BUDAPEST KÖZÚT

Adatvédelmi és Adatbiztonsági Szabályzat

Hatálybalépés dátuma: 2024. augusztus 5.

TARTALOM

MELLÉKLETEK

MÓDOSÍTÁSOK

2024.08.05:	Szervezeti változások átvezetése; 1.1, 1.3-1.5, 2.1.2-2.1.5, 2.2.2 pontok aktualizálása.
2023.08.01:	A teljes szabályzat aktualizálása.
2018.07.01:	A teljes szabályzat aktualizálása.
2017.05.15:	A teljes szabályzat aktualizálása.

1 ÁLTALÁNOS RENDELKEZÉSEK

A Budapest Közút Zrt. a személyes adatok kezelése, nyilvántartása, feldolgozása és továbbítása során az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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 (továbbiakban: általános adatvédelmi rendelet), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.), valamint az adatvédelemre vonatkozó egyéb jogszabályi rendelkezések és hatósági ajánlások alapján jár el. A Szabályzatban meghatározott adatbiztonsági szabályok ezért ezen elsődleges cél megvalósíthatóságának érdekében, a személyes adatokra korlátozódnak.

1.1 A Budapest Közút Zrt. Adatvédelmi és Adatbiztonsági Szabályzatának (AASZ) célja

Az AASZ célja

- A Budapest Közút Zrt. (továbbiakban: Társaság) által kezelt személyes adatok tekintetében érvényt szerezni a vonatkozó jogszabályoknak, biztosítani az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozni a személyes adatokhoz való jogosulatlan hozzáférést, a személyes adatok megváltoztatását és azok jogosulatlan nyilvánosságra hozatalát, valamint meghatározni a Társaság által vezetett nyilvántartások adatvédelemi előírások szerinti kezelésének rendjét.
- A Társaságon belüli egységes adatvédelmi és adatbiztonsági szemlélet kialakítása, az adatvédelmi jogszabályok, előírások maradéktalan érvényesítése.
- Olyan adatvédelmi, adatbiztonsági rendszert, felügyeleti- és ellenőrzési eljárásokat működtetni, melyekkel az adatvédelmi előírások megsértése megelőzhető, az adatvédelmi incidensek elkerülhetők, illetve esetleges bekövetkezésük esetén az incidens érintettekre gyakorolt hatása enyhíthető, az incidenskezelési eljárás során az eset körülményei felderíthetők és a szükséges intézkedések haladéktalanul megtehetők.

1.2 Az AASZ hatálya

Az AASZ személyi hatálya

- Kiterjed a Társasággal munkaviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban álló természetes személyekre.
- A Társasággal szerződéses jogviszonyban álló természetes személyekre, és egyéb jogi entitásokra és az általuk a Társaság munkaterületein, vagy a Társaság részére munkatevékenységet végző munkavállalókra vonatkozóan is.

Az AASZ területi hatálya

Kiterjed a Társaság valamennyi gazdasági egységére – telephelytől függetlenül –, ahol személyes adatokat kezelnek.

Az AASZ tárgyi hatálya

Kiterjed a Társaság szervezeti egységeinél folytatott minden személyes adat részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik, vagy amelyeket egy nyilvántartási rendszer részévé kívánnak tenni.

A Társaság kezelésében lévő közérdekű adatokra és közérdekből nyilvános adatokra vonatkozó szabályokat a Társaság mindenkor hatályos, a közérdekű adatok elektronikus közzétételének és a közérdekű adatok megismerésének rendjéről szóló szabályzata határozza meg.

Az AASZ időbeli hatálya

Időbeli hatálya a hatálybalépés napjától visszavonásig érvényes.

1.3 Az adatvédelmi tevékenységek működtetésének feltételrendszere

A Társaság adatvédelmi feltételrendszerének megteremtéséhez szükséges személyi- és tárgyi feltételek kialakításáról a Társaság vezérigazgatója gondoskodik.

Az Adatvédelmi tisztviselő feladatkörére az adatvédelemmel kapcsolatos felügyeleti feladatok ellátására e szabályzat rendelkezései az irányadók.

Az adatvédelmi tevékenységek működtetéshez szükséges pénzügyi fedezetet a Társaság éves pénzügyi előirányzatában tervezni kell.

1.4 Az adatvédelmi előírások, kötelezettségek megismertetési – megismerési kötelezettsége

Az adatvédelmi előírásokat minden, a Társasággal munkaviszonyban, illetve munkavégzésre irányuló egyéb jogviszonyban álló személlyel, a munkafeladatai ellátásához szükséges mértékben dokumentálható módon ismertetni kell.

A Társaság munkavállalói számára a munkaviszonnyal összefüggő adatkezelésekről a munkaviszony megkezdésekor, illetve az eljárási cselekmények, adatkezelési tevékenységek aktuálissá válásakor a Humán erőforrás főosztály az Adatvédelmi tisztviselő által rendelkezésre bocsátott tájékoztatókban, illetve vele előzetesen egyeztetett tartalommal nyújt érdemi tájékoztatást.

A Társaság fő tevékenységeinek adatkezelési ismereteiről a honlapján nyújt tájékoztatást.

Az adatkezelésre és adatfeldolgozásra jogosult munkavállalók részére az adatvédelmi előírásokat, illetve jogszabályi változásokat az Adatvédelmi tisztviselő oktatja.

Aki az AASZ-ből megismert előírásokat, kötelezettségeket nem tartja be, azzal szemben a hatályos Társasági szabályozók alapján hátrányos jogkövetkezmények, szerződés esetén, az abban meghatározott szankciók alkalmazhatók.

1.5 Az AASZ jogszabályi alapja, szabályozási környezete, kapcsolata a belső szabályzatokkal

Az AASZ főbb jogszabályi alapja

- EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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 (továbbiakban: általános adatvédelmi rendelet)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.)
- Magyarország Alaptörvényének VI. cikke
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2012. évi I. törvény a munka törvénykönyvéről
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. Törvény
- 2013. évi V. törvény a Polgári Törvénykönyvről
- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény
- a minősített adat védelméről szóló 2009. évi CLV törvény
- az államháztartásról szóló 2011. évi CXCV. törvény (továbbiakban: Áht.)
- a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény

Az AASZ harmonizációja a Társaság belső szabályzataihoz

Az AASZ-ben rögzített előírásoknak, kötelezettségeknek összhangban kell lennie az alábbi szabályozások adatvédelmet érintő előírásaival.

- Információbiztonsági Szabályzat (továbbiakban: IBSZ)

- Iratkezelési Szabályzat és Irattári terv (továbbiakban: Iratkezelési Szabályzat)
- Szabályzat a Közérdekű adatok elektronikus közzétételének és a közérdekű adatok megismerésének rendjéről
- Belső visszaélés-bejelentési Szabályzat
- Szervezeti és Működési Szabályzat
- Kollektív Szerződés

A szervezeti egységek saját kiadású szabályozásaiban a jelen AASZ előírásait kell érvényesíteni. Az adatkezeléssel kapcsolatos alapfogalmak értelmezését az AASZ 1. számú melléklete tartalmazza.

2 AZ ADATVÉDELEM, ADATBIZTONSÁG SZERVEZETE, FOLYAMATA

2.1 Az adatvédelem szervezete, az AASZ előírások érvényesítése, felelősségek

2.1.1 A Budapest Közút Zrt. vezérigazgatója

A Budapest Közút Zrt. vezérigazgatója irányítja és ellenőrzi az adatvédelemmel kapcsolatos feladatok végrehajtását.

Megbízza, illetve kinevezi az Adatvédelmi tisztviselőt, biztosítja a feladataik elvégzéséhez szükséges feltételeket.

Kiadja az Adatvédelmi és Adatbiztonsági Szabályzatot.

2.1.2 A Jogi és igazgatási főosztály vezetője

A Vezérigazgató irányításával ellátja az Adatvédelmi tisztviselő felügyeletét.

- Feladata az adatvédelemmel kapcsolatos feladatok ellátásának koordinálása,
- biztosítja az Adatvédelmi tisztviselő bevonását a Társaság adatvédelemmel kapcsolatos feladatainak ellátásába, a Társaság személyes adatok kezelésével járó tevékenységeinek tervezésébe,
- biztosítja az Adatvédelmi tisztviselő munkájának külső befolyástól mentes ellátását és támogatja őt a munkájában,
- vezeti az adatkezelési tevékenységek nyilvántartását, illetve fogadja az esetleges új adatkezelések bejelentéseit.

