:

- a) eset: amennyiben egy, az adatkezelőhöz pályázó Jelölt ehhez külön hozzájárul, úgy önéletrajzát sikertelen jelentkezést követően az adatkezelő adatbázisában tovább tároljuk és felhasználjuk további álláslehetőségekről való értesítés céljából.
- b) eset: kinevezések, munkaszerződések, magánszemélyekkel kötött szerződések teljesítéséhez szükséges adatkezelés, ha a szerződés közvetlenül az adatkezelő és az Érintett között jött létre (pl. munkabérek átutalása, ehhez szükséges bankszámlaadatok rögzítése, tárolása).
- c) eset: az adatkezelő alkalmazottainak adatait az adatkezelő-re vonatkozó jogi kötelezettségek teljesítése érdekében továbbítjuk az adóhatóságnak (pl. a biztosítási jogviszony létrejöttének bejelentésekor).
- d) eset: kivételesen érvényesül, pl. amikor az alkalmazottak baleseti kapcsolattartóinak adatait tároljuk.
- e) eset: akkor valósul meg, amikor az adatkezelésnek szükségesnek kell lennie valamely közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához.
- f) eset: üzleti partnereink, alvállalkozóink kapcsolattartóinak adatait (név, beosztás, munkáltató, e-mail-cím) jogos érdekünk alapján kezeljük, hiszen nem kérünk be az érintettől külön hozzájárulást (ezért az a) eset nem jön szóba, és magát az üzleti szerződést sem a kapcsolattartóval kötjük meg (ezért a b) eset sem jön szóba). Jogos érdekünk abban áll, hogy az üzleti szerződéseik teljesítése során biztosított legyen a mindennapi, akadálymentes és gyorsan megvalósítható kommunikáció.

3.2 **Célhoz kötöttség:** A személyes adatok kezelése csak abból a célból lehetséges, amely miatt az adatok gyűjtésére sor került. Már az adatok gyűjtése során meg kell határozni és dokumentálni kell, hogy az adatokat később milyen célokra használjuk fel. Amennyiben az adatkezelés eredeti célja teljesült, úgy az adatokat törölni kell, kivéve, ha az eredeti céltól eltérő cél érdekében történő adatkezeléshez bármely jogalappal rendelkezünk (pl. új hozzájárulást kértünk, vagy az adatkezelő jogos érdeke indokolja az adatkezelést).

Az adatok konkrét cél nélküli, „készletre" történő tárolása nem jogszerű. Ha egy adatról vagy adatbázisról nem tudjuk, hogy azok milyen célból kerültek gyűjtésre, vagy mi a tárolás vagy felhasználás konkrét célja, akkor ezen adatok kezelése minden bizonnyal jogellenes, ezért az ilyen adatkezelést észlelő Munkatárs köteles a belső adatvédelmi felelőssel egyeztetni a szükséges intézkedések meghatározása érdekében.

Példa: további megkeresések céljából nem szabad felhasználni az egy konkrét álláshirdetésre beérkezett önéletrajzokat, ha a további megkeresésekhez a jelölt nem járult külön hozzá.

3.3 **Adattakarékosság és korlátozott tárolhatóság:** A lehető legkevesebb személyes adatot szabad kezelni és a szükségtelen vagy szükségtelenné váló adatokat a lehető leggyorsabban törölni kell. Ebből adódóan minden adatgyűjtés során ügyelni kell arra, hogy csak az adatkezelés meghatározott célja érdekében ténylegesen szükséges adatokat kérjük el az érintettektől.

Példa: az alkalmazottak adatainak kezelése körében, a baleseti kapcsolattartóra vonatkozó adatok tekintetében, ha az alkalmazott mobiltelefonszámot adott meg (tehát tipikusan egy személyhez tartozik az adott telefonszám), akkor elegendő magának a mobiltelefonszámnak a rögzítése, további személyes adatokra (pl. név és lakcím megadása) nincs szükség.

Szintén az adattakarékossággal van összefüggésben, hogy az adatokat lehetőség szerint névtelenül vagy álnevesítve kell kezelni. Névtelen felhasználásról akkor beszélhetünk, ha az adatok alapján semmilyen következtetés nem vonható le az érintettel kapcsolatban. Az anonimizálás előnye, hogy a személyes vonatkozás hiányában a GDPR már nem alkalmazandó. Álnevesítésről akkor beszélünk, ha az információt az érintettel összekötő további információk csak korlátozottan hozzáférhetők, és így az információ címzettje nem tudja, hogy az információ kire vonatkozik. Az álnevesítés esetén a GDPR alkalmazandó, de nagyon előnyös megoldásnak tekinthető az egyének védelme szempontjából.

Példa: bizonyos, a saját alkalmazottakkal kapcsolatban szolgáltatásokat végző külső partnereknek elegendő lehet csak az alkalmazott törzsszámát, vagy más azonosítószámát továbbítani, a legtöbb esetben ezen szolgáltatóknak nincs szükségük arra, hogy az alkalmazott nevét (és egyéb adatait) is ismerjék.

3.4 **Átláthatóság:** A GDPR értelmében a személyes adatok kezelésének módja az érintett számára átlátható kell, hogy legyen. A személyes adatok gyűjtése során az érintettet oly módon kell tájékoztatni a személyes adatainak tervezett kezeléséről, hogy az számára nyomon követhető legyen. Az adatgyűjtés időpontjában ezért az érintettet tájékoztatni kell a GDPR-ban meghatározott körülményekről (pl. kezelt adatok köre, adatkezelés célja, jogalapja stb.)

Abban az esetben, ha az adatokat nem közvetlenül az érintettől szereztük meg, az érintettet tájékoztatni kell az adatok eredetéről is. Hozzájárulás esetén az érintettet tájékoztatni kell a hozzájárulása önkéntes jellegéről, a pontos tartalmáról, valamint visszavonási jogáról.

3.5 **Pontosság és naprakészség:** Biztosítani kell, hogy a személyes adatok mindig helyesek, teljes körűek és naprakészek legyenek. A pontatlan adatokat haladéktalanul törölni vagy helyesbíteni kell.

3.6 **Integritás és bizalmas jelleg:** az adatkezelő által kezelt személyes adatokat a megfelelő technikai és szervezési intézkedések alkalmazásával minden időben védeni kell, különösen az elvesztésükkel, jogosulatlan hozzáféréssel vagy jogosulatlan módosításokkal szemben.

A különböző adatbázisokban eltérő jogalap mellett és célból elektronikusan kezelt adatállományokat az érintett hozzájárulása hiányában tilos egymással összekapcsolni.

4 Hozzájárulás

4.1 Hozzájárulással szemben támasztott követelmények

Abban az esetben, ha a személyes adatok kezelése hozzájáruláson alapul, az alábbi követelményeket kell figyelembe venni. Amennyiben a lenti követelmények nem teljesülnek, úgy érvényes hozzájárulás nem áll rendelkezésre és az adatok kezelése jogellenesnek minősül.

- **Önkéntesség:** önkéntességtől nem beszélhetünk akkor, ha
  - szerződés megkötését valamilyen eltérő célú hozzájárulás megadásától tesszük függővé,
  - az adatkezelő és a hozzájárulást adó személy között nincs egyensúly (ezért a hozzájárulás, mint jogalap a munkaviszonyban pl. csak kivételes esetben jöhet szóba),
  - különböző adatkezelési folyamatokhoz az érintett nem adott külön hozzájárulást.
- **Specifikus/bizonyos esetre vonatkozik:** A hozzájárulás csak konkrét esetekre vonatkozhat és az adatkezelés minden célját külön kell ismertetni. A különböző célú adatkezeléseket külön-külön és adott esetben külön hozzájáruló nyilatkozatokkal kell lefedni; általános hozzájárulás nem adható.
- **Visszavonható:** Az Érintett személy a hozzájárulását bármikor visszavonhatja. A visszavonásnak ugyanolyan könnyen kell történnie, mint a hozzájárulás megadásának. A hozzájárulás megadásakor fel kell hívni az érintett figyelmét az őt megillető visszavonás jogára. A mindenkor fennálló visszavonási jogra tehát már a hozzájárulás megadása előtt nyomatékosan fel kell hívni a figyelmet. A visszavonás beérkezésének időpontjától kezdve a személyes adatok felhasználása már nem megengedett. Az adatkezelés további feltételeit (pl., hogy hozzájárulás hiányában fennáll-e valamilyen eltérő jogalap, adott esetben jogos érdek az adatkezelésre), minden esetben gondosan meg kell vizsgálni.
- **Tájékoztatás alapján**: Az Érintettnek tisztában kell lennie azzal, hogy mihez járul hozzá. Az Érintettet ezért a hozzájárulás megadása előtt tájékoztatni kell a jelen szabályzatban rögzítettek szerint. Ez a tájékoztatás egyben meghatározza az adatkezelés kereteit is: a hozzájárulás nem terjed ki azon adatkezelési folyamatokra, amelyekről az érintett nem kapott tájékoztatást. A megfogalmazásnak világosnak, könnyen érthetőnek és pontosnak kell lennie. Ebből a célból a Munkatársak rendelkezésére állnak különböző típusú tájékoztatók, illetve sablon tájékoztató.
- **Félreérthetetlen jelleg:** A hozzájárulás megadásához „egyértelmű megerősítő cselekedet" szükséges. Ilyennek minősül, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet („opt-in"). A hallgatólagos elfogadás, a különböző nyilatkozatokban előre bejelölt négyzet nem minősül hozzájárulásnak, ezért, az ilyen módon beszerzett „hozzájárulás" alapján folytatott adatkezelés jogellenes lesz.

4.2 Hozzájárulások dokumentációja és igazolása

Hozzájáruláson alapuló adatkezelés esetében a hozzájárulást kétség esetén az adatkezelőnek kell bizonyítania, ezért a hozzájárulást akként kell beszerezni, hogy annak ténye hitelt érdemlően bizonyítható legyen.

- Az **e-mailben adott** hozzájárulásokat mindig a megfelelő nyilvántartásban kell elmenteni, hogy kétség esetén a hozzájárulás meglétét az adatkezelő bizonyítani tudja.
- Az **írásbeli hozzájárulások**at papírformátumban vagy digitalizálva kell archiválni, és azok tárolására fenti, e-mailes hozzájárulásnál leírtak irányadók.
- A **hozzájárulás visszavonását** a hozzájárulás megadásával egyező módon kell dokumentálni. Biztosítani kell, hogy a visszavonás beérkezését követően az érintett adatainak kezelésére és tárolására csak a megengedett mértékben kerüljön sor (tehát csak akkor, ha az adatkezelésnek van a hozzájáruláson kívül más jogalapja is).
- A hozzájárulások megőrzési ideje 10 év.

4.3 Hozzájárulás visszavonhatósága

Az Érintett a hozzájáruláson alapuló adatkezelés esetén jogosult a hozzájárulását bármikor visszavonni, amely azonban nem érinti a visszavonás előtti adatkezelés jogszerűségét. Erről minden esetben tájékoztatni kell az Érintettet (a jelen szabályzat szerinti űrlapok, illetve az adatkezelő által rendszeresített sablon tájékoztatók ezt tartalmazzák, ugyanakkor, ha a tájékoztatás szóban – pl. telefonon – hangzik el, úgy a megadott tájékoztatásban ennek is el kell hangoznia).

4.4 Kiskorúakra vonatkozó adatkezelések

A 16. életévét be nem töltött kiskorú Érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez szükséges a törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása.

A 16. életévét betöltött kiskorú Érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez nem szükséges törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása.

4.5 Hozzájárulás kétségessége

Amennyiben kétséges, hogy az Érintett a hozzájárulását az adatkezeléshez megadta-e, úgy lehetőség szerint az érintettel személyesen tisztázni kell, hogy hozzájárulását az adatkezeléshez megadta-e. Amennyiben ez nem lehetséges, vagy a hozzájárulás továbbra is kétséges, úgy azt kell vélelmezni, hogy az Érintett a hozzájárulását nem adta meg, ezért – más jogalap hiányában – az adatokat törölni kel, egyúttal tájékoztatni kell a belső adatvédelmi felelőst. Jogi jellegű, vagy értelmezésbeli kérdés esetén a belső adatvédelmi felelőshöz kell fordulni.