2.1.3 Az Adatvédelmi tisztviselő

Az általános adatvédelmi rendelet 37. cikkében foglaltak alapján a Társaság Adatvédelmi tisztviselőt jelölt ki.

A Társaság köteles adatvédelmi tisztviselőjét a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) nyilvántartásába bejelenteni.

Az Adatvédelmi tisztviselő számára biztosítani kell, hogy a személyes adatok védelmével kapcsolatos bármely ügybe megfelelő módon és időben bekapcsolódjon.

Megfelelő erőforrásokat kell biztosítani arra, hogy az Adatvédelmi tisztviselő feladatait végrehajthassa.

Az Adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől nem fogadhat el. Az Adatvédelmi tisztviselő független a Társaság szervezeti egységeitől és a többi belső kontroll funkciótól.

Az Adatvédelmi tisztviselő közvetlenül a Társaság vezérigazgatójának tartozik felelősséggel.

Az Adatvédelmi tisztviselő felügyeletét a Társaság vezérigazgatójának irányításával a Jogi és igazgatási főosztályvezető látja el.

Feladatai teljesítésével kapcsolatban titoktartási kötelezettség terheli. Ez a kötelezettség a kijelölését vagy megbízásának megszűnését követően is fennáll.

Az Adatvédelmi tisztviselő egyidejűleg más adatkezelőnél vagy adatfeldolgozónál is betölthet azonos feladatkört akkor, amennyiben az nem eredményez összeférhetetlenséget.

Az Adatvédelmi tisztviselő az általános adatvédelmi rendeletben és az Infotv-ben foglalt feladatok ellátása körében elsősorban

- elkészíti, illetve véglegesíti és aktualizálja a Társaság adatkezeléseiről szóló Tájékoztatókat, a főtevékenységekre vonatkozók honlapon történő közzétételét ellenőrzi,
- ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a jelen szabályzat rendelkezéseinek betartását; adatvédelmi incidens esetén közreműködik a vizsgálatban, amelyben számba veszi az incidens körülményeit, hatását, javaslatot tesz az adatkezelő számára az intézkedésekre, koordinálja a résztvevő szervezeti egységeket,
- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az Érintettek jogainak biztosításában,
- kivizsgálja a személyes adatkezeléssel összefüggésben hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót,
- felügyeli a belső adatvédelmi nyilvántartás vezetését,
- támogatja az adatkezelőt és adatfeldolgozót a jogszabályi előírások teljesítésében,
- kapcsolatot tart a Nemzeti Adatvédelmi és Információszabadság Hatósággal (NAIH, továbbiakban: Hatóság) a Társaságot érintő adatvédelmi ügyekben,
- a Jogi és igazgatási főosztályvezetővel együttműködve koordinál az egyes szervezeti egységek között az egységes adatvédelmi szemlélet megvalósítása érdekében,
- szakmai tanácsokkal segíti a hatásvizsgálat készítését,
- a Jogi és igazgatási főosztály kérésére a más vállalkozással kötött szerződések keretein belül adatvédelmi kérdésekben tanácsadó, ellenőrző tevékenységet végez,
- véleményezi a részére megküldött, adatvédelmi kérdéseket érintő belső szabályozási dokumentumok tervezetét,
- az adatvédelmi kérdésekkel összefüggésben tájékoztatja a Társaság vezetését,
- adatvédelmi szempontból kritikus szabályzatokat felülvizsgálja, azok módosítására szövegszerű javaslatot tesz,

Az Adatvédelmi tisztviselő köteles évente legalább 1 alkalommal általános adatvédelmi oktatást tartani a Társaság munkavállalói részére.

Az Adatvédelmi tisztviselőt az oktatások megszervezésében és lebonyolításában a Jogi és igazgatási főosztály vezetője, a Humán erőforrás főosztály vezetője és az Informatikai igazgató, illetve az általuk kijelölt munkavállaló segíti.

2.1.4 Az adatkezelő szervezeti egység vezetője

- biztosítja, hogy a személyes adatok kezelése a Társaság vezérigazgatójának vagy a Jogi és igazgatási főosztály vezetőjének utasításai és/vagy az Adatvédelmi tisztviselő javaslatainak megfelelően, a GDPR-nak és a releváns jogszabályoknak megfelelően történjen,
- szükség esetén kikéri az Adatvédelmi tisztviselő tanácsát,
- biztosítja, hogy az Adatvédelmi tisztviselő ellenőrizhesse az adatkezelő szervezeti egység által folytatott, személyes adatok kezelésével járó tevékenységeket,
- elvégzi a belső adatvédelmi nyilvántartásba bejelentésre kötelezett nyilvántartások bejelentését,
- részt vesz a Társaság Adatvédelmi és Adatbiztonsági Szabályzatának elkészítésében és aktualizálásában,
- kérésre közreműködik az Adatvédelmi tisztviselő feladatainak ellátásában,
- kérésre részt vesz az adatvédelem terén bekövetkezett incidensek kivizsgálásában,
- intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az Adatvédelmi tisztviselőt, és informatikai rendszer érintettsége esetén az elektronikus információs rendszer üzemeltetőjét,
- új adatkezelés létrehozása esetén közreműködik az adatvédelmi követelmények betartásában, konzultál az Adatvédelmi tisztviselővel,
- intézkedik az Adatvédelmi tisztviselő felé az Érintett által hozzá benyújtott, tiltakozás, illetve tájékozódási jog teljesülése érdekében.

- A szervezeti egységébe érkező új munkatársakról, valamint az onnan távozókról köteles az Informatikai igazgatóságot írásban értesíteni a jogosultságok aktualizálása céljából, akkor is, ha a személyi változás belső áthelyezésből ered. Ez a kötelezettség a szerződéssel alkalmazott munkatársakra vonatkozóan is fennáll.

2.1.5 Az adatkezelést végző munkavállaló

- köteles gondoskodni arról, hogy az adatkezelés teljes folyamatában maradéktalanul érvényesüljenek az adatvédelmi előírások,
- kezeli a feladata ellátása során birtokába került adatokat, ügyel a nyilvántartások biztonságos kezelésére és tárolására,
- gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz illetéktelen személy ne férhessen hozzá,
- betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat,
- részt vesz az adatkezeléssel, adatvédelemmel összefüggő belső szakmai képzéseken.

2.1.6 Az információbiztonsági felelős

- a jogszabályok és belső szabályzatok előírásainak megfelelően segíti az Adatkezelővel szemben támasztott adatbiztonsági követelmények teljesülését,
- együttműködik az Informatikai igazgatósággal az információbiztonsági követelmények érvényesülésében,
- együttműködik az Adatvédelmi tisztviselővel a személyes adatok biztonságával kapcsolatos ügyekben,
- szükség esetén részt vesz az adatvédelmi incidenskezelő csoport munkájában,
- szükség esetén felkérésre részt vesz az adatvédelmi hatásvizsgálat lefolytatásában.

2.2 Az adatkezelési tevékenységek nyilvántartása

Az adatkezelést végző szervezeti egység vezetője nyilvántartásba vétel céljából, a 4. számú melléklet alapján köteles a Társaság Jogi és igazgatási főosztály vezetőjének bejelenteni az új, e szabályzat hatálybalépését követően megkezdett adatkezelésre vonatkozó adatokat.

Az adatkezelésről szóló bejelentést az adatkezelés megkezdését megelőzően legalább 15 (tizenöt) nappal meg kell küldeni.

Meglévő adatkezelésből történő legyűjtés eredményeként létrejövő adatkezelés új adatkezelésnek számít, amennyiben az adatkezelés célja eltérően kerül megfogalmazásra, vagy az adatkezelő személye megváltozik. Ilyen esetben erre vonatkozóan is bejelentési, illetve szabályzatkészítési kötelezettség lép életbe. Vitás esetben az Adatvédelmi tisztviselő állásfoglalását kell kérni.

A belső adatkezelési tevékenységek nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője 8 (nyolc) napon belül köteles bejelenteni a Társaság Jogi és igazgatási főosztály vezetőjének, aki ennek megfelelően módosítja a belső adatvédelmi nyilvántartás adatait.

2.2.1 Személyes adatok kezelése, alapelvek

Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Személyes adat a Társaság által akkor kezelhető, ha annak az általános adatvédelmi rendelet szerinti megfelelő jogalapja biztosított.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

A Társaság gondoskodik arról, hogy az adatokhoz csak olyan munkavállalók, adatfeldolgozók férhessenek hozzá, akik, vagy amelyek adatkezelése, adatfeldolgozása vonatkozásában a hozzáférés igazolható.

Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és – ha az adatkezelés céljára tekintettel szükséges – naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen

azonosítani. A Társaság ezért folyamatosan törekszik arra, hogy az érintett szervezetek figyelmét felhívja az adatok meghatározott időnkénti frissítésére, amelyet egyéb belső szabályzatokban is külön meghatározhat.

Személyes adat akkor is kezelhető, ha az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.

Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az e törvény és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor a Társaság az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

A Társaság szervezetén belül a kezelt személyes adat – a feladat elvégzéséhez szükséges mértékben és ideig – csak az üggyel érintett gazdasági egységhez továbbítható, feltéve, hogy a személyes adatok megismerése nélkül az ügyben érdemileg eljárni nem lehet. Amennyiben az adatkezelés célhoz kötöttsége kétséges, a személyes adatgazda köteles a kérdésben az Adatvédelmi tisztviselő állásfoglalását beszerezni.

A személyes adatok kezelése az Adatkezelő esetében számos tevékenység vonatkozásában közérdekű feladat végrehajtásához szükséges.

Az adatkezelés jogalapja

Amennyiben az adatkezelés az Adatkezelő közérdekű vagy rá ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, abban az esetben a személyes adatok kezelésének jogalapja a GDPR 6. cikk (1) bekezdésének e) pontja.

Személyes adatot az adatkezelő az Érintett hozzájárulásán túlmenően akkor kezelhet, ha

- az adatkezelés szerződés teljesítéséhez, vagy a szerződés megkötését megelőző Érintett kérései alapján szükséges,
- az adatkezelés az adatkezelő jogi kötelezettségnek teljesítéséhez szükséges,
- az Érintett létfontosságú érdekeinek védelme miatt szükséges,
- az adatkezelés az adatkezelő vagy egyéb harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

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

Különleges adatot a Társaság meghatározott esetekben kezelhet, ha

- az Érintett kifejezett hozzájárulását adta,
- az adatkezelőre vonatkozó foglalkoztatási, szociális biztonsági és védelmi kérdéseket szabályozó előírásai alapján szükséges,
- az Érintett személy létfontosságú érdekei miatt szükséges, és ha az Érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását adni,
- valamilyen jogi igény érvényesítéséhez kell,
- megelőző munkahelyi egészségügyi célokból van szükség és megfelelő egészségügyi szakértelemmel kijelölt szerv vagy személy felelőssége és titoktartása mellett történik az adatkezelés.

Ha az Érintett a Társasággal írásban kötött szerződés teljesítése érdekében adja meg személyes adatait, akkor a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az

Érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételét.

Az Érintett előzetes tájékoztatásának követelménye

Az Érintett részére a személyes adatok kezelését megelőzően, illetve az adatok felvételekor tájékoztatást kell adni a GDPR 13-14. cikke szerinti tartalommal.

Az adatkezelés megkezdése előtt az adatkezelést végzőnek az Érintettet – kérés nélkül is – előzetesen egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen

- az adatkezelés milyen jogalappal történik (hozzájárulás vagy egyéb jogalap alapján),
- az adatkezelésre milyen célból van szükség,
- az adatkezelő személyéről, adatfeldolgozás esetén az adatfeldolgozó kilétéről,
- az adatkezelés időtartamáról,
- a kezelt adatok köréről,
- az adattovábbítás címzettjeiről,
- az Érintett jogairól,
- jogorvoslati lehetőségeiről: adatvédelmi hatósághoz, bírósághoz forduláshoz lehetőségről,
- kik ismerhetik meg az adatokat.

Kötelező adatkezelés esetén a tájékoztatás megtörténhet az információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

A tájékoztatást:

a) az álláspályázatot benyújtók számára az álláspályázati felhívás közzétételekor, illetve a pályázati eljárást megelőzően közvetlenül a pályázónak kell nyújtani a Humánpolitikai Szabályzatban szereplő Adatkezelési tájékoztató által;

b) az Adatkezelővel munkaviszonyt létesítők részére a jogviszony létrejöttekor a vonatkozó adatkezelési tájékoztatók szerinti tartalommal kell nyújtani a Humánpolitikai Szabályzatban szereplő Adatkezelési tájékoztató által.

Az Adatkezelő főtevékenységeinek ellátásából adódó tevékenységeiről a tájékoztatásokat a https://www.budapestkozut.hu/ oldalon kell közzétenni az Adatvédelmi tisztviselő javaslatainak figyelembevételével.

2.2.2 Az Érintett jogai

Hozzáféréshez való jog

Az érintett személy kezdeményezheti személyes adataihoz való hozzáférést. E jog keretében a Társaság honlapján közzétett elérhetőségeken keresztül, írásban tájékoztatást kérhet a Társaságtól arról, hogy

- milyen személyes adatait,
- milyen jogalapon,
- milyen adatkezelési cél miatt,
- milyen forrásból,
- mennyi ideig kezeli,
- A Társaság kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait. A Társaság az érintett kérelmét legfeljebb egy hónapon belül, az általa megadott elérhetőségre küldött levélben teljesíti.

A helyesbítéshez való jog

Az érintett személy a Társaság honlapján közzétett elérhetőségeken keresztül, írásban kérheti, hogy a Társaság módosítsa valamely személyes adatát (például bármikor megváltoztathatja az e-mail címét vagy postai elérhetőségét).

A Társaság a kérelmet legfeljebb egy hónapon belül teljesíti, és erről az általa megadott elérhetőségre küldött levélben értesíti.

A törléshez való jog

Az érintett személy a Társaság honlapján közzétett elérhetőségeken keresztül, írásban kérheti a Társaságtól a személyes adatainak a törlését.

A Társaság köteles a személyes adatot törölni, amennyiben

- az adatokra nincs többé szükség,
- ha az érintett visszavonta hozzájárulását,
- ha az érintett tiltakozik az adatkezelés ellen,
- ha azt jogellenesen kezelték, vagy jogszabály alapján kell törölni.

A Társaság a kérelmet legfeljebb egy hónapon belül teljesíti, és erről az e célból megadott elérhetőségre küldött levélben értesíti az érintettet.

Az adatkezelés korlátozásához való jog

Törlés helyett a Társaság korlátozza a személyes adatot, ha

- az Érintett vitatja az adatkezelést a pontosságra való hivatkozással,
- az adatkezelés jogellenes, de az Érintett ellenzi a törlést,
- nincs szükség az adatkezelésre, de valamely jogi igény előterjesztése miatt szükséges lehet,
- az Érintett tiltakozik a személyes adatkezelés ellen, addig az ideig, amíg megállapításra nem kerül, hogy az Érintett adatkezelőnek jogos indokai elsőbbséget élveznek-e az Érintett indokaival szemben.

Ha az adatkezelés korlátozás alá esik, az ilyen személyes adatokat tárolni kell, és csak az Érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

A Társaság megjelöli az általa kezelt személyes adatot, ha az Érintett annak helyességét vagy pontosságát vitatja, de a rendelkezésre álló dokumentumok alapján nem állapítható meg egyértelműen annak helytelensége vagy pontatlansága.

Az adatok törléséről, a helyesbítéséről, a korlátozásáról, a megjelöléséről az Érintettet, továbbá mindazokat értesíteni kell, akiknek korábban azt adatkezelés céljára továbbították.

Az értesítés abban az esetben mellőzhető, ha az – tekintettel az adatkezelés céljára – nem sérti az Érintett jogos érdekét.

A tiltakozáshoz való jog

Az érintett személy a Társaság honlapján közzétett elérhetőségeken keresztül, írásban tiltakozhat az adatkezelés ellen a saját helyzetével kapcsolatos okokból, amennyiben az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, vagy az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges.

Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Így például tiltakozhat az ellen, ha a Társaság hozzájárulása nélkül a személyes adatot tudományos kutatás céljából felhasználná.

Az adatkezeléssel kapcsolatos jogérvényesítési lehetősége

Személyes adatok védelméhez fűződő joga megsértése vagy ennek veszélye esetén az érintett az adatvédelmi tisztviselőhöz fordulhat, aki a panaszt megvizsgálja és annak megalapozottsága esetén a Társaság ügyvezetésénél intézkedést kezdeményez.

Az érintetti kérelem elutasítása esetén a Társaság a kérelem kézhezvételét követő 1 hónapon belül írásban közli az elutasítás indokait, továbbá tájékoztatja az érintettet a bírósági jogorvoslat, valamint a Hatósághoz fordulás lehetőségéről.

Az érintett a személyes adatainak védelméhez fűződő joga sérelme esetén jogorvoslatért fordulhat a Nemzeti Adatvédelmi és Információszabadság Hatósághoz (postacím: 1363 Budapest, Pf. 9, telefon: +36 (1) 391-1400, e-mail: ugyfelszolgalat@naih.hu).

Az érintett továbbá polgári pert kezdeményezhet az Adatkezelő ellen. A per elbírálása a törvényszék hatáskörébe tartozik. A per – az érintett választása szerint – az érintett lakóhelye szerinti törvényszék előtt is megindítható (a törvényszékek felsorolását és elérhetőségét az alábbi linken keresztül tekintheti meg: http://birosag.hu/torvenyszekek).

Adatvédelmi tisztviselő neve, elérhetősége:

dr. Révész Balázs

e-mail: Balazs.Revesz@budapestkozut.hu

Tel: +36 30 256 5986

2.2.3 Adatfeldolgozó

- A Társaság a munkaviszonyból, illetve tevékenységének ellátáshoz származó kötelezettségek teljesítése céljából az adatszolgáltatás céljának megjelölésével az érintettek személyes adatait az adatfeldolgozó számára átadhatja, amelyről az Érintetteket előzetesen tájékoztatni kell.
- A Társaság határozza meg az általa megbízott adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelésre vonatkozó jogszabályi előírások keretei között. Az adatkezelési műveletekre vonatkozó szabályzatok jogszerűségéért és jelen szabályzat előírásainak történő megfelelőségéért a Társaság, illetve az adatkezelő szervezet vezetője a felelős.
- Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Társaság belső szabályozási dokumentumaiban szabályozott módon dolgozhatja fel, ezek felhasználásával saját célra adatfeldolgozást nem végezhet, továbbá köteles a személyes adatokat a belső szabályozási dokumentumokban meghatározott módon tárolni és megőrizni.
- A Társaságnak az adatfeldolgozásra vonatkozó szerződéseit írásba kell foglalnia.
- A szerződésnek tartalmaznia kell minden olyan információt, amely a személyes adatok kezelése szempontjából releváns, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, az adatfeldolgozás célját, a kezelendő adatok biztonságával kapcsolatos elvárásokat, az adatok kezelésének ellenőrzési lehetőségét. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben akár közvetett, akár közvetlen módon érdekelt. A szerződés kidolgozása során biztosítani kell az Adatvédelmi tisztviselő véleményezési jogát.
- Az adatfeldolgozó tevékenységének ellátása során egyes adatfeldolgozási műveletek elvégzésére további adatfeldolgozót a Társaság előzetes írásbeli hozzájárulására alapján vehet igénybe. Az adatkezelésben Érintettek vonatkozásában olyan szerződéses kötelezettségeket kell meghatározni, amely az adatkezelés teljes folyamatában biztosítja a megfelelő védelmi szintet.

2.3 Az adatok továbbítása

Adattovábbítás megkeresés alapján

A Társaságon kívüli szervtől vagy magánszemélytől érkező, adatközlésre irányuló megkeresést az érintett szervezeti egység vezetője válaszolja meg, kiemelkedő fontosságú ügyekben az Adatvédelmi tisztviselő bevonásával.

Az érintett előzetesen is adhat ilyen tartalmú felhatalmazást, amely szólhat valamely időtartamra és a megkereséssel élő szervek meghatározott körére.

Az érintett nyilatkozattételétől függetlenül teljesíteni kell a büntető ügyekben eljáró hatóságoktól – rendőrség, bíróság, ügyészség, vám- és pénzügyőrség –, valamint a nemzetbiztonsági szolgálatoktól érkező megkereséseket.

E szervek megkereséseiről az illetékes adatkezelő – közvetlenül vagy szolgálati felettese útján – köteles tájékoztatni a Társaság Adatvédelmi tisztviselőjét. **Az adatszolgáltatás csak az Adatvédelmi tisztviselő jóváhagyásával teljesíthető.**

Adatszolgáltatás csak írásbeli megkeresésre és írásban teljesíthető.

A megkeresés és a válasz egy példányát az adatkezelés helyén kell megőrizni, a rendőrség és a hatósági adatkérések kivételével, egy példányt pedig az Adatvédelmi tisztviselőnek kell megküldeni.

A megkeresésből, illetve a válaszból egyértelműen megállapíthatónak kell lennie:

- a megkeresést kezdeményező szerv, vagy személy megnevezése, postacíme, telefonszáma
- az adatkérés célja, rendeltetése
- az adatkérés jogszabályi alapja, illetve az érintett hozzájáruló nyilatkozata
- az adatkérés időpontja
- az adatszolgáltatás alapjául szolgáló adatkezelés megnevezése
- az adatszolgáltatást teljesítő szervezeti egység megnevezése
- az érintettek köre
- a kért adatok köre
- az adattovábbítás módja

Az adatközlésekre irányuló kiemelkedő fontosságú kérelmeket és válaszokat az Adatvédelmi tisztviselőnek nyilván kell tartania.

Az Adatvédelmi és Adatbiztonsági Szabályzat hatása a belső szabályozásokra és a Társaság szerződéskötéseire

A Társaság belső szabályozásainak kiadásra előkészítése során vizsgálni kell, hogy azokban adatvédelmi kötelezettségek felmerülnek-e, ezért a szabályozástervezetet véleményezésre az Adatvédelmi tisztviselő részére meg kell küldeni.

Az Adatvédelmi tisztviselő a szabályozástervezet véleményezése részeként megteszi a szabályozás adatvédelmi jogszerűségére vonatkozó észrevételeit, javaslatait.

Jelen szabályozást kell alkalmazni a Társaság által kötött szerződések adatvédelmi rendelkezéseire, a személyes adatok kezeléséről szóló tájékoztatókra, valamint a hozzájáruló nyilatkozatokra is, melyek betartásáért a **szerződést készítő vezető a felelős**.

2.4 Az adatbiztonság

Adatbiztonság

Az adatbiztonsági rendszabályok és intézkedések célja a manuálisan és az elektronikusan kezelt személyes adatok, valamint az adathordozók védelme a sérülés, rongálódás, megsemmisülés és illetéktelen hozzáférés ellen (lásd Infotv. 7. §).

Az adatbiztonság általános szempontjai

A Társaság az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok ésszerűen elvárható legmagasabb szintű biztonságáról (adatbiztonság elve). A Társaság köteles megtenni azokat a technikai és szervezési intézkedéseket továbbá kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi jogszabályok érvényre juttatásához szükségesek.

Az adatkezelő köteles gondoskodni az általa kezelt adatok védelméről.

Az adatokat védeni kell a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

Adatkarbantartást csak az erre felhatalmazott adatkezelő végezhet.

A számítástechnikai rendszerek üzemeltetését ellátó munkavállalók a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják. Rendellenesség észlelése esetén, kötelesek azt azonnal jelezni az Informatikai igazgatónak, valamint az Adatvédelmi tisztviselőnek.

Az adatbiztonság érdekében megfogalmazott előírások betartásáért, betartatásáért az Informatikai igazgatóság által üzemeltetett informatikai rendszerek vonatkozásában az **Informatikai igazgatóság vezetője**, a lokális adatfeldolgozási rendszerek vonatkozásában az adatfeldolgozást végző **szervezeti egység vezetője** a felelős.

Az adatokhoz való hozzáférés szabályozása

Az adatokhoz való hozzáférést jelszavas védelemmel és jogosultsági rendszer működtetésével kell érvényesíteni.

A központi rendszerhez, illetve a szerver központi tárterületeihez való hozzáférés jelszavait és jogosultsági rendszerét az Informatikai igazgatóság állítja be és kezeli az IBSZ előírásai szerint.

Az egyedi alkalmazások lokális gépein a speciális adatfeldolgozó szoftver saját jelszó és jogosultsági rendszerét kell alkalmazni. A jelszavak használatáért, azok rendszeres változtatásáért és dokumentálásáért az adatfeldolgozást végző **gazdasági egység vezetője** felelős.

A központi rendszer és az egyedi rendszerek hozzáférési jogosultságának működtetésére egyaránt érvényesek az IBSZ-ben rögzített előírások.

Az adatok mentése, az adathordozók biztonsága

Az adatok mentésének és az adathordozók biztonságának előírásait az IBSZ rögzíti.

A központi szervereken tárolt adatok rendszeres mentése az IBSZ-ben előírt „Mentési Rend” szerint történik.

A lokális adatfeldolgozási rendszerek adatainak mentéséért, a mentések naplózásáért az adathordozók nyilvántartásának-, biztonságos tárolásának megfelelőségéért az **adatkezelő** felelős.