5 Tájékoztatás

5.1 Tájékoztatással szemben támasztott követelmények

Habár az adatkezelő által alkalmazott sablon tájékoztatók tartalmazzák a kötelező elemeket és megfelelnek a velük szemben tájékoztatott követelményeknek, lehetnek olyan esetek, amikor egyedi tájékoztatót kell megszövegezni, vagy a tájékoztatást szóban kell megadni. Ebből a célból fontos, hogy a Munkatársak tisztában legyenek az adatvédelmi tájékoztatás alapvető követelményeivel.

5.1.1 A tájékoztatást **tömör, átlátható, érthető és könnyen hozzáférhető** formában kell megfogalmazni.

5.1.2 Mit kell tartalmaznia a tájékoztatásnak a GDPR szerint?

- Az adatkezelő és képviselője neve és elérhetősége.
- Az adatvédelmi tisztviselő elérhetőségei.
- Az adatkezelés célja és jogalapja.
- Érdekmérlegelésen alapuló jogalap esetén a jogos érdekek megnevezése.
- Adattovábbítás esetén a személyes adatok címzettjei, illetve a címzettek kategóriái, harmadik országba történő adattovábbítással kapcsolatos információk, garanciák.
- Adatok tárolásának időtartama, vagy (ha konkrét időtartam meghatározása nem lehetséges) az időtartam meghatározásának szempontjai.
- Az Érintett jogai (ideértve a hozzáféréshez, helyesbítéshez, törléshez, korlátozáshoz, tiltakozáshoz, adathordozhatósághoz való jogot, továbbá a hozzájárulás visszavonásához való jogot, amely nem érinti a visszavonás előtti adatkezelés jogszerűségét, valamint panasz benyújtásának joga a hatósághoz).
- Annak ténye, ha a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul, vagy szerződés kötésének előfeltétele, valamint tájékoztatás arról, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása.
- Automatizált döntéshozatallal, profilalkotással kapcsolatos információ (az alkalmazott logikára és arra vonatkozó információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír).

- Ha az adatokat nem az érintettektől szerezték meg, akkor a tájékoztatásban szerepelnie kell az adatok forrásának, valamint annak is, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

5.1.3 Mikor kell megtenni a tájékoztatást?

- Ha az Érintettől származik az adat: az adatfelvételkor.
- Ha nem az érintettől származik az adat: a tájékoztatást a megszerzéstől számított ésszerű határidőn belül, legfeljebb egy hónapon belül.
- Amennyiben az adatkezelés kapcsolattartási célú, úgy az első kapcsolatfelvétel alkalmával.
- Ha az adatkezelő a személyes adatokon az eredeti céltól eltérő célból további adatkezelést kíván végezni, ezt megelőzően új tájékoztatást kell adnia az Érintetteknek.

5.1.4 Mikor mellőzhető a tájékoztatás?

- Ha az Érintett már rendelkezik az információkkal (a bizonyítás az adatkezelő felelőssége).
- Ha nem az Érintettől származnak az adatok és

– a tájékoztatás megtétele lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, vagy

– jogszabály által elrendelt adatkezelés esetén, vagy ha jogszabály által előírt szakmai vagy egyéb titoktartási kötelezettség alapján a személyes adatoknak bizalmasnak kell maradnia.

5.2 AZ ADATKEZELŐ által alkalmazott tájékoztatás minták

Különböző tájékoztató minták állnak az adatkezelő rendelkezésére a különböző típusú adatkezelések vonatkozásában. Ezek felhasználásáról minden esetben egyeztetni kell az belső adatvédelmi felelőssel, illetve – kétség esetén – az adatvédelmi tisztviselővel.

6 Adattovábbítás

Adatok harmadik felek részére történő továbbítása csak abban az esetben megengedett, ha a továbbításhoz megfelelő jogalap áll rendelkezésre.

Adattovábbítás szempontjából az alábbi eseteket kell megkülönböztetni:

a) adattovábbítás harmadik felek részére

b) adattovábbítás harmadik országokba

c) adattovábbítás adatfeldolgozás keretein belül

d) az adatok átadása az adatkezelő szervezetén belül

6.1 ad a) adattovábbítás harmadik felek részére

Adattovábbításnak minősül az adatok továbbadása valamely harmadik fél részére. Már az adatok harmadik fél számára történő puszta rendelkezésre bocsátása is adattovábbításnak minősül. Formálisan nem történik adattovábbítás abban az esetben, ha az adatokat nem harmadik fél részére, hanem az érintett, vagy az adatkezelő-en belüli személyek vagy vállalati egységek részére adják tovább.

Az adattovábbításhoz, mint minden adatkezelési művelethez, megfelelő jogalap szükséges.

Azt, hogy az adatok továbbításának jogalapja ténylegesen fennáll-e, minden egyes esetben ellenőrizni kell.

Az adattovábbítás tipikus esetei az adatkezelőnél:

- Adattovábbítás lehetséges, ha azt valamely jogszabály írja elő (pl. biztosítottak adatainak bejelentése a NAV-hoz, munkabaleseti jegyzőkönyv továbbítása az illetékes munkavédelmi hatóság részére).
- Adattovábbítás történhet jogos érdekből, pl. alkalmazottak elérhetőségi adatainak továbbítása valamely szerződő fél részére, a szerződés teljesítése során a kommunikáció gördülékenysége végett, az adatkezelő jogos érdeke alapján.
- Adattovábbítás történhet az adatkezelő jogi igényeinek előterjesztése, érvényesítése, illetve védelme céljából jogi képviselők részére, az adatkezelő jogos érdeke alapján.

- Amennyiben az alkalmazottak vonatkozásában a bérszámfejtést a **Magyar Államkincstár** végzi, továbbá ellátja a társadalombiztosítási kifizetőhely jogszabályban meghatározott feladatait, úgy a bérszámfejtéshez szükséges adatok és igazolások továbbításra kerülnek a Magyar Államkincstár részére.
- Egyéb esetekben a harmadik felek részére történő adattovábbításhoz az intézmény vezetésének előzetes engedélye szükséges. A belső adatvédelmi felelőst – és a vezetést, ha az engedély beszerzése bármely ok miatt nem volt lehetséges – az adattovábbításról minden esetben értesíteni kell, lehetőleg az adattovábbítást megelőzően.
- Miskolc Megyei Jogú Város Önkormányzata, mint fenntartó részére történő adattovábbítás minden esetben egyedi mérlegelést és vezetői engedélyt igényel, a jogalap pontos meghatározásával.

6.2 ad b) adattovábbítás harmadik országokba

Harmadik országnak minősül az Európai Unió, ill. az Európai Gazdasági Térség területén kívül elhelyezkedő valamennyi ország. Abban az esetben, ha az Európai Bizottság az adott harmadik ország adatvédelmi szintjét megfelelőnek értékelte (pl. Andorra, Argentína, Kanada, Feröer-szigetek, Guernsey, Izrael, Man, Jersey, Új-Zéland, Svájc és Uruguay), a szóban forgó ország „biztonságos" harmadik országnak minősül. (Ugyanakkor fontos, hogy ez esetben is be kell tartani az adattovábbítás általános szabályait.) Egyéb esetben az adott ország „nem biztonságos harmadik országnak" tekintendő és az adatoknak az ilyen országokban székhellyel rendelkező vállalatok részére történő továbbítása csak a további szigorú előírások betartása (pl. bizonyos szerződéses kikötések) mellett lehetséges.

Mivel az ilyen jellegű adattovábbítás különös kockázatokkal jár, és az adatkezelő alapvetően nem jogosult a nem biztonságos harmadik országokba történő adattovábbításra, a nem biztonságos harmadik országokba történő adattovábbítás előtt a belső adatvédelmi felelős szükséges.

6.3 ad c) adattovábbítás adatfeldolgozás keretén belül

Abban az esetben, ha az adatkezelő valamely harmadik fél részére személyes adatok tárolásával, kezelésével, stb. kapcsolatos megbízást ad, az adatfeldolgozó az adatkezelő utasításai szerint köteles eljárni, rendszerint adatvédelmi értelemben vett adatfeldolgozás történik.

Példák: adatok tárolása más tulajdonában álló szerveren, más cég által végzett informatikai jellegű szolgáltatás, támogatás, külső cég által végzett adatrögzítés stb.

Bár ebben az esetben a továbbítást nem kell jogszabállyal vagy hozzájárulással megalapozni, az adatkezelő az adatfeldolgozóval köteles adatfeldolgozási szerződést kötni. Az adatfeldolgozási szerződés kizárólag írásban érvényes, és rendelkeznie kell bizonyos tartalmi elemekkel, amelyeket a GDPR 28. cikke ír elő.

Abban az esetben, ha egy adott tevékenység kapcsán adatfeldolgozási szerződés nem áll rendelkezésre, vagy a Munkatárs nem biztos abban, hogy adott esetben adatfeldolgozás történik-e, köteles felvenni a kapcsolatot a belső adatvédelmi felelőssel vagy az ügyvezetéssel.

Az adatfeldolgozóval kötött alapszerződés és az adatfeldolgozói kiegészítés másolatát minden esetben a belső adatvédelmi felelős rendelkezésére kell bocsátani. Az adatfeldolgozási szerződések módosításait minden esetben egyeztetni kell a belső adatvédelmi felelőssel.

Adatfeldolgozó igénybevétele csak az adatkezelő vezetésének engedélyével, a belső adatvédelmi felelős egyidejű tájékoztatása mellett lehetséges. Kizárólag olyan adatfeldolgozókat lehet igénybe venni, amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. E tekintetben a belső adatvédelmi felelős által kezelt megfelelő ellenőrző listát kell alkalmazni.

Adatfeldolgozó igénybevétele esetén is tekintettel kell lenni a harmadik országba történő adattovábbítás során megkövetelt többletgaranciákra.

Az adatkezelő különböző mintákkal rendelkezik az adatfeldolgozói szerződés, az adatfeldolgozó által rendelkezésre bocsátott adatfeldolgozói szerződés megfelelőségének értékelése, valamint az adtafeldolgozó személye, az általa megtett adatbiztonsági intézkedések megfelelőségének megítélése tekintetében, amely mintákat a belső adatvédelmi felelős tud a Munkatársak rendelkezésére bocsátani. Ezen dokumentumok használata a Munkatársak kötelessége, a - szerződés megszűnését követő 10 évig történő - tárolásuk a belső adatvédelmi felelős feladata.

A belső adatvédelmi felelős nyilvántartást vezet az adatfeldolgozói jogviszonyokról és ezzel kapcsolatban aláírt szerződésekről.

6.4 ad d) az adatok átadása az adatkezelő szervezetén belül

Bár nem minősül adattovábbításnak, minden esetben figyelemmel kell lenni arra, hogy a személyes adatok valamely Munkatárs által az adatkezelőnél alkalmazásban álló másik Munkatárs részére történő átadása vagy más módon történő megismerhetővé tétele is csak abban az esetben lehetséges, ha a másik Munkatárs, az adatkezelő nevében ellátott feladatából adódóan, jogosult az adatokba való betekintésre, azok kezelésére.

Az adatkezelő szervezetén belül is biztosítani kell, hogy a hozzáférés csak az arra jogosult személyek számára legyen lehetséges. Ez megfelelő jogosultsági koncepciók segítségével biztosítható, amelyekben meg kell határozni, hogy

- mely adatokhoz/adatbázisokhoz
- ki (rendszerint itt a munkavállaló munkakörének leírása)
- milyen módon (olvasás, írás, törlés)
- milyen célból (pl. elszámolás, kiértékelések készítése) férhet hozzá.