Az adatvédelmi incidens

Az Adatvédelmi tisztviselő, az Informatikai igazgató és a Jogi és igazgatási főosztály vezetője, szükség szerint az információbiztonsági felelős és az incidensben érintett szakterület vezetője együtt vesznek részt az adatvédelmi incidensek kezelésére vonatkozó eljárásrend kidolgozásában és működtetésében (továbbiakban: Adatvédelmi Bizottság).

Az adatvédelmi incidensek a következő három klasszikus adatbiztonsági kritériumon keresztül kategorizálhatók:

- „Bizalmas jelleg sérülése” – a személyes adatok jogosulatlan vagy véletlen közzététele vagy az ezekhez való hozzáférés
- „Integritás sérülése” – a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítása
- „Rendelkezésre állás sérülése” – a személyes adatok véletlen vagy jogosulatlan megsemmisítése vagy a személyes adatok elvesztése

Az adatvédelmi incidenst indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 (hetvenkettő) órával azután, hogy az adatvédelmi incidens a Társaság valamely munkavállalójának tudomására jutott, be kell jelenteni az illetékes Hatóságnak.

Az incidens adatkezelő általi tudomásszerzésnek minősül például:

- ha harmadik személy jelzi az adatkezelőnek, hogy az ügyféléről véletlenül személyes adatokat kapott meg, és az ennek alátámasztására alkalmas bizonyítékokat juttat el az adatkezelő részére – ekkor nincs kétség afelől, hogy az adatkezelő tudomást szerzett az adatvédelmi incidens bekövetkezéséről,
- ha az adatkezelő észleli, hogy behatolás történt a hálózatába és megállapítja, hogy a hálózaton tároltak személyes adatokat, illetve, hogy azokat érintően következett be az incidens.

Az a munkavállaló, aki a Társaság által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, azaz a biztonság olyan sérülését észleli, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést észlel, az köteles haladéktalanul megtenni a bejelentést, megadva a nevét, telefonszámát és/vagy e-mail címét, dátum és pontos idő megadásával mikor észlelte az incidenst, az incidens tárgyát, valamint azt, hogy az incidens milyen eszközt, alkalmazást, rendszert érint.

A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

Az incidenssel kapcsolatos bejelentéseket az adatvedelmitisztviselo@budapestkozut.hu e-mail címen lehet megtenni.

Az adatvédelmi incidens kezelése

- Az incidens bejelentése alapján az Adatvédelmi Bizottság tagjai a bejelentést követően haladéktalanul felveszik egymással a kapcsolatot e-mailben, személyesen, vagy telefonon annak érdekében, hogy az incidens bekövetkezéséről, körülményeiről – a 72 (hetvenkettő) órán belüli hatósági bejelentési határidőre tekintettel – értékelést, vizsgálatot végezzenek, illetve az incidens operatív kezelésére maguk közül egy tagot kijelöljenek. Az Adatvédelmi Bizottság elkészíti az incidens kivizsgálására vonatkozó jegyzőkönyvet, dönt az incidens minősítéséről, a szükséges intézkedésekről, az egyes intézkedésekért felelős személyekről és határidőkről.
- Az adatvédelmi incidenskezelésre irányadó jegyzőkönyvmintát jelen Szabályzat 2. számú melléklete tartalmazza.

A bejelentés minősítése során különösen az alábbiakat kell figyelembe venni:

- az incidens eseményének elemzését,
- az érintettek kategóriáit (természetes személy vagy jogi személy ügyfél, ügyfélnek nem minősülő harmadik személy, munkavállaló, hozzátartozók, kiskorú személyek stb.),
- az érintettek – legalább hozzávetőleges – számának beazonosítását,
- az incidenssel érintett adatok kategóriáját (személyazonosító adatok, gazdasági adatok, pénzügyi adatok, családi állapotra vonatkozó adatok stb.),
- az incidenssel érintett adatok hozzávetőleges számát,
- az incidenssel érintett további kockázatok meghatározását,
- a kockázat alacsony vagy magas voltának meghatározását,
- a bekövetkezett károk azonosítását,
- az elhárításra tett intézkedések elemzését.

Amennyiben megállapítják, hogy az adatvédelmi incidens a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járhat, az Adatvédelmi Bizottság adott incidensre kijelölt tagja megkezdi a Hatóság részére a szakaszos bejelentést.

Az incidens bejelentést a Hatóság honlapján kell megtenni. Amennyiben a bejelentés teljesítéséhez további adatok, információk, dokumentumok szükségesek, akkor az Adatvédelmi Bizottság bejelentésre kijelölt tagja jogosult a Társaság bármely Érintett szervezeti egységét felhívni a kért adatok, információk átadására.

A bejelentés részletekben is teljesíthető, de törekedni kell arra, hogy a tudomásra jutástól számított 72 (hetvenkettő) órán belül legalább a bejelentés megkezdésére sor kerüljön.

Amennyiben a bejelentés megkezdése nem kezdődik meg 72 (hetvenkettő) órán belül, akkor a bejelentés mellé mellékelni kell a késedelem igazolására szolgáló indokokat is.

A Társaság, mint adatkezelő nyilvántartást vezet a bejelentett incidensekről, feltüntetve benne az adatvédelmi incidensekhez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a Hatóság ellenőrizze az adatvédelmi incidensek nyilvántartására vonatkozó jogszabályi követelményeknek való megfelelést.

A bejelentett incidens alapján a megvalósítandó további intézkedések végrehajtását figyelemmel kell kísérni.

Az adatvédelmi incidens nyilvántartásában rögzíteni kell:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens elhárítására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

2.5 Adatvédelmi hatásvizsgálat

Az adatvédelmi hatásvizsgálat elvégzésének három esetköre lehetséges:

a) Kötelező adatvédelmi hatásvizsgálatot végezni, amennyiben az adatkezelés szerepel a NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott listáján.
b) Kötelező adatvédelmi hatásvizsgálatot végezni, amennyiben az adatkezelés, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.
c) Önkéntes alapon, az adatkezelő döntése alapján.

Az adatvédelmi hatásvizsgálatban az alábbi személyek részvétele kötelező:

a) az adatkezeléssel érintett szervezeti egység vezetője vagy az általa kijelölt munkatárs;
b) az Adatvédelmi tisztviselő.

Az adatvédelmi hatásvizsgálatot a tervezett adatkezelést megelőzően, legkésőbb a személyes adatok kezelésének megkezdésének időpontjáig kell elvégezni.

Annak érdekében, hogy az Adatkezelő eleget tudjon tenni a fentiekben foglalt kötelezettségének, az adott tevékenység tervezése során a lehető leghamarabb biztosítani kell annak lehetőségét, hogy az Adatvédelmi tisztviselő megvizsgálhassa a tervezett adatkezelési műveletet vagy műveleteket.

Amennyiben az adatvédelmi hatásvizsgálat elvégzése indokolt, azt az adatvédelmi tisztviselő javaslatát követő lehető leghamarabb el kell kezdeni. Az adatvédelmi hatásvizsgálat megkezdésének idejéről tájékoztatni kell az Adatvédelmi tisztviselőt.

Az adatkezelő szervezeti egység vezetője vagy az általa kijelölt munkatárs köteles:

a) előkészíteni az adatvédelmi hatásvizsgálatot, különös tekintettel a szükséges adatok, információk és tények összegyűjtésére, rendszerezésére;
b) az adatvédelmi hatásvizsgálatot lefolytatni;
c) szükség esetén igénybe venni a külső szakértő vagy tanácsadó segítségét;
d) biztosítani, hogy az Adatvédelmi tisztviselő ellenőrizhesse az adatvédelmi hatásvizsgálat lefolytatását, illetve annak eredményét.

Az adatkezelő szervezeti egység vezetője vagy az általa kijelölt munkatárs tanácsot, információt és felvilágosítást kérhet az Adatvédelmi tisztviselőtől az adatvédelmi hatásvizsgálat lefolytatásáról, továbbá köteles minden szükséges információt és felvilágosítást megadni az Adatvédelmi tisztviselő részére az adatvédelmi hatásvizsgálat lefolytatásával kapcsolatban.

Az adatvédelmi hatásvizsgálatnak legalább a következő elemekre kell kiterjednie:

a) az adatkezelés módszeres leírása;
b) az adatkezelés szükségességének és az arányosságának értékelése;
c) az érintett jogait és szabadságait érintő kockázatok és azok kezelésére tett intézkedések;
d) az érdekelteket bevonására vonatkozó információk.