A jogosultsági koncepció meghatározása és folyamatos karbantartása a belső adatvédelmi felelős és az informatikai vezető feladatkörébe tartozik.

6.5 Adattovábbítási nyilvántartás

Az adatkezelő minden egyedi és rendszeres adattovábbításról adattovábbítási nyilvántartást vezet. A nyilvántartás vezetése a belső adatvédelmi felelős feladata.

7 Különleges adatok kezelése

7.1 A GDPR értelmében különleges adatok kezelése főszabály szerint tilos. A tilalom nem áll fenn az alábbi esetekben:

a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez (*pl. egy speciális munkakörhöz való alkalmasság megítélése szempontjából a jelölt egészségi állapotára vonatkozó információk bekérése indokolt, ebben az esetben kifejezet hozzájárulást kell kérni az adatkezeléshez*), kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy a tilalom nem oldható fel az érintett hozzájárulásával,

b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges *(pl. ki kell töltenünk a munkabaleseti jegyzőkönyvet),* ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi, vagy

c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni, vagy

d) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott, vagy

e) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el, vagy

f) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében.

8 Adatok tárolása, korlátozása, törlése és visszaadása

8.1 Biztonsági előírások

Adatok tárolására, hozzáférés korlátozására és törlésére az adatkezelő informatikai biztonsági szabályzatával összhangban kerülhet sor.

Az e-mail és internethasználattal, valamint az adatkezelő informatikai eszközeinek használatával kapcsolatban releváns rendelkezéseket az adatkezelő informatikai biztonsági szabályzata tartalmaz.

8.2 Adatok korlátozása, törlése, megsemmisítése és visszaadása

8.2.1 Célhoz kötött adatkezelés

- Az adatokat csak annyi ideig lehet tárolni, ameddig szükség van rájuk, ill. ameddig a tárolás jogszabály alapján lehetséges. Így például adó- vagy számviteli jogi előírások alapján szükség lehet az adatkezelővel szerződő felekre vonatkozó adatok, például a kibocsátott vagy befogadott számlák) akár 8 évig történő tárolására is. Az archivált adatokat ez esetben már csak pl. adójogi célokra lehet felhasználni és egyéb célok vonatkozásában a felhasználásukat (és az egyes Munkatársak általi hozzáféréseket) korlátozni kell a szükséges mértékre.
- A vállalati levelezőrendszerben küldött/kapott, személyes adatokat tartalmazó e-maileket rendszeresen törölni kell, ha az abban szereplő adatok kezelése már nem jogszerű, vagy az adatok a megfelelő nyilvántartásban már rögzítésre kerültek.
- A word alapú dokumentum tervezeteket is törölni kell a levelezőrendszerekből és a mapparendszerből, ha azok személyes adatokat tartalmaznak, és az adat tárolása már nem jogszerű.
- Olyan Jelölt esetén, aki egy konkrét álláshirdetésre jelentkezett, de nem járult hozzá az adatainak későbbi nyitott pozíció kapcsán történő felhasználásához sem, a személyes adatokat a jelentkezés elbírálásától számított 90 napon belül vissza kell küldeni, illetve meg kell semmisíteni. Nem szabad megfeledkezni arról, hogy az adatokat ilyen esetben törölni kell a megfelelő nyilvántartásokból és a levelezőrendszerekből is (pl. Munkatársaknak e-mailben továbbított önéletrajzok esetén magának az e-mailnek a törlése).
- Az adatkezelőnél elhelyezkedni kívánó Jelölt pályázatát és az abban szereplő személyes adatokat, amennyiben a Jelölt nem nyer felvételt, legkésőbb a döntéstől számított 90 nap elteltével részére vissza kell küldeni, illetve meg kell semmisíteni, elektronikus úton benyújtott pályázat esetén törölni kell (a levelezőrendszerből és egyéb fájlokból is). **Pályázati anyagának, ill. adatainak a toborzási adatbázisban történő megőrzése csak a Jelölt írásbeli hozzájárulása esetén lehetséges** (nem minősül hozzájárulásnak az, ha a Jelölt részére küldendő válasz e-mailbe beleírjuk, hogy ellenkező nyilatkozatáig adatait megőrizzük és felhasználhatjuk). A hozzájárulás legkorábban az elutasító döntés közlésével egyidejűleg kérhető.

- Munkaügyi részlegen a személyazonosító és egyéb személyes okmányok általános jellegű fénymásolása és tárolása – erre irányuló jogszabályi kötelezettség hiányában – tilos. Ez nem zárja ki azt, hogy a személyes okmányokat ellenőrzés céljából megtekintsük, vagy e-mailben bekérjük, de az ellenőrzés lefolytatását követően az elektronikus fájlokat törölni kell, mivel ezen fájlok tárolásának nincs további célja. Ezzel szemben jogszabály alapján le kell másolni és a személyügyi anyagban kell tárolni pl. a munkaviszony alatt született gyermekek születési anyakönyvi kivonatait (halotti bizonyítványai), illetve megváltozott munkaképességű munkavállaló esetén a fogyatékosság igazolására irányuló iratokat.

8.2.2 Adattörlési koncepció / Irattári terv

Az **adattörlési koncepció, illetve irattári terv elkészítése és karbantartása a belső adatvédelmi felelős és az informatikai vezető felelőssége.**

Az adatok, fájlok, iratok besorolása, valamint a tárolással és törléssel kapcsolatos követelmények vonatkozásában felmerülő kérdések vagy bizonytalanságok esetén haladéktalanul fel kell venni a kapcsolatot a belső adatvédelmi felelőssel, aki a szükséges intézkedéseket koordinálja.

8.2.3 Megsemmisítés

Biztosítani kell, hogy a személyes adatok megsemmisítése vagy törlése az adatvédelmi előírásokkal, a vonatkozó iratkezelési szabályzattal (amennyiben az adatkezelő ilyennel rendelkezik), valamint a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet előírásaival összhangban történjen. A szisztematikus, a törlési koncepció szerinti iratselejtezésről a fenti Korm. rendeletnek megfelelő selejtezési jegyzőkönyvet kell készíteni, amelyet, a selejtezést megelőzően a belső adatvédelmi felelős által kell jóváhagyatni. Az iratoknak a bennük szereplő személyes adatok felismerhetetlenné tétele nélküli kidobása adatvédelmi incidenst valósít meg.

A szisztematikus, törlési koncepció / irattári terv szerinti iratselejtezéseket minden tárgyévet követő január 31-ig kell végrehajtani, az iratkezelési szabályzat rendelkezései szerint.

Az iratokat az irattárban a selejtezési idők szerint elkülönítetten kell elhelyezni.

9 Szervezeti adatvédelem

9.1 A Munkatársak titoktartási kötelezettsége

A Munkatársakat titoktartási kötelezettségvállalási nyilatkozat aláírásával titoktartásra kell kötelezni. A titoktartási kötelezettség a tevékenységük befejezését követően is fennáll.

9.2 Adatbiztonság

9.2.1 Az adatkezelés során gondoskodni kell az adatok biztonságáról, meg kell tenni továbbá azokat a technikai és szervezési intézkedéseket, és ki kell alakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

9.2.2 Az adatokat megfelelő technika alkalmazásával és megfelelő intézkedésekkel is védeni kell az esetleges adatvédelmi incidens ellen. A Munkatárs a tőle elvárható módon és a rendelkezésére álló eszközökkel köteles megakadályozni az incidens bekövetkezését.

9.2.3 Adatkezelési tevékenység elektronikusan – az adatfeldolgozás kivételével – kizárólag az adatkezelő által üzemeltetett és/vagy az adatkezelő által használt számítógépeken végezhető. A személyes adatokat tartalmazó fájlok létrehozójának, az adatállományt módosító személynek, valamint a létrehozás, valamint a módosítás időpontjának azonosíthatónak kell lennie.

9.2.4 Az adatkezelés során be kell tartani az adatkezelő mindenkori informatikai előírásait. A Munkatársaknak az általuk kezelt személyes adatokat és adatbázisokat védeniük kell a technikai és egyéb hibákból eredő károsodások ellen. Meghibásodás esetén minden tevékenységet fel kell függeszteni, és haladéktalanul értesíteni kell az informatikai vezetőt.

9.2.5 Személyes adatokat tartalmazó fájlok, dokumentumok, iratok akár nyomtatott formában, akár bármely egyéb mobil adathordozón az adatkezelő területéről csak indokolt esetben és a belső adatvédelmi felelős előzetes írásos tájékoztatásával vihetők ki. Kivételt képeznek ez alól azon esetek, amikor a feladatellátás végrehajtása magában foglalja a személyes adatok munkaidőben, külső helyszínen történő kezelését. Személyes adatok – a harmadik személy részére történő adattovábbítás kifejezett és jogszerű esetét ide nem értve – nem küldhetők el olyan e-mail címre, amely nem az adatkezelő által biztosított e-mail cím (pl. freemail, gmail, yahoo stb.). Google drive és hasonló megosztó oldalak nem használhatóak munkavégzési célokra.

9.2.6 Személyes adatot nyomtatott formában, illetve személyes adatot tartalmazó adathordozót munkaidőn kívül is biztonságos helyen, elzárva kell tartani. A munkaidőt követően nem szabad az íróasztalokon, elzáratlanul személyes adatokat is tartalmazó iratokat, feljegyzéseket hagyni. Amennyiben a Munkatárs az íróasztalát ideiglenesen elhagyja, meg kell győződnie arról, hogy jogosulatlan személyek a távolléte alatt nem férhetnek hozzá személyes adatokhoz. Céges laptopot, mobiltelefont tilos őrizetlenül hagyni. Gépjárműben felügyelet nélkül laptopot, mobiltelefont tilos otthagyni.

9.2.7 A Munkatárs nem közölheti illetéktelen személyekkel és ilyen személyeknek nem teheti hozzáférhetővé a vállalati eszközökhöz vagy alkalmazásokhoz tartozó jelszavát. Kifejezetten tilos a jelszavakat bárhová felírni, vagy sms-ben, e-mailben másnak elküldeni.

9.2.8 A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt jogszabály lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók.

9.2.9 Több lehetséges adatkezelési megoldás közül minden esetben azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget vagy többletköltséget jelentene. Ez utóbbi esetben sem választható olyan adatkezelési megoldás, amely a személyes adatok magas szintű védelmét nem biztosítja.

9.2.10 Az adatkezelő informatikai eszközeinek, az adatkezelő által biztosított levelezőrendszernek a magáncélú használata tilos. Mindazonáltal az informatikai eszközök és levelezőrendszerbe történő betekintés esetén be kell tartani a vonatkozó adatvédelmi követelményeket és a fokozatosság elve szerint kell eljárni (a Munkatárs jelenlétét a lehetőségekhez képest biztosítani kell, és mindig az adott célt elérő, legkevésbé korlátozó intézkedést kell választani, pl. lehetséges, hogy elég csak az e-mailek tárgyának vizsgálata, azok tartalma megtekintése nélkül).

9.2.11 A Munkatárs jogviszonyának megszűnése esetén az utolsó feladatteljesítési napon köteles minden olyan – technikai és/vagy nem technikai – adathordozót vagy adattárolásra egyébként alkalmas tárgyat, eszközt átadni a Munkatárs feletti irányítási, felügyeleti jogkört gyakorló vezetőnek vagy a vezető által kijelölt más alkalmazottnak, amely személyes adatot bármilyen formában hordoz, tartalmaz. A Munkatárs jogviszonyának megszűnése esetén az utolsó feladatteljesítési napon a Munkatárs minden olyan jogosultságát meg kell szüntetni, amely adatkezelési tevékenység végzésének lehetőségét biztosította számára. A Munkatárs jogviszonyának megszűnését követően sem közölhet, illetve fedhet fel személyes adatot arra illetéktelen személy előtt.

9.2.12 A Munkatárs jogviszonyának megszűnése esetén az utolsó feladatteljesítési napon köteles törölni minden, az adatkezelő tulajdonában álló eszközön vagy a levelezőrendszerben, illetve közös mapparendszeren tárolt, és nem az adatkezelő kezelésében álló személyes adatot, tartalmat.

9.2.13 Az adatbiztonság vonatkozásában be kell tartani az adatkezelő mindenkor hatályban lévő és Informatikai jellegű szabályzatait.

9.3 A foglalkoztatásra irányuló jogviszonnyal összefüggő magatartás ellenőrzésének szabályai

9.3.1 A Munkatárs az adatkezelő által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert (a továbbiakban: számítástechnikai eszköz) - eltérő megállapodás hiányában - kizárólag a jogviszony teljesítése érdekében, munkavégzési célból használhatja.

Az adatkezelő a tevékenysége során a jogszabályi és munkavégzési előírások betartásának védelmében, jogos gazdasági érdekeinek előmozdítása, és a visszaélések megelőzése és felderítése érdekében belső ellenőrzéseket hajthat végre.

9.3.2 Az adatkezelő az ellenőrzése során a munkavégzés céljából használt számítástechnikai eszközön tárolt, a jogviszonnyal összefüggő adatokba tekinthet be, a jogviszonnyal nem összefüggő személyes adatok nem ellenőrizhetők. Az ellenőrzési jogosultság szempontjából a jogviszonnyal összefüggő adatnak minősül a fenti korlátozás betartásának ellenőrzéséhez szükséges adat. Az ellenőrzés során használt eszközök, módszerek a lent részletesen kifejtettek szerint nem sérthetik az emberi méltóságot és az eszközök ellenőrzése során be kell tartani a célhoz kötött és tisztességes adatkezelés, valamint a fokozatosság elvét.

9.3.3 Az ellenőrzésre vonatkozó szabályok akkor is irányadók, ha a felek megállapodása alapján a Munkatárs a jogviszony teljesítése érdekében saját számítástechnikai eszközt használ.

9.3.4 A Munkatárs ellenőrzésének jogalapja az adatkezelő tevékenységére tekintettel a jogszabályi és munkavégzési előírások betartásának védelmére, a jogos gazdasági érdekeinek, az adatkezelő tevékenysége folyamatosságának biztosítására, az emberi élet, testi épség védelmére, bűncselekmények, szabálysértések, belső visszaélések megelőzésére, felderítésére és vagyonvédelemre vonatkozó jogos munkáltatói érdek. Az ellenőrzés módjai az alábbiak:

- a Munkatársak rendelkezésére bocsátott e-mail fiók használatának ellenőrzése;
- a Munkatársak rendelkezésére bocsátott laptop és számítógép használatának ellenőrzése;
- a Munkatársak internethasználatának korlátozása;
- a Munkatársak rendelkezésére bocsátott gépjárművek tartózkodási helyének, használatának ellenőrzése.

9.3.5 A Munkatársak személyiségi jogaik megsértése esetén a GDPR-ban, valamint a vonatkozó adatkezelési tájékoztatóban is felsorolt jogérvényesítési eszközökkel élhet.

9.3.6 A Munkatársak rendelkezésére bocsátott e-mail fiókok ellenőrzésére vonatkozó részletes szabályok:

- az adatkezelő által a Munkatársak rendelkezésre bocsátott munkahelyi e-mail fiókot a Munkatársak kizárólag a munkavégzésükkel összefüggésben használhatják. A munkahelyi e-mail fiók magáncélra való használata tilos. Az adatkezelő az e-mail fiókok teljes tartalmát jogosult ellenőrizni, ugyanakkor az adatkezelő nem jogosult betekinteni a Munkatársak által az adatkezelő felszólítására személyes adatként megjelölt adatokba.
- az e-mail fiókokról a rendszeres mentés során biztonsági másolat készül.
- az adatkezelő az e-mail fiókok biztonsági másolatait az Informatikai Biztonsági Szabályzatban meghatározott ideig őrzi.
- az adatkezelő által a Munkatársak rendelkezésére bocsátott e-mail fiókokba, informatikai rendszerekbe való betekintésre vezetői engedéllyel a kijelölt informatikai munkatárs és a belső adatvédelmi felelős együttesen jogosultak.
- a Munkatársak rendelkezésére bocsátott e-mail fiókok, informatikai eszközök ellenőrzésének menete:

- az adatkezelő a Munkatársak munkahelyi e-mail fiókjába bármikor betekinthet, annak kizárólag munkavégzéssel összefüggésben való használatára vonatkozó korlátozás betartásának ellenőrzése, és a jogszabályi és munkavégzési előírások betartásának védelme, a jogos gazdasági érdekeinek, az adatkezelő tevékenysége folyamatosságának biztosítása, az emberi élet, testi épség védelme, bűncselekmények, szabálysértések, belső visszaélések megelőzése, felderítése és vagyonvédelemre vonatkozó jogos munkáltatói érdeknek céljából;
- az adatkezelő a Munkatársak munkahelyi e-mail fiókjába, informatikai eszközébe történő betekintést megelőzően tájékoztatja a Munkatársat az e-mail fiók, informatikai eszköz ellenőrzésének konkrét céljáról, helyéről és idejéről és biztosítja, hogy jelen legyen az ellenőrzésnél. Az ellenőrzés során a Munkatárs jelezheti valamely e-mail tartalmának megtekintése előtt, hogy azok személyes adatot tartalmaznak. A magánjellegű levelek tartalmát az adatkezelő nem jogosult megismerni. Az ellenőrzésről jegyzőkönyvet kell készíteni.
- az ellenőrzés során be kell tartani a fokozatosság elvét. (Példa a fokozatosság elvére: az ellenőrzés első lépéseként az e-mail cím és a levél tárgyának az ellenőrzése is elegendő lehet, hiszen bizonyos esetekben már pusztán az e-mail cím felépítéséből és az e-mail tárgyából is lehet látni azt, hogy az magáncélú e-mail lesz, és ezért nem szükséges megismerni az e-mail tartalmát.)

9.3.7 A Munkatársak rendelkezésére bocsátott laptop és számítógép használatának ellenőrzésére vonatkozó részletes szabályok:

- az adatkezelő által a Munkatársak részére rendelkezésre bocsátott munkahelyi laptopot és számítógépet a Munkatársak a munkavégzésükön túl magáncélra nem használhatják. Az adatkezelő a munkahelyi laptopon és számítógépen tárolt adatok teljes tartalmát jogosult ellenőrizni;
- a munkahelyi laptopon és számítógépen tárolt adatokról biztonsági másolat készül;
- az adatkezelő a munkahelyi laptopon és számítógépen tárolt adatokat a Munkatársak foglalkoztatásra irányuló jogviszonyának fennállását követően az Informatikai Biztonsági Szabályzatban meghatározott ideig őrzi. Az adatkezelő által a Munkatársak rendelkezésére bocsátott laptopon és számítógépen tárolt adatokba való betekintésre ügyvezetői engedéllyel a kijelölt informatikus és a belső adatvédelmi felelős együttesen jogosultak.
- a munkahelyi laptopokon és számítógépen tárolt adatok ellenőrzésével kapcsolatos eljárás során az e-mail fiókok ellenőrzésével kapcsolatos megállapítások szerint kell eljárni.

9.3.8 A Munkavállalók internethasználatának korlátozása:

Az adatkezelő a Munkatársak rendelkezésére bocsátott elektronikus eszközökön, a magáncélú internethasználatot nem engedélyezi, és jogosult ennek ellenőrzésére az Informatikai Biztonsági Szabályzatban foglaltak szerint.

9.3.9 A Munkatársak rendelkezésére bocsátott mobiltelefonok ellenőrzésének részletes szabályai:

- Az adatkezelő által a Munkatársak részére rendelkezésre bocsátott munkahelyi mobiltelefonok a Munkatársak által magáncélra nem használhatóak.
- Az adatkezelő megismerheti a hívásokat abból a célból, hogy a magáncélú hívásokat elkülönítse a munkavégzési célúaktól és a magáncélú hívások létét deklarálja;
- a munkahelyi mobiltelefonok híváslistája ellenőrzésének célja:

- az adatkezelő tevékenységére tekintettel, a jogszabályi és munkavégzési előírások betartásának védelme, a jogos gazdasági érdekein túl belső visszaélések megelőzése és felderítése;
- az adatkezelő által a Munkatársak rendelkezésére bocsátott mobiltelefon híváslistájának ellenőrzésére vezetői engedéllyel a kijelölt informatikai munkatárs és belső adatvédelmi felelős együttesen jogosultak;

- a munkahelyi mobiltelefonok híváslistája ellenőrzésének menete:
  - az adatkezelő a Munkatársak munkahelyi mobiltelefonjának híváslistáját bármikor jogosult a szolgáltatótól lekérni és ellenőrizni;
  - az adatkezelő a Munkatársak munkahelyi mobiltelefonjának híváslistájába annak ellenőrzése céljából bármikor jogosult betekinteni;
  - a betekintést megelőzően az adatkezelő felhívja a Munkatársak, hogy a híváslistáról a magáncélú hívások esetén a hívott/hívó fél telefonszámait tegye felismerhetetlenné azért, hogy azokat az adatkezelő nem ismerje meg, vagy nyilatkozzon arról, hogy a híváslistán magánjellegű hívás nem szerepel.

9.4 Adatvédelmi incidensek

9.4.1 Tájékoztatási kötelezettség

Valamennyi Munkatárs köteles a felettesét és a belső adatvédelmi felelőst haladéktalanul tájékoztatni abban az esetben, ha a tevékenysége során adatvédelmi jogszabálysértést vagy adatvédelmi incidenst tapasztalt.

Adatvédelmi incidens esetén az adatkezelő a GDPR 33. cikke szerint alapvetően köteles a NAIH-ot haladéktalanul, legkésőbb 72 órán belül értesíteni (ez alól kivétel, ha az incidens nem jár kockázattal az érintettek jogaira nézve). Ezen túlmenően az adatkezelő a GDPR 34. cikke szerint, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, köteles az érintettet tájékoztatni az adatvédelmi incidensről (a továbbiakban: „**adatvédelmi incidens**").

9.4.2 Adatvédelmi incidens fogalma

Adatvédelmi incidens áll fenn akkor, ha az adatbiztonság megsértése a továbbított, tárolt vagy egyéb módon kezelt személyes adatok megsemmisülését, elvesztését, módosulását, jogosulatlan nyilvánosságra hozatalát vagy jogosulatlan elérését eredményezi. Jogosulatlan nyilvánosságra hozatalról beszélhetünk pl. akkor, ha az adatok nyilvánosságra kerültek úgy, hogy az érintettek a nyilvánosságra hozatalhoz nem járultak hozzá, és azt jogszabály sem teszi lehetővé. Az is adatvédelmi incidenst jelent, ha az ilyen jellegű esemény bekövetkezése bizonyos valószínűséggel feltételezhető.

Adatvédelmi incidensről beszélhetünk például az alábbi esetekben:

- adatvesztés (pl. laptop vagy más adathordozó elvesztése vagy eltulajdonítása, ha az azon található adatok nem vagy nem megfelelően titkosítottak);
- videokamera, fényképezőgép, pendrive elvesztése, ill. eltulajdonítása;
- adatokat tartalmazó, nem titkosított lista véletlen elektronikus elküldése arra jogosulatlan Munkatárs részére;
- hackertámadások;
- adatok nyilvánosságra hozatala az interneten, technikai hiba következtében.

9.4.3 Adatvédelmi incidens esetén követendő eljárásrend

Az adatvédelmi incidensre adott helyes és megfelelő időben történő reakció érdekében az alábbi eljárásrendet kell követni.

9.4.3.1 Incidens bejelentése a szervezeten belül

Amennyiben a Munkatárs megállapítása vagy véleménye szerint adatvédelmi incidens történt vagy történhetett, úgy erről köteles a felettesét haladéktalanul (de legkésőbb 12 órán belül) tájékoztatni. A felettes, amennyiben megítélése szerint adatvédelmi incidens történt, köteles az vezetést, a belső adatvédelmi felelőst és az adatvédelmi tisztviselőt haladéktalanul, legkésőbb a tudomásszerzéstől számított 12 órán belül írásban tájékoztatni.

A bejelentésben az alábbi információkra kell kitérni:

- Hogyan, miért és milyen módon került sor az adatvédelmi incidensre?
- Milyen adattípusok, ill. hány fájl és személy érintett?
- Ki az adatvédelmi tisztviselő és mik az elérhetőségei?
- Milyen következményekkel járhat az adatvédelmi incidens?
- Mikor állapították meg az adatvédelmi incidens tényét a vállalaton belül?
- Milyen intézkedéseket tett a vállalat az adatvédelmi incidens felfedését követően annak megszüntetésére vagy mérséklésére?
- Az érintettek tájékoztatása már megtörtént? Hogyan és milyen tartalommal került sor a tájékoztatásra?
- Bejelentették az adatvédelmi incidenst az adatvédelmi felügyeleti hatóságnál vagy már bevonták a hatóságot az ügybe?

A bejelentés megtételére és annak kivizsgálására a 1/a. sz. mellékletben szereplő formanyomtatványt kell használni.

9.4.3.2 Incidens okainak kivizsgálása

Az incidens megszüntetését, következményeinek elhárítását és az okainak kivizsgálását haladéktalanul meg kell kezdeni.

A belső adatvédelmi felelős haladéktalanul tájékoztatja az informatikai részleg vezetőjét a bejelentésről, továbbá a vezetést, és az adatvédelmi tisztviselőt, amennyiben a tájékoztatás mindezidáig nem történt volna meg.

A belső adatvédelmi felelős ezt követően az informatikai részleg vezetőjével közösen megvizsgálja a tényállást, és a vezetés részére értékelést, ill. javaslatot nyújt be. Szükség esetén a jogi vezető vagy az adatkezelő jogi tanácsadója bevonható.

A belső adatvédelmi felelős ezen túlmenően az informatikai részleg vezetője, valamint a bejelentést tevő személy együttműködésével kitölti (kiegészíti), véglegesíti és a vezetés rendelkezésére bocsátja az *„Adatvédelmi incidensről szóló jegyzőkönyv és bejelentés”* elnevezésű formanyomtatványt, amelyben az 1/b. sz. mellékletben megjelölt információk szerepelnek. A belső adatvédelmi felelős köteles az incidens kockázatait értékelni a kockázatértékelésre vonatkozó belső előírások szerint és a kockázatértékelés dokumentációját a jegyzőkönyvvel együtt 10 évig megőrizni.

A konkrét helyzetben szükséges teendőkkel kapcsolatos döntést a vezetés hozza meg az adatvédelmi tisztviselővel és az informatikai megbízottal történt egyeztetést követően, a bejelentés megtételét követő 36 órán belül.

9.4.3.3 **Incidensek nyilvántartása**

Minden incidensről – függetlenül attól, hogy az az adatkezelés mely szegmensét és milyen mértékben érintette – nyilvántartó lapot kell felvenni, amelyben a 1/b. sz. melléklet szerinti információk szerepelnek. Az adatkezelő az adatvédelmiincidens-nyilvántartási kötelezettségét a nyilvántartási lap felvételével, valamint egy összefoglaló táblázat vezetésével teljesíti; e nyilvántartást a belső adatvédelmi felelős vezeti és kezeli.

9.4.3.4 **Incidens bejelentése a NAIH-nak**

Az incidenst indokolatlan késedelem nélkül, de legkésőbb az adatkezelő általi tudomásszerzéstől számított 72 órán belül az adatkezelő bejelenti a NAIH-nak, amennyiben az incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Tudomásszerzésnek az számít, amikor bármely Munkatárs az incidens először észlelte.

A bejelentésben ismertetni, illetve közölni kell legalább:

a) az adatvédelmi incidens jellegét, 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 incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket,

e) késedelmes bejelentés esetén a késedelem igazolására szolgáló indokokat.

A bejelentést a NAIH erre a célra szolgáló elektronikus bejelentő felületén kell megtenni.

Mellőzhető a NAIH felé irányuló bejelentés, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. E körben a belső adatvédelmi felelős állásfoglalása irányadó. Ez a pont nem érinti az incidens kivizsgálásának és nyilvántartásának kötelezettséget.

Ha a fenti szerinti bejelentésben valamely információkat nem lehetséges egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

9.4.3.5 **Érintettek értesítése**

Ha az incidens – az adatvédelmi felelősnek a vezetéssel és az adatvédelmi tisztviselővel egyeztetett állásfoglalása szerint – valószínűsíthetően magas kockázattal jár, az adatkezelő haladéktalanul értesíti az Érintettet az incidensről, amely tájékoztatást a belső adatvédelmi felelős állít össze a vezetéssel és az adatvédelmi tisztviselővel történt egyeztetést követően, és amely tájékoztatásban közérthetően és világosan

a) ismertetni kell az incidens jellegét,

b) közölni kell a 9.4.3.4 pont b)-d) pontjában említett információkat és intézkedéseket.

Az incidensről az Érintettet nem kell tájékoztatni, ha

a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az incidens által érintett adatok tekintetében alkalmazta, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat, vagy

b) az adatkezelő az incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az Érintett jogaira és szabadságaira jelentett – a magas kockázat a továbbiakban valószínűsíthetően nem valósul meg, vagy

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

A fenti c) pont szerinti esetben az Érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

9.4.3.6 **További rendelkezések**

- Incidens észlelése esetén tilos azt harmadik személyeknek vagy a jelen pontban meghatározottakon kívüli más Munkatársnak kommunikálni.
- Tekintettel arra, hogy a GDPR 33. cikkében foglaltak megsértése jelentős pénzbírság kiszabását és az adatkezelő megítélésének súlyos károsodását vonhatja maga után, ezért az adatkezelő vezetésének feladata annak eldöntése, hogy az adott helyzetben miként járjanak el, ill. hogy az eseményt a nyilvánosság irányába kommunikálják-e, és ha igen, milyen módon.
- Az adatvédelmi incidensek érzékenysége késedelem nélküli szervezeten belüli bejelentési folyamatot követel meg.
- A Munkatársak kötelesek a bejelentésében a lehető legpontosabban ismertetni a történteket.

9.5 Hatósági megkeresések, ellenőrzések

A közigazgatási és az igazságszolgáltatási szervek azon felhatalmazott tisztviselői részére, akiknek a munkavégzése során az adatokhoz, különösen a személyes adatokhoz való hozzáférésre jogszabályban rögzített feladatuk ellátása érdekében szükségük van, a hozzáférést – a szer általi írásbeli megkeresés esetén – biztosítani kell. Minden ehhez szükséges intézkedést a vezetés és a belső adatvédelmi felelős koordinál és felügyel.

Ezért, amennyiben személyes adatok átadását is magában foglaló hatósági megkeresés érkezik, haladéktalanul értesíteni kell a vezetést és a belső adatvédelmi felelőst.

9.6 A NAIH által végzett ellenőrzések

NAIH által, az adatkezelő-t érintő ellenőrzésekről történő tudomásszerzés esetén haladéktalanul értesíteni kell a vezetést és a belső adatvédelmi felelőst.

A GDPR rendelkezései szerint a NAIH, mint felügyeleti hatóság köteles a GDPR és más adatvédelmi jogszabályok betartását ellenőrizni és felügyelni. Ezek alapján a NAIH alapvetően jogosult a felügyelete alá tartozó adatkezelők ingatlanjaiba és üzlethelyiségeibe munka- és nyitvatartási időben belépni, ott vizsgálatokat és megfigyelést végezni, és ennek során a vállalati dokumentumokba, valamint a tárolt személyes adatokba és az adatkezelő programokba betekinteni. Nem szükségszerű, hogy a NAIH a helyszíni vizsgálatát előzetesen bejelentse.

Az adatkezelőnek el kell fogadnia a NAIH intézkedéseit és gondoskodnia kell arról, hogy azok a helyiségek, amelyekben az adatkezelés történik (pl. a Munkatársak irodái, archívum), valamint a szükséges jelszavak és a releváns dokumentumok előkészítésre kerüljenek és a NAIH képviselőinek rendelkezésére álljanak. Ezen túlmenően kérés esetén a NAIH rendelkezésére kell bocsátani a feladatai elvégzéséhez szükséges információkat is.

9.7 Képzés

Az adatkezelő az adatkezelési műveletekkel jellemzően érintett területen foglalkoztatott Munkatársait a mindenkor érvényes jogszabályok adatvédelmi rendelkezéseire vonatkozó rendszeres képzésben részesíti. A képzések évente legalább egyszer kerülnek megtartásra. A Munkatársak képzését a képzés tartalmának, dátumának és az oktató nevének feltüntetésével dokumentálni kell, a dokumentáció 10 évig történő megőrzése a belső adatvédelmi felelős feladata.

9.8 Adatkezelési tevékenységek nyilvántartása

A GDPR 30. cikke értelmében az adatkezelőnél el kell készíteni és vezetni kell az ún. adatkezelési tevékenységek nyilvántartását. Ez vonatkozik az adatkezelő által végzett adatkezelési és adatfeldolgozási műveletekre is.

Az adatkezelési tevékenységek nyilvántartását a NAIH által végzett ellenőrzés során az aktuálisan végzett adatkezelési tevékenységek áttekintéseként a hatóság rendelkezésére kell bocsátani.

Ennek érdekében biztosítani kell, hogy a nyilvántartás mindig naprakész legyen.

A nyilvántartás vezetése és karbantartása a belső adatvédelmi felelős feladata.

Új eljárás vagy új adatkezelés esetén a nyilvántartást az eljárás vagy adatkezelés bevezetése előtt el kell készíteni.

9.9 Adatvédelmi hatásvizsgálat

Bizonyos esetekben az adatkezelőnek úgynevezett adatvédelmi hatásvizsgálatot kell készítenie, pl. abban az esetben, ha az adatkezelés az Érintett számára magas kockázattal járhat. Magas kockázat merülhet fel az alkalmazottak teljesítményének és magatartásának automatizált ellenőrzése esetén.

Azt, hogy adatvédelmi hatásvizsgálatot kell-e készíteni, többek között a vezetés, az adatvédelmi tisztviselő és a belső adatvédelmi felelős határozza meg. Ők határozzák meg azt is, hogy egyedi esetben kit kell bevonni a folyamatba, ill. ki működik közre támogatóként a hatásvizsgálat végrehajtásában.

10 Adatvédelmi szervezet

Az adatkezelő a GDPR rendeletnek való megfelelés érdekében külön definiált, önálló adatvédelmi szervezetet működtet, melyet az alábbiak szerint határoz meg:

a) adatvédelmi tisztviselő
b) vezetőség
c) belső adatvédelmi felelős
d) szervezeti egységek vezetői, mint szakterületi adatvédelmi felelősök
e) telephelyek vezetői, mint helyi adatvédelmi felelősök
f) adatkezeléssel foglalkozó beosztott munkavállalók

10.1 Adatvédelmi tisztviselő

Az adatkezelő adtavédelmi tisztviselőt jelölt ki, aki a GDPR előírásainak megfelelően koordinálja az adatvédelmi kérdéseket az adatkezelőnél.

Az adatkezelő adatvédelmi tisztviselőjének elérhetőségei: adatvedelem@bdolegal.hu, telefonszám: +36 1 235 30 10, cím: BDO Legal, 1103 Budapest, Kőér u. 2/A. C. ép.

Az adatvédelmi tisztviselő segíti a Munkatársakat az adatvédelmi szempontból jelentős kérdések eldöntésében, továbbá szakmai tanácsokkal segíti a vezetést és a belső adatvédelmi felelőst a megfelelő döntések meghozatalában. Hatósági eljárások esetén az adatvédelmi tisztviselő tartja a kapcsolatot a NAIH-hal.

10.2 A vezetés / vezető

- jogosult meghatározni az adatvédelmi feladat és hatásköröket, dönt az adatvédelmi szervezet kialakításáról,
- az adatvédelmi szervezetben meghatározott egyes feladatokat és felelősséget megállapítja, és ezeket hozzáigazítja az általános szervezeti működéshez,
- az adatvédelemmel kapcsolatos belső szabályozásokra tekintettel dönt új munkaköri leírások, munkaköri feladatkatalógusok kiadásáról, ezek aktualizálásáról, módosításáról
- fegyelmi jogkört gyakorol az adatvédelmi kötelezettségek teljesítése kapcsán,
- megbízást ad külső, független szakértő szolgáltatók részére az adatkezelés rendjének és az adatbiztonság rendjének évenként történő felülvizsgálata kapcsán,
- végső döntést hoz az olyan adatvédelemmel kapcsolatos kérdésekről, mint amilyenek
- a beépített és alapértelmezett adatvédelemnek való megfelelés és ennek vállalati eszközei,

- jóváhagyja az adatfeldolgozásra irányuló szerződések tartalmát, formátumát és megköti az adatfeldolgozásra irányuló szerződéseket,
- vezetői értekezleten beszámoltatja az adatvédelmi szervezet egyes területeiért, vagy szintjeiért felelős munkatársakat,
- végső döntést hoz az érdekmérlegelés alapján történő adatkezelés jogalapjáról,
- végső döntést hoz adatvédelmi hatásvizsgálatokkal kapcsolatos kérdésekről,
- adatvédelmi incidensek hatóság felé történő bejelentéséről, illetve arról, ha ez nem szükséges
- kinevezi vagy visszahívja az adatvédelmi tisztviselőt, ha ez indokolttá válik.

10.3 Belső adatvédelmi felelős

10.3.1 Az adatvédelmi szervezet operatív működtetése a belső adatvédelmi felelős feladata, aki

a) elkészíti és karbantartja a jelen szabályzat szerinti nyilvántartásokat és szabályzatokat, illetve formanyomtatványokat, sablonokat,
b) az érintetti kérelmeket megválaszolja,
c) elkészíti, és szükség esetén módosítja az adatkezelő GDPR 13. és 14. cikkei szerinti adatkezelési tájékoztatásokat,
d) hozzájáruláson alapuló adatkezelés esetén elkészíti a hozzáhárulást, meghatározza annak megadása módját, illetve ellenőrzi a hozzájárulás megfelelőségét, gondoskodik a hozzájárulások 10 évig történő megőrzéséről,
e) hozzáfér és kezeli a cinemis@t-online.hu e-mail címet,
f) a jogi vezetővel/jogi tanácsadóval, valamint szükség esetén az adatvédelmi tisztviselővel együttműködve elvégzi és nyilvántartja a szükséges érdekmérlegelési teszteket,
g) nyilvántartja az adatkezelő adatfeldolgozói jogviszonyait és szerződéseit, tárolja az adatfeldolgozó megfelelőségére vonatkozó értékeléseket,
h) feltárja az adatvédelmi incidenseket és a vezetéssel egyeztetve azokat bejelenti a NAIH-nak és szükség esetén tájékoztatja az érintetteket, vezeti az adatvédelmi incidens nyilvántartást, lefolytatja a kockázatértékelést és megőrzi a vonatkozó dokumentációt,
i) a vezetéssel és az adatvédelmi tisztviselővel egyeztetve lefolytatja a hatásvizsgálatokat, amennyiben azok szükségesek,
j) vezeti az adattovábbítási nyilvántartást,
k) kezeli és megőrzi az adatvédelmi dokumentációt.

10.3.2 A belső adatvédelmi felelős jogai:

a) A belső adatvédelmi felelős jogosult az adatkezelő nevében megvalósuló adatkezeléseket ellenőrizni, jogosult továbbá az adatkezelésekkel kapcsolatos információkat a Munkatársaktól bekérni. A Munkatársak kötelesek a belső adatvédelmi felelőssel együttműködni.
b) A belső adatvédelmi felelős jogosult a vezetéshez és/vagy az adatvédelmi tisztviselőhöz fordulni az adatvédelemmel kapcsolatos döntések meghozatala érdekében, illetve a jogi vezetőhöz/jogi tanácsadóhoz fordulni jogi kérdésekben.

10.3.3 Munkatársak tájékoztatási kötelezettsége a belső adatvédelmi felelős irányába:

a) Minden, személyes adatok kezelésével érintett folyamat kialakításába vagy megváltoztatásába a belső adatvédelmi felelőst be kell vonni.
b) A Munkatárs haladéktalanul köteles a belső adatvédelmi felelős felé írásban jelezni, ha az általa az adatkezelő nevében, feladatai ellátása során kezelt személyes adatok vonatkozásában a Munkatárs számára kétséges, hogy az adatkezelés jogalapja, célja, jellege, terjedelme jogszerű-e (például kétséges, hogy a kezelt adatok vonatkozásában rendelkezésre állnak-e az Érintettek hozzájárulásai). E kötelezettség elmulasztása esetén a Munkatárs mindennemű jogellenes adatkezelésért felelős az adatkezelővel szemben.

c) A belső adatvédelmi felelőst tájékoztatni kell az adatkezelő-en kívüli adattovábbításról.

d) Bármely olyan szerződés megkötése esetén, amely személyes adatok kezelésére, adatfeldolgozásra, vagy adattovábbításra vonatkozó rendelkezést tartalmaz, egyeztetni kell a belső adatvédelmi felelőssel, és a megállapodás egy példányát az adatkezelő adatkezelésre vonatkozó dokumentumai közötti megőrzés céljából a belső adatvédelmi felelős részére haladéktalanul át kell adni.

e) A Munkatársak – adatkezeléssel, jelen szabályzat, a GDPR vagy más jogszabály értelmezésével kapcsolatban felmerült – kérdéseikkel jogosultak és kötelesek a belső adatvédelmi felelőshöz fordulni, aki a lehetőségekhez mérten rövid időn belül válaszol a feltett kérdésre.

10.4 Szakterületi adatvédelmi felelősök

Az adatvédelmi szervezet részeként szakterületi adatvédelmi felelősök – a vezetés utasítása és a belső adatvédelmi felelős útmutatása alapján - végzik a saját szakterületükhöz tartozó alábbi adatvédelmi teendők operatív irányítását:

- minden új adatkezelési művelet előtt, előzetesen még megfelelő időben köteles a belső adatvédelmi felelőssel egyeztetni és annak útmutatásai szerint eljárni,
- adatvédelmi incidens felmerülése esetén késedelem nélkül értesíti a belső adatvédelmi felelőst,
- köteles a területéhez tartozó adatkezelési nyilvántartások vezetésére, ha az adatok kezelése nem szükséges, jogalapja megszűnt az adatok a nyilvántartásokból való törlés, azok azokban szereplő adatok tisztítása,
- beosztott munkavállalóik adatvédelmi tudatosságának fejlesztése, melynek keretében:
  - jó példát mutatnak a személyes adatok kezelése tekintetében,
  - folyamatosan egyeztetnek a beosztottakkal az adatkezelési műveletek jobb, biztonságosabb elvégzése érdekében,
- köteles felszólítani a szervezetéhez tartozó Munkatársat, hogy a szervezet tulajdonát képező olyan eszközökről, melyeket kizárólagosan használt (telefon, számítógép, stb.) törölje le az összes személyes adatát, magánlevelezését, még abban az esetben is, ha ez a belső szabályok által eleve tilos volt és nyilatkozatot tegyen, miszerint az utolsó munkában töltött napján letörölte, elvitte az esetlegesen vele kapcsolatos személyes adatokat,
- köteles a kilépő Munkatárs titoktartási nyilatkozatát bekérni, mely az üzleti titkokon túl a személyes adatokkal kapcsolatos adatokra is vonatkozik.

10.5 Helyi adatvédelmi felelősök

Az adatvédelmi szervezet részeként helyi adatvédelmi felelősök – a vezetés utasítása és a belső adatvédelmi felelős útmutatása alapján - végzik az adatkezelő egyes telephelyei kapcsán az alábbi adatvédelmi teendők operatív irányítását:

- ha a munkaterületen közzétett adatvédelemmel kapcsolatos képi vagy szöveges tájékoztatások hiányosak, azok észlelése vagy a beosztott Munkatársak jelzése alapján haladéktalanul köteles jelezni azt a belső adatvédelmi felelős felé
- minden új adatkezelési művelet előtt, előzetesen még megfelelő időben köteles a belső adatvédelmi felelőssel egyeztetni és annak útmutatásai szerint eljárni,
- adatvédelmi incidens felmerülése esetén késedelem nélkül értesíti a belső adatvédelmi felelőst,
- beosztott munkavállalóik adatvédelmi tudatosságának fejlesztése, melynek keretében:
  - jó példát mutatnak a személyes adatok kezelése tekintetében,
  - folyamatosan egyeztetnek a beosztottakkal az adatkezelési műveletek jobb, biztonságosabb elvégzése érdekében.

10.6 Adatkezeléssel foglalkozó beosztott Munkatársak

Az adatkezelő minden olyan alkalmazottja, aki adatkezeléssel érintőlegesen is foglalkozik, köteles

- személyes adatok kezelésére vonatkozó szabályokat – ideértve a jelen szabályzatot - ismerni és betartani, az adatkezelő által alkalmazott tájékoztatásokat ismerni,
- adatvédelmi oktatásokon részt venni, az ott elhangzottak a jogviszonyra vonatkozó utasításként kezelni, napi ügymenet gyakorlatába beépíteni,
- minden egyes személyes adat felvétele előtt az Érintett részére előzetes és számára érthető módon történő tájékoztatására, majd a hozzájárulás – feltéve, hogy az adatkezelés jogalapja hozzájárulás - dokumentált módon, jelen szabályzat, vagy a külön konkretizáló utasítások szerinti beszerzésére az elszámoltatható és átlátható adatkezelés elősegítése végett,
- bármilyen adatvédelemmel kapcsolatos panasz, szóbeli észrevétel vagy megjegyzés esetén köteles azt emailen jelezni a helyi, szakterületi és a belső adatvédelmi felelős részére,
- ha a munkaterületen közzétett adatvédelemmel kapcsolatos képi vagy szöveges tájékoztatások hiányosak, azt haladéktalanul köteles jelezni a helyi, szakterületi és a belső adatvédelmi felelős felé,
- személyes adatok védelméről köteles szervezetben elfoglalt helyének, feladat és hatáskörének megfelelően eleget tenni, így különösen, de nem kizárólagosan:
    - csak a szükséges és indokolt személyes adatok felvétele,
    - a személyes adatokat tartalmazó iratok, adathordozók védelme,
    - az író-, illetve munkaasztalát üresen tartani a jogosulatlan hozzáférés, az információvesztés és információ-sérülés kockázatának csökkentése érdekében (Clean Desk Policy),
    - csak olyan iratokat tartani az asztalon, amivel éppen dolgozik,
    - minden olyan személyes adatot tartalmazó irat, amivel éppen nem dolgozik biztonságosan elzárni,
    - a rá bízott iratokat záró szekrény a kulcsát a számzáras széfben tartani,
    - tilos a személyes adatokat tartalmazó iratok, adathordozók felügyelet vagy más biztonsági intézkedés nélküli, illetéktelenek számára elérhető módon történő tárolása,
    - az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak az adott iroda, adott munkaállomására beosztott munkavállaló jogosult használhatják,
    - tilos a személyi számítógépeket, munkaállomásokat felügyelet nélkül hagyni úgy, hogy azok a szokásos bejelentkezési procedúra nélkül használhatók legyenek,
    - a munkahely átmeneti elhagyásának esetén biztosítani kell, hogy a berendezést illetéktelen személy ne használhassa (pl. lock-olás).
    - a jelszavait bizalmas helyen tárolni,
    - a bizalmas információ kinyomtatására elkülönített nyomtatót kell használni, a kinyomtatott anyagokat a nyomtatás befejezése után azonnal el kell távolítani a nyomtatóból, a nyomtatót ellenőrizni szükséges,
    - a tévesen nyomtatott vagy felesleges példányokat, melyek személyes adatokat tartalmaznak, le kell darálni,
    - személyes adatot tartalmazó dokumentumok átadás-átvételekor gondoskodni kell arról, hogy csak az illetékes részére történjen azok átadása és azokhoz jogosulatlanul ne lehessen hozzáférni,
    - az irodákat biztonsági zárakkal, vagy ráccsal, vagy riasztóval kell felszerelni;
    - munkaidőn túl az irodákban csak engedéllyel lehet tartózkodni;
    - a rá bízott laptopot, telefont őrizni, azt tilos őrizetlen helyen (pld. gépjárműben) felügyelet nélkül hagyni.