Az Adatvédelmi tisztviselő köteles:

a) értékelni az adatvédelmi hatásvizsgálat lefolytatásának szükségességét;
b) dokumentálni az adatvédelmi hatásvizsgálat szükségességének értékelését;
c) kérésre szakmai tanácsot adni az adatvédelmi hatásvizsgálat lefolytatását illetően;
d) nyomon követni és ellenőrizni az adatvédelmi hatásvizsgálat lefolytatását és eredményét;
e) véleményezni az adatvédelmi hatásvizsgálat lefolytatását és eredményét.

Az adatvédelmi hatásvizsgálat lefolytatására irányadó formanyomtatványokat jelen szabályzat 5. számú mellékletei tartalmazzák.

3 A MUNKAVÁLLALÓK SZEMÉLYES ADATAINAK KEZELÉSE

A munkavállalók személyes adatainak kezelése tekintetében a személyes adatgazda a Humán erőforrás főosztály.

A munkavállalók személyes adatainak kezelésére vonatkozó tájékoztatókat a Humánpolitikai Szabályzat tartalmazza.

A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a Cafeteria és egyéb szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.

A Humán erőforrás főosztály a személyi nyilvántartásban a munkavállalók következő adatait (együtt: személyi anyag) kezelheti:

- a munkavállaló természetes személy azonosító adatait, nemét, lakóhelyét, tartózkodási helyét,
- állampolgárságát,
- TAJ számát,
- adóazonosító jelét,
- munkába lépésének kezdő és befejező időpontját,
- munkakörét, iskolai végzettségét, szakképzettségét, nyelvismeretét, az ezt igazoló okiratok másolatát, a tanulmányi szerződést,
- a munkavállaló önéletrajzát,
- munkabérének összegét, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatokat,
- a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozást, illetve ennek jogosultságát,
- a munkavállaló által igénybe vett betegszabadság időtartamát,
- a munkavállaló rendes szabadságával, rendes és rendkívüli munkaidejével, szabadságának kiadásával, egyéb munkaidő-kedvezményével kapcsolatos adatokat,
- a munkavállalóval kötött munkaszerződés egyéb lényeges adatait (pl. a munkavállaló számára biztosított kedvezményeket, a munkavállaló napi/havi munkaidejét, a szerződés fajtáját),
- a munkavállaló munkájának értékelését,
- a munkavállaló fényképét,
- a munkaviszony megszűnésének módját, indokait,
- erkölcsi bizonyítványának feljegyzett számát,
- a munkaköri alkalmassági vizsgálatok összegzését,
- magán nyugdíjpénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezését, azonosító számát és a munkavállaló tagsági számát,

- minden egyéb olyan személyes adatot, amelynek kezelését törvény írja elő, vagy amelyhez az Érintett hozzájárult. Ilyen különösen a családi adókedvezmény igénybevételéhez szükséges adat, a munkavállaló saját gépjárművének adata, a szociális-jóléti juttatások folyósításához (segély, lakáscélú támogatás, albérleti hozzájárulás), megváltozott munkaképességet, egészségkárosodást, vagy fogyatékosságot igazoló szakhatósági véleményt, vagy fogyatékosságot igazoló szakorvosi aláírással ellátott zárójelentés.

A törvény felhatalmazása, jogi kötelezettség teljesítése alapján vagy az Érintett hozzájárulására – az erre feladatkörük meghatározásával kijelölt szervezeti egységei útján – kezelheti továbbá a munkavállalók következő adatait is, így különösen:

- munkavállalót ért balesetek jegyzőkönyveiben rögzített adatokat,
- a Társaságnál biztonsági és vagyonvédelmi célból alkalmazott kamerarendszerek által rögzített adatokat.

Az adott szakterületnél már rendelkezésre álló személyes adatok (többszöri, nem frissítés célú) ismételt kérése tilos. Ebben az esetben az adatok megadásának megtagadása miatt a munkavállalót semmiféle hátrány nem érheti. A Társaság a munkavállaló egyéb személyes adatait kizárólag az Érintett – írásbeli – hozzájárulásával, vagy a Társaság jogszerű érdekeinek érvényesítése céljából kezelheti.

A munkaviszony létesítésére szolgáló eljárás keretében, a munkavállaló közreműködése nélkül, kizárólag a nyilvánosság számára, az Érintett által korlátozás nélkül (pl. internet, sajtó) hozzáférhetővé tett információ használható fel.

Az Érintett kifejezett hozzájárulása, illetve jogszabályi előírás hiányában, a munkaviszony létesítésének meghiúsulása esetén, a felvételi eljárás során rögzített (az eljáráshoz tartozó egyéb jegyezetek) személyes adatokat 30 (harminc) munkanapon belül törölni kell. A törlésről minden esetben jegyzőkönyvet kell készíteni.

A munkavállaló adatait a következő személyek ismerhetik meg:

- az Érintett
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig a Társaság meghatározott szervezeti egységeinek a vezetője, munkavállalója, illetve meghatározott – az Érintett személyi anyagát kezelő – munkavállaló,
- a feladataik ellátásához elengedhetetlenül szükséges esetben, mértékben és ideig az Érintett munkahelyi vezetői (a munkáltatói jogkörgyakorló vezetővel bezárólag) és az általa kijelölt munkatársai,
- konkrét ellenőrzés céljából az ahhoz elengedhetetlenül szükséges esetben, mértékben és ideig az Adatvédelmi tisztviselő, a Vezérigazgató, valamint a vizsgálati jogkörrel felruházott szervezeti egység munkatársai,
- bíróság, ügyészség, nyomozó hatóság, illetve más eljáró hatóság hivatalos megkeresés alapján az igényelt mértékig,
- más személyek – indokolt esetben – az Érintett írásos hozzájárulásával, a hozzájárulás mértékéig.

A munkavállaló adatainak megőrzésével, ill. törlésével kapcsolatosan a Társaság mindenkori Iratkezelési Szabályzat és Irattári terve szerint kell eljárni. A törlés az írásbeli megállapodásban nem szereplő munkavállalói adatokra terjed ki.

Nem kell, illetve nem szabad törölni a munkaviszony megszűnését követően sem a munkavállaló azon adatait, amelyek törvény felhatalmazása alapján a továbbiakban is nyilvántarthatók vagy megőrzendők.

Egészségügyi alkalmassággal kapcsolatos egészségügyi adatok kezelése

A munkavállalók egészségügyi adatainak kezelése tekintetében az személyes adatgazda a Humán erőforrás főosztály, amely szervezeti egység csak az egészségügyi alkalmasság tényét bizonyító adatot kezeli.

Az Érintett egészségügyi alkalmassággal kapcsolatos adatait nem ismeri meg és nem kezeli egyetlen Érintett adatát a célon túlterjeszkedő mértékben. A Humán erőforrás főosztály az egészségügyi alkalmasság eldöntése céljából a megbízott üzemorvostól származó alkalmassági eredmény alapján dönt az adott/leendő dolgozó egészségügyi alkalmasságáról.

Amennyiben a munkaszerződés megkötésének folyamata során derül ki, hogy az Érintett alkalmatlan a munkakör betöltésére és ezért a jogviszony nem jött létre vagy ennek hatására szűnik meg, úgy az adatkezelés határideje és módja is ezzel párhuzamos.

Hozzátartozók adatainak kezelése munkaviszonnyal összefüggésben

A Humán erőforrás főosztály a munkavállaló hozzátartozóinak adatait is kezeli a Társaság által biztosított kedvezmények érvényesítése céljából. Az így beszerzett harmadik személy adatai a szükséges adattartamot meg nem haladóan vehetők fel és kezelhetők. Ilyen kedvezmény lehet a pótszabadság, családi adókedvezmény igénybevétele, adómentes iskolakezdési támogatás vagy akár a baleset esetén értesítendő személy nyilvántartása a gyors kommunikáció elősegítése céljából.

Abban az esetben, ha a munkavállaló harmadik személy adatait adja meg, úgy köteles az adatkezeléshez a harmadik személy hozzájárulását megszerezni, amellyel a Társaság igazolni tudja, hogy a harmadik személy adatainak kezelésére felhatalmazással rendelkezik.

Fénykép-, videó-, illetve hangfelvétel készítés szabályai

Általános szabályok:

Adott személyekről készített fénykép-, videó-, illetve hangfelvétel személyes adatnak minősül, amelynek elkészítéséhez és felhasználásához – törvényi felhatalmazás eseteit kivéve fő szabályként – az Érintett személy hozzájárulása szükséges.

A hozzájárulás ráutaló magatartással is megadható, azonban célszerű ehhez írásbeli hozzájárulást kérni.

Nem szükséges a hozzájárulást beszerezni akkor, amikor a felvétel összhatásában örökít meg nyilvánosság előtt lezajlott eseményeket például tömegfelvétel, illetve nyilvános közéleti szereplés esetén, függetlenül attól, hogy a felvételen az Érintett felismerhető-e.

1. számú melléklet

AZ ADATKEZELÉSSEL KAPCSOLATOS ALAPFOGALMAK ÉRTELMEZÉSE

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül, vagy közvetve – azonosítható természetes személy.

Személyes adat: azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Különleges adat:

- a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
- az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.

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

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.

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

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.

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

Személyes adatok határokon átnyúló adatkezelése:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint Érintetteket.

Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel, vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

Adatok korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerve, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatot kezel.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

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

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.

Anonimizálás: olyan technikai eljárás, amely biztosítja az Érintett és az adat közötti kapcsolat helyreállítási lehetőségének végleges kizárását.

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

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

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

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

Nemzeti Adatvédelmi és Információszabadság Hatóság: NAIH, akinek a jogállását és feladatait az Info tv. 38.§-a határozza meg (továbbiakban: Hatóság).

Kötelező adatkezelés: a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy kormányzati rendelet határozza meg.

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

2. számú melléklet

JEGYZŐKÖNYV (minta) adatvédelmi incidens kezeléséhez

Értekezlet részletei

Az értekezlet neve és célja:	
Dátum és helyszín:	
Jegyzőkönyv száma:	
Jegyzőkönyvvezető:	
Résztvevők neve és munkaköre:	

1. Előzmények:

2. Az esemény besorolása

A leírtak alapján megállapítható, hogy adatvédelmi incidens történt/nem történt, amely ez eset biztonsági incidensnek is minősül egyben/nem minősül. (indok: …)

3. Adatvédelmi incidens jellemzői:

- *Az érintettek jellege:*
- *Az érintettek száma:*
- *Sérülés jelleg:*
- *Adatvédelmi incidens jellege:*
- *Adatvédelmi incidens oka:*
- *Az adatvédelmi incidens körülményei és hatásai:*
- *Az adatvédelmi incidens előtt alkalmazott intézkedések leírása:*
- *Az adatvédelmi incidens következményei:*
- *Az érintett személyes adatok jellege:*

4. Megállapítások és javaslatok:

Tekintettel az adatvédelmi incidens jellegére és súlyossági fokára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira, az Adatvédelmi Bizottság úgy határozott, hogy szükséges/nem szükséges bejelentést tenni a Hatóság felé, az adatvédelmi incidens magas kockázattal jár/nem jár az érintettek jogaira és szabadságaira, azaz a magánszférájukra.

5. Az Adatvédelmi Bizottság javaslatai:

a)

Intézkedés:

Felelős:

Határidő:

Kelt:

……	……	……
név, munkakör	név, munkakör jegyzőkönyvvezető	név, munkakör

3. számú melléklet

AZ ELEKTRONIKUS- ÉS MANUÁLIS IRATKEZELÉS, VALAMINT A LAKOSSÁGI PANASZOK KEZELÉSÉNEK ADATVÉDELMI SZABÁLYAI

Az elektronikus iratkezelésre vonatkozó adatvédelmi szabályok

Az iratkezelésre a jelen Szabályzatban leírt általános adatvédelmi előírásokon túl, a Társaság Iratkezelési Szabályzatában rögzített előírások az irányadók.

Az elektronikus iratokhoz való hozzáférési jogosultságokat a szervezeti egységek vezetőinek kezdeményezésére – az Informatikai igazgató utasítása alapján – a rendszergazda állítja be és tartja nyilván.

Az elektronikus iratkezelésre vonatkozó adatvédelmi előírások teljesülését az adatvédelmi felelős ellenőrzi.

Manuális iratkezelésre vonatkozó adatvédelmi szabályok

A manuális iratkezelés szabályait a Társaság Iratkezelési Szabályzata tartalmazza. Adatvédelmi szempontból kiemelt jelentőségű előírásai, kötelezettségei:

A Társaság kezelésében lévő személyes adatot tartalmazó manuális kezelésű iratokhoz a feldolgozás során csak az írásban azok kezelésére, betekintésre feljogosított munkavállalók férhetnek hozzá.

Az iratokat zárható helyiségben, zárható iratszekrényekben kell elhelyezni, védeni az illetéktelen hozzáféréstől, fizikai sérüléstől.

A passzív kezelésben lévő iratok archiválását évente el kell végezni. Az iratokat zárható, tűz- és vagyonvédelmi technikai eszközökkel ellátott helyiségben kell tárolni.

Mindazon iratot, amelyet a Fővárosi Levéltár történeti értékűnek minősít, őrzésre át kell adni a Levéltár részére. A levéltári átadás legkorábban az irat keletkezésétől számított 15 év eltelte után történhet. A levéltári kezelésbe átadott iratok adatvédelméért, a beszállítást követően, a Fővárosi Levéltár a felelős.

Lakossági bejelentések, panaszok során keletkezett dokumentumok védelme

A lakossági panaszok, bejelentések során beérkező, aktív kezelésben lévő iratok személyes és különleges adatainak védelme során az Iratkezelési Szabályzatban, valamint az e Szabályzatban foglalt előírások az irányadók.

A lakossági panaszok, bejelentések passzív iratanyagait elkülönített, az adatvédelmi és adatbiztonsági előírásoknak megfelelő irattárban kell megőrizni.

4. számú melléklet

ADATKEZELÉSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA – BEJELENTŐLAP

1. Adatkezelő

1.1 Az adatkezelő neve és elérhetősége:	
1.2 Közös adatkezelő neve és elérhetősége:	
1.3 Adatvédelmi tisztviselő neve és elérhetősége:	
1.4 Kapcsolattartó:	

2. Adatkezelés

2.1 Az adatkezelési tevékenység megnevezése:	
2.2 Az adatkezelés célja:	
2.3 Ha több célja van:	

3. Jogalapja

3.1 Jogszabályhely vagy más jogalap:	
3.2 Jogszabály címe:	
3.3 A tényleges adatkezelés helye:	
3.4 Az adatkezelés automatizáltsága:	

4. Adatfeldolgozás

4.1 Az adatfeldolgozó megnevezése:	
4.2 Címe:	
4.3 Telefonszáma:	
4.4 Kapcsolattartó:	

5. Az adatok forrása

5.1 Adatok forrása, adatfelvétel módja:	

6. Érintettek, címzettek kategóriái

6.1 Érintetti kategóriák:	
6.2 Személyes adat kategóriák:	
6.3 Címzettek kategóriái (akikkel közlik):	

7. Adattovábbítás(ok)

7.1 Továbbított adatokra vonatkozó információk:	
7.2 Adatfajta megnevezése:	
7.3 Adattovábbítás országa:	
7.4 Címzett neve:	

8. Az adattovábbítás jogalapja

8.1 Jogszabályhely vagy más jogalap:	
8.2 Jogszabály címe:	
8.3 Az adattovábbítás módja:	
8.4 Időpontja:	

9. Adatkategóriák törlési ideje

9.1 Adatkategória:	
9.2 Törlési idő:	

10. Technikai és szervezési intézkedések általános leírása

10.1 Intézkedés megnevezése:	
10.2 Általános leírása:	

5. sz. melléklet

ADATVÉDELMI HATÁSVIZSGÁLAT SZÜKSÉGESSÉGÉNEK ÉRTÉKELÉSE

Azonosító:

Az adatkezelési módszeres leírására, beleértve az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, a kezelt személyes adatok, illetve az adatkezeléshez használt eszközök ismertetését is.

A. A NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott lista szerinti vizsgálat

Az adatkezelés szerepel a NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott listáján: □ igen □ nem

Amennyiben az adatkezelés szerepel a NAIH GDPR 35. cikk (4) bekezdése alapján kibocsátott listáján, kérjük, jelölje be, hogy melyik feltétel(ek) teljesülése alapján szükséges az adatvédelmi hatásvizsgálatot elvégezni.