11 Az Érintettek jogai

Az Érintettet személyes adatainak kezelésével kapcsolatban különféle jogok illetik meg. A megkeresések megválaszolása alapvetően a belső adatvédelmi felelős feladata.

Alapvetően a 2. sz. mellékletként csatolt űrlapokat kell alkalmazni a megkeresések megválaszolására.

Az Érintettet az alábbi jogok illetik meg:

11.1 Tájékoztatáshoz való jog

Az Érintett bármikor díjmentesen kérhet tájékoztatást az adatkezelő által kezelt adatairól, az adatkezelés céljáról, a tárolás időtartamáról és a tárolási időtartam meghatározására vonatkozó kritériumokról, valamint az adatok címzettjéről. Az Érintettet e vonatkozásban tájékoztatni kell a helyesbítéshez, törléshez és az adatkezelés korlátozásához való jogáról vagy a panasz benyújtásához való jogáról.

A fentieken túlmenően az Érintettnek jogában áll az adatait másolatban megkapni.

Kérdés vagy panasz esetén valamennyi Érintett jogosult a felelős szervezeti egységhez fordulni. A tájékoztatást megfelelő és érthető formában, haladéktalanul meg kell adni az érintettnek. A tájékoztatás írásban vagy elektronikus formában adható.

A tájékoztatás kérésével kapcsolatban ügyelni kell arra, hogy az információkat csak az Érintett kapja meg. Ezért a személyes adatokra vonatkozó tájékoztatás megadása előtt a tájékoztatást kérő személyt minden esetben egyértelműen azonosítani kell (pl. e-mail cím, regisztrációs szám, stb. alapján).

11.2 Helyesbítéshez, törléshez és az adatkezelés korlátozásához való jog

A fentieken túlmenően az Érintetteket az adatkezelő által tárolt pontatlan személyes adatai vonatkozásában helyesbítéshez való jog illeti meg.

Ezen kívül az adatkezelő köteles az általa tárolt személyes adatokat törölni, ha az adatok kezelésének jogalapja megszűnt. Abban az esetben, ha a személyes adatok törlésére vonatkozó jog fennáll, de a törlés nem lehetséges (pl. törvényes tárolási határidők miatt), a személyes adatok felhasználását a nem megengedett felhasználási célok vonatkozásában korlátozni kell.

Az Érintett kérheti az adatkezelés korlátozását, ha véleménye szerint az adatai helytelenek, az adatokat alapvetően törölni kellene, de azokra az adatkezelőnek jogi igények érvényesítéséhez még szüksége van, vagy az érintett az adatainak az adatkezelő által jogos érdek alapján történő kezelésével szemben tiltakozik, mert azt a saját helyzetével kapcsolatos okokra történő hivatkozással vitatja.

Abban az esetben, ha az adatkezelő az adatokat továbbította, az adatok esetleges címzettjeit tájékoztatni kell a helyesbítésről, törlésről vagy korlátozásról, kivéve, ha ez nem lehetséges vagy aránytalan ráfordítással járna.

11.3 Adathordozhatósághoz való jog

Ha az Érintett az adatait hozzájárulása alapján vagy az adatkezelővel fennálló szerződéses jogviszonya keretein belül az adatkezelő rendelkezésére bocsátotta, az adatkezelő köteles ezeket az adatokat kérés esetén széles körben használt formátumban a rendelkezésére bocsátani vagy – ha az technikai szempontból lehetséges – az általa megjelölt harmadik fél részére továbbítani.

11.4 Tiltakozáshoz való jog

Amennyiben az adatkezelő az adatokat jogos érdek alapján kezeli, úgy az Érintett a saját helyzetével kapcsolatos okokra történő hivatkozással jogosult az adatkezelés ellen tiltakozni. A tiltakozáshoz való jog nem áll fenn abban az esetben, ha az adatkezelő az adatokat pl. valamely jogának érvényesítéséhez vagy gyakorlásához használja fel, vagy az adatkezelő érdekei szemben állnak az adatkezelés befejezésével.

11.5 Hozzájárulás visszavonásához való jog

Amennyiben az Érintett a személyes adatainak kezelésével kapcsolatban hozzájárulását adta, úgy azt a jövőre nézve bármikor visszavonhatja, de ez nem érinti a hozzájárulás visszavonása előtt történt adatkezelés jogszerűségét. Ha az adatokra más összefüggésben szükség van (pl. jogszabályból fakadó archiválási kötelezettségek), akkor az adatokat csak az adott célra lehet felhasználni és az elérhetőségüket minden egyéb felhasználás vonatkozásában korlátozni kell.

11.6 Panasz benyújtásához való jog

Az Érintett bármikor jogosult közvetlenül az adatkezelőhöz fordulni esetleges panaszával. Ezen túlmenően jogosult a NAIH-nál panaszt benyújtani és a bírósághoz fordulni.

12 Záró rendelkezések

12.1 Kapcsolattartók

Adatvédelmi tisztviselő

Név: BDO Legal Jókay Ügyvédi iroda

Telefon: +36 1 235 30 10

E-mail: adatvedelem@bdolegal.hu

Belső adatvédelmi felelős:

Név: Kovács Katalin

Telefon: +36 46/ 325 000

E-mail: cinemis@t-online.hu

A szakterületi adatvédelmi felelősöket és helyi adatvédelmi felelősöket a vezetés külön utasításban jelöli ki.

12.2 Jelen szabályzat személyes adatok kezelésére vonatkozó rendelkezései kizárólag a természetes személyek személyes adatainak kezelésére vonatkoznak, tekintettel arra, hogy jogi személyek, illetve jogi személyeknek nem minősülő egyéb szervezetek adatai nem minősülnek az Infotv. szerinti személyes adatoknak.

12.3 A személyes adatok és a bizalmas információk védelme az adattárolás minden formáját érinti, így az adathordozók továbbadását, a képernyőtartalmakba történő betekintést vagy a számítógépről kinyomtatott anyagok továbbadását is.

12.4 A Munkatárs teljes kártérítési felelősséggel tartozik azért a kárért, amelyet szándékos vagy súlyosan gondatlan magatartásával jelen szabályzat vagy a vonatkozó jogszabályok megsértésével az adatkezelőnek okoz. A Munkatárs enyhe gondatlansággal okozott kár esetén négyhavi távolléti díja erejéig felel az okozott kárért.

12.5 Jelen szabályzat szerinti, az adatkezelőn belüli írásos értesítés e-mailen, megfelelő Munkatársnak az adatkezelő által biztosított e-mail címére történő elküldés útján is teljesíthető.

12.6 Jelen szabályzat 2021. július 01-től hatályos. A jelen szabályzatot az adatkezelő jogosult egyoldalúan megváltoztatni. A szabályzat változásairól az adatkezelő tájékoztatja a Munkatársakat

Elfogadva a 2021/5. sz. ügyvezetői utasítással.

Kelt: Miskolc, ...

Mellékletek:

1/a. sz. melléklet: Belső vizsgálati jegyzőkönyv biztonsági eseménnyel kapcsolatban

1/b. sz. melléklet: Adatvédelmi incidensről szóló jegyzőkönyv és bejelentés mintája

1/c. sz. melléklet: Adatvédelmi incidens nyilvántartás

2. sz. melléklet Űrlapok érintetti kérelmek megválaszolására

CINE-MIS Nonprofit Kft
Belső adatvédelmi szabályzat
1/a. sz. melléklet
Belső vizsgálati jegyzőkönyv biztonsági eseménnyel kapcsolatban

Vizsgálat tárgya	
Az esemény leírása	
Az érintett személyek hozzávetőleges száma és kategóriája	
Az eseménnyel érintett személyes adatok kategóriái és hozzávetőleges száma	
Amennyiben köthető az eset egy adatfeldolgozó személyéhez, ennek az adatfeldolgozónak az adatai és az általa végzett tevékenység	
Az esemény valószínű következményei adatvédelmi szempontból	
Az esemény orvoslására tett vagy tervezett, ideértve a sérelem hatásainak enyhítése érdekében tett vagy ajánlott intézkedéseket	
Bármilyen kockázattal jár-e az esemény az érintettek jogaira és szabadságaira nézve, ha igen, akkor a kockázatot magasnak kell-e értékelni, illetve ennek indokolása	
Az érintetteket az adatkezelő tájékoztatta-e az eseményről, ha igen, milyen formában (magas kockázat esetén, kivéve GDPR 34. cikk (3) bekezdés)	
Az esemény dátuma és időpontja	
A tudomásszerzés időpontja	
A tudomásszerzés módja	
Az esemény adatvédelmi incidensnek minősül-e, és ha igen, azt be kell-e jelenteni az illetékes felügyeleti hatóságnak	

Kelt: .....

Aláírás: .....

Név: .....

CINE-MIS Nonprofit Kft

CINE-MIS Nonprofit Kft

Belső adatvédelmi szabályzat
1/b. sz. melléklet
Adatvédelmi incidensről szóló jegyzőkönyv és bejelentés mintája
(a dőlt betűvel szedett rész csak az incidens hatóság részére történő bejelentése esetén alkalmazandó)

Adatvédelmi incidensről szóló jegyzőkönyv és bejelentés

Címzett: *Nemzeti Adatvédelmi és Információszabadság Hatóság*
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c, postacím: 1530 Budapest, Pf.:5
Telefon: (1) 391 1400, E-mail: ugyfelszolgalat@naih.hu

Tárgy: *Adatvédelmi incidens bejelentése*

Tisztelt Nemzeti Adatvédelmi és Információszabadság Hatóság!

Az Európai Unió általános adatvédelmi rendeletének (GDPR) 33. cikke alapján az alábbi adatvédelmi incidenst szeretnénk bejelenteni. Az incidenssel kapcsolatos további kérdések vagy szükséges információk kapcsán a jelzett elérhetőségeken mindenkor állunk a Tisztelt Hatóság rendelkezésére.

Az adatkezelő neve és elérhetőségei	CINE-MIS Nonprofit Kft. Cím: 3525 Miskolc, Kossuth u. 11. Telefon: +36 46 325 000 E-mail: cinemis@t-online.hu
Kapcsolattartó vagy adatvédelmi tisztviselő neve és elérhetősége	Az adatkezelő adatvédelmi tisztviselőjének elérhetőségei: adatvedelem@bdolegal.hu, telefonszám: +36 1 235 30 10, cím: BDO Legal, 1103 Budapest, Kőér u. 2/A. C. ép. Kapcsolattartó elérhetősége: [***]
Az adatvédelmi incidens **jellege**	
Az érintett személyek hozzávetőleges száma és kategóriája	
Az adatvédelmi incidenssel érintett adatok kategóriái és hozzávetőleges száma	
Amennyiben köthető az eset egy **adatfeldolgozó** személyéhez, ennek az adatfeldolgozónak az adatai és az általa végzett tevékenység	
Az adatvédelmi incidens **valószínű következményei**	
Az adatvédelmi incidens orvoslására tett vagy tervezett, ideértve a **sérelem hatásainak enyhítése érdekében** tett vagy ajánlott intézkedéseket	
Bármilyen kockázattal jár-e az incidens az érintettek jogaira és szabadságaira nézve, ha igen, akkor a kockázatot magasnak kell-e értékelni, illetve ennek indokolása	
Az **érintetteket az adatkezelő tájékoztatta-e** az incidensről, ha igen, milyen formában (magas kockázat esetén, kivéve GDPR 34. cikk (3) bekezdés)	
Az esemény **dátuma és időpontja**	
A **tudomásszerzés** időpontja	
A tudomásszerzés módja	
Indokolás arra vonatkozólag, amennyiben a bejelentésre az adatkezelő tudomásszerzésétől számított több, mint 72 óra elteltével kerül sor	

Kelt: .....

Aláírás: .....
Név: .....
CINE-MIS Nonprofit Kft.

CINE-MIS Nonprofit Kft.
Belső adatvédelmi szabályzat
1/c. sz. melléklet
Adatvédelmi incidens nyilvántartás

Vállalkozás neve CINE-MIS Nonprofit Kft.

2021

Incidens sorszáma	Incidens megnevezése	Incidens dátuma	Az incidenssel kapcsolatos jelentős tények leírása	Az incidens hatásai	Az incidens orvoslására tett intézkedések	Csatolt mellékletek (pl. kitöltött vizsgálati jegyzőkönyv, bejelentés)
1/2021						
2/2021						
3/2021						
4/2021						
5/2021						

CINE-MIS Nonprofit Kft.
Belső adatvédelmi szabályzat
3. sz. melléklet

Űrlapok érintetti kérelmek megválaszolására

A kérelmekre késedelem nélkül, legfeljebb 1 hónapon belül válaszolni kell. A tájékoztatást és intézkedést díjmentesen kell biztosítani (kivételekkel kapcsolatban ld. szabályzat megfelelő rendelkezését). Az érintett kérelmének beérkezésekor mindenekelőtt meg kell győződni a személyazonosságáról, amire lehetőség van a szerződéses adatok, esetleg a lakcím, írásbeli megkeresés esetén az aláírás ellenőrzésével. Ha kétség van az érintett személyazonosságával kapcsolatban, akkor észszerű mértékben további információk kérhetők be. Tájékoztatás csak az érintettel közölhető (családtaggal, egyéb rokonnal, ismerőssel tájékoztatás nem közölhető tájékoztatás, kivéve a kiskorú törvényes képviselőjét).

A válasz kitöltése és elküldése alapvetően a belső adatvédelmi felelős feladata, ezért bármely felhasználást megelőzően egyeztessen a belső adatvédelmi felelőssel.

Az egyes kérelmek megválaszolásának mintái:

A) TÁJÉKOZTATÁSHOZ VALÓ /HOZZÁFÉRÉSI JOGGAL KAPCSOLATOS KÉRELEMRE ADANDÓ VÁLASZ MINTÁJA

„érintett neve és címe
dátum

Tájékoztatáshoz, illetve hozzáféréshez való jog – Az Ön (dátum) napján kelt megkeresése

Tisztelt Uram/ Asszonyom,

Az Európai Unió adatvédelmi rendeletének (GDPR) 15. cikke alapján ezúton igazoljuk az Ön számára, hogy a CINE-MIS Nonprofit Kft. az Ön személyes adatait kezeli.

A továbbiakban az alábbi információkat bocsátjuk a rendelkezésére:

- **1. számú melléklet**: a GDPR 15. cikk (1) bekezdése szerinti tájékoztatás és
- **2. számú melléklet:** a GDPR 15. cikk (3) bekezdése alapján az általunk kezelt személyes adatairól készült másolat.

Adatvédelmi tájékoztatónkat itt olvashatja [***] [vagy, nem a Honlappal kapcsolatos adatkezelés esetén] mellékelten csatoljuk.

Az adatkezelő adatvédelmi tisztviselőjének elérhetőségei: adatvedelem@bdolegal.hu, telefonszám: +36 1 235 30 10, cím: BDO Legal, 1103 Budapest, Kőér u. 2/A. C. ép.

További kérdések, illetve kérések esetén kérjük lépjen velünk kapcsolatba a lenti elérhetőségek bármelyikén:

Név: CINE-MIS Nonprofit Kft.
Cím: 3525 Miskolc, Kossuth u. 11.
Telefon: +36 46 325 000
E-mail: cinemis@t-online.hu

Tisztelettel:

…"

1. számú melléklet: Információnyújtás az adatvédelmi GDPR 15. cikk (1) bekezdése alapján

A CINE-MIS Nonprofit Kft. a GDPR 15. cikkében foglaltak alapján a következő információkat bocsátja rendelkezésére és tájékoztatja arról, hogy az Ön személyes adatait vállalkozásunk kezeli az alábbiak szerint:

1. **Az adatkezelés célja:**

[Itt az összes adatkezelési cél rövid leírása szükséges; elegendő kulcsszavak megadása, pl: az érintettel való szerződéskötés vagy a szerződés teljesítése érdekében történő adatkezelés, áruszállítás, könyvelési célok, közvetlen marketingtevékenységek, adatbiztonság, törvényi kötelezettség teljesítése.]

2. **Személyes adatok kategóriái:**

[A kategóriák rövid leírása, pl: elérhetőségre vonatkozó adatok, banki adatok, szerződéses viszonyra vonatkozó adatok].

3. **Címzettek/címzettek kategóriái, akikkel a személyes adatokat közölték vagy közölni fogják, ideértve a harmadik országbeli címzetteket:**

[A címzetteket meg kell nevezni (legalább kategóriánként, pl: IT- szolgáltató). Az érintett személyt tájékoztatni kell arról is amennyiben adatainak továbbítását az Európai Unión kívüli országba tervezik]

4. **Adott esetben a harmadik országba történő adattovábbítás jogalapja:**

[Amennyiben az adattovábbítást egy Európai Unión kívüli országba tervezik akkor erről az érintett személyt a jogalap megjelölésével tájékoztatni kell (pl.: az ország egy megfelelő adatvédelmi szintet biztosít, kötelező erejű vállalati szabályok kerülnek alkalmazásra.]

5. **Tárolási időtartam vagy – amennyiben ennek feltüntetése nem lehetséges – a tárolási időtartam meghatározásának jellemzői:**

[A személyes adat tárolásának időtartamára vonatkozó információk. Amennyiben ennek meghatározása nem lehetséges, akkor a tájékoztatásnak a tárolási időtartam meghatározásának kritériumait kell tartalmaznia. Az időtartamot egyértelmű formában kell feltüntetni. (napok, hónapok, évek). Lásd bővebben: a belső adatvédelmi szabályzat törlési koncepcióra von. 1. sz. mellékletét]

6. **A helyesbítéshez, törléshez, zároláshoz, tiltakozáshoz való joga:**

Amennyiben az általunk kezelt személyes adatok helytelenek vagy hiányosak, ha Ön tiltakozást nyújtott be az adatkezeléssel szemben, vagy az adatkezelésre jogszerűtlenül kerül sor, akkor kijavítjuk, illetve kiegészítjük a személyes adatokat, korlátozzuk az adatkezelést vagy töröljük a személyes adatokat, amennyiben erre a törvény alapján lehetőség van. Kérem, hogy az adataiban történt változásokról haladéktalanul tájékoztasson minket.

7. **Felügyeleti hatósághoz címzett panasztételi jog:**

Panasz esetén a következő felügyeleti hatóságokhoz fordulhat:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postacím: 1530 Budapest, Pf.:5
Telefon: 0630 1 391 1400
Fax: 0636 1 391 1410
E-mail: ugyfelszolgalat@naih.hu

8. **A megszerzett adatok forrására vonatkozó információk:**

[ez csak akkor releváns, amennyiben a személyes adatok beszerzése nem közvetlenül az érintett személytől történt; információ arra vonatkozólag, hogy kitől kerültek átadásra az adatok (pl: lakcím) vagy azok honnan származnak, amennyiben különböző forrásból származnak akkor elegendő általánosan megjelölni a forrásokat. Pl. online tudakozó, más állásportál vagy munkaközvetítő megnevezése stb.]

9. **Automatizált döntéshozatalra vonatkozó információk (beleértve a profilalkotást):**

Vállalkozásunk nem alkalmaz automatizált döntéshozatalt, illetve profilalkotást.

2. számú melléklet: Adatok másolata

B) KOMBINÁLT KÉRELEMRE VONATKOZÓ VÁLASZ MINTÁJA

„érintett neve és címe
dátum

.... napján kelt kérelem az Ön személyes adatainak helyesbítésére/ törlésére/ zárolására/ átadására

Tisztelt Uram/ Asszonyom,

A ... napján kelt kérelmére válaszul hivatkozunk az adatvédelmi GDPR (GDPR) 16. cikkében foglaltakra.

Igazoljuk, hogy kérelmét megkaptuk, és hogy a CINE-MIS Nonprofit Kft. kezeli az Ön személyes adatait. A kérelem érvényesítését követően az alábbiakról tájékoztatjuk:

A helytelen személyes adatait kérésének megfelelően kijavítottuk./

A személyes adatait kérésének megfelelően kiegészítettük./

A személyes adatait kérésének megfelelően töröltük./

A személyes adatainak kezelését kérésének megfelelően korlátoztuk./

Kérésének megfelelően eleget teszünk az adatok átadásának. Mellékelten találja az Ön által rendelkezésünkre bocsátott személyes adatainak másolatát./

Kérésének megfelelően eleget teszünk az adatok átadásának és az Ön által rendelkezésünkre bocsátott személyes adatainak másolatát továbbítjuk az Ön által meghatározott címzett részére./

Tiltakozása miatt az Ön személyes adatait a meghatározott célra nem kezeljük tovább./

A személyes adatainak kezelésére vonatkozó tiltakozása ellenére adatait a GDPR 6. cikk (1) bekezdésének f.) pontja alapján továbbra is kezelni fogjuk, mivel az adatkezelést kötelező erejű jogszabályi indokok alapozzák meg. Ezek az alábbiak:..... /

A személyes adatainak kezelésére vonatkozó tiltakozása ellenére, adatait a GDPR 6. cikk (1) bekezdésének f.) pontja alapján továbbra is kezelni fogjuk mivel ezeket az adatokat jogi igényérvényesítés indokolására, gyakorlására, védelme érdekében kezeljük./

Kérelmét ezúton sajnálattal kénytelenek vagyunk elutasítani, mivel az nyilvánvalóan megalapozatlan / túlzó, az alábbi okok miatt:...../

Tájékoztatom, hogy kérelme teljesítéséért .....összegű díjat számítunk fel, mivel kérelme nyilvánvalóan megalapozatlan/túlzó, az alábbi okok miatt:...../.

A kérelem elutasítása miatt az illetékes felügyeleti hatóságnál panaszt nyújthat be vagy jogorvoslattal élhet.

A felügyeleti hatóság:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Postacím: 1530 Budapest, Pf.:5
Telefon: 06 1 391 1400
Fax: 06 1 391 1410
E-mail: ugyfelszolgalat@naih.hu

Személyes adatainak címzettjeit személyes adatainak (kijavításáról, törléséről, zárolásáról) tájékoztattuk./

Személyes adatainak címzettjeit személyes adatainak (kijavításáról, törléséről, zárolásáról) nem tájékoztattuk, mivel ez nem lehetséges az alábbi okok miatt...../

Személyes adatainak címzettjeit személyes adatainak (kijavításáról, törléséről, zárolásáról) nem tájékoztattuk, mivel ez aránytalan költséggel járna./

Az adatkezelő adatvédelmi tisztviselőjének elérhetőségei: adatvedelem@bdolegal.hu, telefonszám: +36 1 235 30 10, cím: BDO Legal, 1103 Budapest, Kőér u. 2/A. C. ép.

További kérdések, illetve kérések esetén kérem, vegye fel velünk a kapcsolatot az alábbi elérhetőségek bármelyikén

Név: CINE-MIS Nonprofit Kft.
Cím: 3525 Miskolc, Kossuth u. 11.
Telefon: +36 46 325 000
E-mail: cinemis@t-online.hu

Tisztelettel:

..."