Feltétel	Teljesülés
Biometrikus adat kezelése módszeres megfigyelés céljából	
Kiszolgáltatott helyzetben lévő érintettek biometrikus adatának kezelése	
Pontozás	
Harmadik személytől begyűjtött személyes adatok felhasználása az érintettre vonatkozó döntés meghozatalánál	
Profilozás	
Joghatással bíró vagy az érintettet hasonlóképpen jelentős mértékben érintő döntéshozatal	
Módszeres megfigyelés	
Helymeghatározási adatok kezelése módszeres megfigyelés vagy profilalkotás céljából	
Munkatársak munkájának megfigyelése	
Különleges adatok nagy számban való kezelése	
Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos, nagy számban kezelt adatok eredeti céltól eltérő felhasználása	
Gyermekek személyes adatainak kezelése profilozás, automatikus döntéshozatal, vagy marketing, vagy közvetlenül részükre kínált, információs társadalommal összefüggő szolgáltatások ajánlása céljából	
Új technológiai megoldások használata	
Egészségügyi adatok nagy számban történő felhasználása	
Több adatkezelő egy egész ágazat által közösen használt alkalmazást, rendszert, eszközt, illetve platformot tervez létrehozni, amelyben különleges adatokat is kezelnek	
Különböző forrásokból származó adatok összevonása, egymással való megfeleltetése vagy összehasonlítása	

Egyéb megjegyzések:

B. Az adatkezelés kockázatai szerinti vizsgálat

Az adatkezelés esetén teljesül az alábbi feltételek körül legalább kettő: □ igen □ nem

Amennyiben az adatkezelés esetén teljesül az alábbi feltételek körül legalább kettő, kérjük, jelölje be, hogy melyik feltételek teljesülése alapján szükséges az adatvédelmi hatásvizsgálatot elvégezni.

Feltétel	Teljesülés
Értékelés, pontozás vagy profilalkotást	
Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal	
Módszeres megfigyelés	
Különleges adatok vagy fokozottan személyes jellegű adatok kezelése	
Nagy számban kezelt adatok	
Adatkészletek egymással való megfeleltetése vagy összevonása	
Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok kezelése	
Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása	
Az adatkezelés megakadályozza, hogy az érintettek a jogaikat gyakorolják, szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek	

Egyéb megjegyzések:

C. Adatvédelmi hatásvizsgálat a Társaság döntése alapján

Az adatvédelmi hatásvizsgálatot kell végezni a Társaság döntése alapján az adatkezelés vonatkozásában: □ igen □ nem

A Társaság azon döntésének ismertetése, amelynek értelmében az adatkezeléssel kapcsolatban adatvédelmi hatásvizsgálat kell végezni, beleértve annak a B. pont szerinti feltételnek a bemutatását is, amely a döntés alapjául szolgál.

D. Adatvédelmi hatásvizsgálat alóli mentesülés

Nem kell adatvédelmi hatásvizsgálatot, amennyiben az alábbi feltételek valamelyike teljesül az adatkezelés vonatkozásában: □ igen □ nem

Feltétel	Teljesülés
Az adatkezelés valószínűsíthetően nem jár magas kockázattal	
Az adatkezelés hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat	
Az adatkezelést valamely uniós tagállam adatvédelmi felügyeleti hatósága korábban ellenőrizte	
Az adatkezelés a Társaságra vonatkozó jogi kötelezettség teljesítéséhez szükséges, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat	
Az adatkezelés szerepel a NAIH GDPR 35. cikk (5) bekezdése alapján a összeállított jegyzékében	

Dátum:

Készítette:

_____

név
munkakör
szervezeti egység

Közreműködött:

_____

név
munkakör
szervezeti egység

Adatvédelmi tisztviselő:

_____

ADATVÉDELMI HATÁSVIZSGÁLATI JELENTÉS

Azonosító:

A. Az adatkezelési módszeres leírására.

Ismertesse az adatkezelés az adatkezelés céljait, jogalapját, a kezelendő személyes adatokat, a személyes adatok forrását, az érintettek kategóriáit, a személyes adatok tárolásának időtartamát, valamint az adatkezelés egyéb jellemzőit!

Ismertesse az adatkezeléssel kapcsolatos felelősségi viszonyokat, különös tekintettel az adatkezelő(k)re, az adatfeldolgozó(k)ra, illetve a címzettekre!

Ismertesse az adatkezelésre vonatkozó esetleges belső és külső szabványokat!

B. A szükségesség és arányosság értékelése

1. Ismertesse az adatkezelés arányosságát és szükségességét előmozdító intézkedéseket!

Az adatkezelés célja vagy céljai meghatározottak, egyértelműek és jogszerűek?

Mutassa be a jogszerűség követelményének érvényesüléséhez szükséges jogalapot!

Miként érvényesül az adattakarékosság elve?

Miként érvényesül a pontosság elve?

Miként érvényesül a korlátozott tárolhatóság követelménye?

2. Ismertesse az érintettek jogait támogató intézkedéseket!

Az adatkezelésre az érintett hozzájárulása esetén kerül sor? □ igen □ nem

Amennyiben igen, ismertesse a hozzájárulás visszavonásához való jog érvényesülését!

Ismertesse az érintettek részére nyújtott tájékoztatást és annak módját!

Ismertesse a hozzáféréshez való jog érvényesülésének módját!

Ismertesse a helyesbítéshez való jog érvényesülésének módját!

Ismertesse a törléshez (elfeledtetéshez) való jog érvényesülésének módját!

Ismertesse az adatkezelés korlátozásához való jog érvényesülésének módját!

Az adatkezelés esetén teljesülnek a GDPR 20. cikk (1) bekezdésében foglalt feltételek? □ igen □ nem

Amennyiben igen, ismertesse az adathordozhatósághoz való jog érvényesülésének módját!

Az adatkezelés esetén teljesülnek a GDPR 21. cikk (1),(2), vagy (6) bekezdésében foglalt feltételek? □ igen □ nem

Amennyiben igen, ismertesse az adathordozhatósághoz való jog érvényesülésének módját!

Az adatkezelés esetén teljesülnek a GDPR 22. cikk (1) bekezdésében foglalt feltételek? □ igen □ nem

Amennyiben igen, ismertesse az érintett egyedi ügyekben hozott automatizált döntéshozatallal kapcsolatos jogai érvényesülésének módját!

2. Ismertesse garanciális jelentőségű kiegészítő intézkedéseket!

Sor kerül adatfeldolgozó igénybevételére az adatkezelés során? □ igen □ nem

Amennyiben igen, az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés?

Sor kerül Európai Unión kívüli adattovábbításra az adatkezelés során? □ igen □ nem

Amennyiben igen, megfelelő védelemben részesülnek a személyes adatok?

C. Kockázatelemzés és a kockázatok kezeléséhez szükséges intézkedések

1. A kockázatok felmérése és a szükséges intézkedések

Milyen főbb következményekkel járna az érintettekre a személyes adatokhoz való jogosulatlan hozzáférés?

Milyen forrásai lehetnek a személyes adatokhoz való jogosulatlan hozzáférésnek?

Milyen jelenlegi intézkedések védik a személyes adatokat a jogosulatlan hozzáférés ellen?

Milyen jelenlegi intézkedések védik az érintetteket a jogosulatlan hozzáférés következményei ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet a személyes adatokat a jogosulatlan hozzáférés ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az érintettek részére a jogosulatlan hozzáférés következményei ellen?

Egyéb információk:

Milyen főbb következményekkel járna az érintettekre a személyes adatok véletlen vagy jogellenes megváltoztatása?

Milyen forrásai lehetnek a személyes adatok véletlen vagy jogellenes megváltoztatásának?

Milyen jelenlegi intézkedések védik a személyes adatokat a véletlen vagy jogellenes megváltoztatás ellen?

Milyen jelenlegi intézkedések védik az érintetteket a személyes adatok a véletlen vagy jogellenes megváltoztatásának következményei ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet a személyes adatokat véletlen vagy jogellenes megváltoztatása ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az érintettek részére a személyes adatok véletlen vagy jogellenes megváltoztatásának következményei ellen?

Egyéb információk:

Milyen főbb következményekkel járna az érintettekre a személyes adatok elvesztése?

Milyen forrásai lehetnek a személyes adatok elvesztésének?

Milyen jelenlegi intézkedések védik a személyes adatokat az adatvesztés ellen?

Milyen jelenlegi intézkedések védik az érintetteket az adatvesztés következményei ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az adatvesztés ellen?

Milyen további intézkedések biztosíthatnak hatékonyabb védelmet az érintettek részére az adatvesztés következményei ellen?

Egyéb információk:

2. Intézkedése terv

D. Az érdekeltek bevonása

Az adatvédelmi tisztviselő véleménye

Sor került-e az érintettek bevonására? □ igen □ nem

Amennyiben igen, ismertesse az érintettek véleményét, valamint a Társaság intézkedéseit!

Amennyiben nem, ismertesse az érintettek bevonása elmaradásának okait!

Adatvédelmi és Adatbiztonsági Szabályzat

Dátum:

Készítette:

_____

név
munkakör
szervezeti egység

Közreműködött:

_____

név
munkakör
szervezeti egység

Adatvédelmi tisztviselő:

_____

név

Mellékletek:
