Hajdúböszörményi Járóbeteg Rendelőintézet

ADATVÉDELMI INCIDENS KEZELÉSI SZABÁLYZAT

Hajdúböszörmény, 2026. február

A **Hajdúböszörményi Járóbeteg Rendelőintézet**, mint **Adatkezelő** tiszteletben tartja mindazon személyek magánszféráját, akik számára személyes adatot adnak át és elkötelezett ezen adatok

védelmében. Az Európai Unió Általános Adatvédelmi Rendelet (679/2016. számú rendelet, a továbbiakban: GDPR.) alapján az alábbi szabályzatot alkotja:

1. Általános rendelkezések

1.1. A szabályzat célja

Jelen szabályzat elsődleges célja, hogy szabályozza az esetlegesen bekövetkező adatvédelmi incidensek kezelését, elhárítását, károk enyhítését, és megelőzését.

1.2. A szabályzat hatálya

Időbeli hatály: jelen szabályzat 2026. február 15. napjától további rendelkezésig, vagy visszavonásig érvényes.

Személyi hatály: kiterjed a Adatkezelő valamennyi munkatársára és mindazon személyekre, akik jogait vagy jogos érdekét az adatvédelmi incidens érinti.

Tárgyi hatály: kiterjed az Adatkezelőnél bekövetkezett adatvédelmi incidensekre

1.3. Fogalmak

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 vagy a jogosultak számára hozzáférhetetlenné férését eredményezi.

Felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), székhelye: 1055 Budapest, Falk Miksa u. 9-11.

Adatvédelmi incidensnek minősülnek például:

- Személyes adatok dokumentumon, hordozható eszközön, adathordozón vagy informatikai rendszeren (pl.: levelezéssel) történő illegális/nem engedélyezett/nem jogszerű továbbítása.
- Illetéktelen hozzáférések személyes adatokat kezelő informatikai rendszerhez vagy alkalmazáshoz (pl.: a jelenlegi, vagy volt munkavállaló véletlen vagy tudatos közreműködése által, vagy biztonsági rés kihasználásával).
- Személyes adatokat tartalmazó adatbázis egy részének, vagy egészének sérülése, vagy elvesztése.
- Az informatikai rendszer egy részének, vagy egészének használhatatlanná válása vírus vagy egyéb rosszindulatú szoftver által, stb.

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

1.4. Az adatvédelmi incidensek értékelése:

Jelentős adatvédelmi incidens:

- adatvédelmi incidenssel érintett adatok köre: különleges adat vagy személyes adat;

- adatvédelmi incidenssel érintettek száma: személyes adat esetében 100 vagy ennél több érintett, adatvédelmi incidenssel érintett különleges adat esetében legalább 1 érintett;
- azonnali intézkedést igényel;
- partner adatát érinti, függetlenül attól, hogy hány partnerről vagy adatról van szó;
- hatás: jelentős vagy visszafordíthatatlan következmények;
- jelentős reakciót igényel a normális működésen túl;
- büntetőjogi következményei lehetnek;
- az adatvédelmi incidens és/vagy körülménye elektronikus vagy nyomtatott médiában elérhető

Közepes adatvédelmi incidens:

- adatvédelmi incidenssel érintett adatok köre: személyes adat;
- adatvédelmi incidenssel érintettek száma: 100 érintettnél kevesebb érintett;
- hatás: közepes, érintettek kényelmetlenségeket tapasztalhatnak;
- az észlelés napján igényel intézkedést, de azonnali intézkedést nem igényel;
- függetlenül attól, hogy az intézkedés az észlelést követően azonnal megtörténik);
- büntetőjogi következmény nem merülhet fel, de más jogi következmény felmerülhet (pl.: polgári jogi)

Jelentéktelen adatvédelmi incidens:

- adatvédelmi incidenssel érintett adatok köre: olyan adat, amely segítségével nem azonosítható be érintett;
- adatvédelmi incidenssel érintettek száma: nem értelmezhető, mert érintett nem beazonosítható;
- hatás: minimális (pl.: informatikai leállás tapasztalható);
- az adatok visszaállítása egyszerűen kivitelezhető.

1.5. Az adatvédelmi incidens által okozott kár

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között:

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

2. Megelőző és felderítő intézkedések

Adatkezelő az adatvédelmi incidensek megelőzése és felderítése érdekében a következő technikai és szervezési intézkedéseket tette meg és ezen intézkedések megtételét rendszeresen ellenőrzi:

- adatvédelmi szabályozási rendszert hozott létre és tart naprakészen;
- az Adatvédelmi és Adatkezelési Szabályzatban meghatározta az adatvédelem szervezetét;

- adatvédelmi tisztviselőt nevezett ki;
- munkatársakat informálta és folyamatosan informálja, oktatja az adatvédelmi szabályozásról, annak változásáról;
- a munkatársak megismerik és nyilatkozatokban fogadják el az adatvédelmi szabályozási rendszer rendelkezéseit;
- a munkatársak a személyes adatokkal kizárólag az adatvédelmi szabályozási rendszerben meghatározott jogosultságok alapján, célból és módon kerülhetnek kapcsolatban, azokat csak a meghatározott módon kezelhetik;
- az adatkezelő az adatvédelmi incidensek megelőzése és felderítése céljából az IBSZ- ben meghatározott naplózási rendet vezet be és folyamatosan ellenőriz;
- az adatkezelő egyéb, az IBSZ-ben meghatározott informatikai eszközök segítségével akadályozza meg az adatok jogellenes kezelését, vagy azokhoz történő jogellenes hozzáférést.

3. Eljárás adatvédelmi incidens bekövetkezése esetén

3.1. A munkatársak kötelezettségei adatvédelmi incidens észlelésekor

Függetlenül attól, hogy az adatvédelmi incidens csekély jelentőségű-e vagy feltételezett adatvédelmi incidens történt, a munkatárs köteles az észlelést követően azonnal, késedelem nélkül:

- értesíteni az esetről és annak körülményeiről az Intézmény igazgatóját és az adatvédelmi tisztviselőt;
- feljegyezni a körülményeket, így:
- az észlelés napját és időpontját, valamint, ha megállapítható (a feltételezett) adatvédelmi incidens bekövetkezésének napját és időpontját;
- azoknak a személyes adatoknak a körét, amelyeket az adatvédelmi incidens érint;
- a jogsértés okát és terjedelmét, valamint az érintett adatok és a jogsértés közötti összefüggést.

3.2. A Hajdúböszörményi Járóbeteg Rendelőintézet igazgatójának kötelezettségei adatvédelmi incidens bejelentésével kapcsolatban

Az igazgató az értesítést követően azonnal, késedelem nélkül köteles:

- értesíti az adatvédelmi tisztviselőt, ha az ő értesítése valamely okból elmaradt;
- az incidens gyors és pontos kivizsgálása érdekben késedelem nélkül bevonni (értesíteni) minden olyan munkatársat és/vagy külső szakértőt (pl. informatikai szakértő, rendszergazda, érintett adatfeldolgozó), akik az incidens felderítéséhez szakmai tudásukkal hozzá tudnak járulni
- megtenni minden intézkedést a (feltételezett) adatvédelmi incidens (jogsértés) megszüntetése és a kárenyhítés érdekében, és
- a megtett intézkedésekről, továbbá az intézkedések kimeneteléről, hatásairól, beleértve azt az álláspontot és annak alapját is kifejtve, hogy van-e további intézkedésre szükség, valamint az intézkedések megtételének dokumentálásának megtörténtéről, annak elküldésével értesíteni az adatvédelmi tisztviselőt.

3.3. Az adatvédelmi tisztviselő kötelezettségei adatvédelmi incidens bejelentésével kapcsolatban

Az adatvédelmi tisztviselő az értesítést követően, azonnal, késedelem nélkül köteles:

- felülvizsgálni a már megtett intézkedéseket, azokról és hatásaikról további részletes tájékoztatást kérni;
- megtenni minden további intézkedést a (feltételezett) adatvédelmi incidens megszüntetése és kárenyhítés érdekében, szükség esetén, példálózó felsorolással élve Munkatársak jogosultságait átmenetileg megvonni vagy módosítani, jelszavakat módosítani, adathordozókat zárolni, elérhetetlenné tenni, pontokat lezárni;
- elvégezni az adatvédelmi incidens értékelését:
  felmérni az adatvédelmi incidenssel érintett adatok számát;
  felmérni az adatvédelmi incidenssel érintett érintettek körét és számát;
  felmérni az adatvédelmi incidens hatásait az érintettekre és az adatkezelőre nézve;
  az értékelésről írásos összefoglalást készíteni;
- amennyiben az adatvédelmi incidens közepes vagy jelentős hatású, tájékoztatni az érintetteket az adatvédelmi incidens körülményeiről, hatásairól, elhárítására tett intézkedésekről, megelőző intézkedésekről;
- az újabb adatvédelmi incidens bekövetkezésének megelőzése céljából intézkedéseket, valamint ha szükséges, javaslatokat is tenni az adatkezelő mindenkori vezetője felé;
- amennyiben szükséges, egyéb informatikai vonatkozású intézkedéseket tenni az adatvédelmi incidens körülményeire tekintettel, példálózó felsorolással élve adatmentést, adat visszaállítást végezni; amennyiben a jogszabályi feltételek fennállnak, a feljelentés alapjául szolgáló dokumentációt összeállítani és a feljelentést megfogalmazni;
- a fentiekről és minden egyéb körülményről jelentést létrehozni és megküldeni az adatkezelő mindenkori vezetője számára;
- a belső nyilvántartást vezetni az adatvédelmi incidensről.
- az adatvédelmi incidens bejelentése a Hatóság részére legkésőbb 72 órán belül (jelentéstételi kötelezettség)

3.4. Belső nyilvántartás vezetése az adatvédelmi incidensekről

Az adatvédelmi tisztviselő az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza az érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Az adatvédelmi tisztviselő az adatvédelmi incidens nyilvántartást az 1. sz. melléklet mintáját felhasználva vezeti.

3.5. Az adatvédelmi incidens bejelentése

Adatkezelő a személyes adatok vonatkozásában az incidens észlelését követően a leghamarabb, indokolatlan késedelem nélkül, de **legkésőbb 72 órán belül jelenteni kötelesek a NAIH-nak (Hatóságnak).**

A NAIH-nak történő incidens bejelentésének minimum a következő adatokat kell tartalmaznia:

- az adatvédelmi incidens jellege, beleértve - ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát,
- az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,

- az adatvédelmi tisztviselő vagy további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
- az adatvédelmi incidensből eredő, valószínűsíthető következmények,
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

Amennyiben az adatkezelési incidens első bejelentésekor még az incidensre és annak megoldására vonatkozó összes adat nem áll rendelkezésre, úgy az első bejelentéskor a rendelkezésre álló adatokat kell bejelenteni, valamint a többi adatot azok rendelkezésre állásának ütemében, de indokolatlan késedelem nélkül pótlólag kell a Hatóságnak bejelenteni.

3.6. Tájékoztatási kötelezettség adatvédelmi incidens esetén

Érintettek tájékoztatása az adatvédelmi incidensről

Adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintetteket valamennyi olyan adatvédelmi incidensről, ami olyan személyes adatokat érint, amely tekintetében adatkezelőként jár el, és amely valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságaira nézve.

Adatkezelő az adatvédelmi incidensre vonatkozó tájékoztatásban világosan és közérthetően nyújt tájékoztatást az alábbiakról:

- Adatvédelmi incidens jellege;
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
- az adatvédelmi incidensből eredő, valószínűsíthető következmények;
- az általa az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Nem kell azonban az érintetteket tájékoztatni, ha

- Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták;
- az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az Érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg; vagy
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

Amennyiben a tájékoztatás aránytalan erőfeszítést tenne szükségessé, akkor Adatkezelő nyilvánosan közzétett információk útján tájékoztatja az érintetteket, vagy olyan hasonló intézkedést hoz, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Az adatvédelmi tisztviselő feladata, hogy az Adatvédelmi Incidens megtörténtét a jogszabály által elvárt nyilvántartásba felvegye, valamint gondoskodjék az illetékes adatvédelmi hatóság felé történő bejelentéséről.

3.7. Az adatvédelemért felelős vezető és a rendszergazda együttes feladatai

Az adatvédelemért felelős vezető, illetve amennyiben az incidens informatikai eszközzel, erőforrással kapcsolatba hozható, akkor az adatvédelemért felelős és a rendszergazda együttes további feladatai:

- A bejelentett adatvédelmi incidens nyugtázása, az incidenssel kapcsolatos további adatok, információk gyűjtése.
- Az adatvédelmi incidens hatásának vagy potenciális hatásának elemzése, meghatározása a Szeretetszolgálat és intézményei, valamint az érintettek jogai szempontjából.
- Szükség esetén azonnali eszkalálás, válságkezelési terv elindítása.
- A megtámadott információs rendszer, szolgáltatás és/vagy hálózat elkülönítésének és lekapcsolásának lehetővé tétele.
- A kapcsolódó folyamatok/tevékenységek felelőseinek értesítése az incidensről.
- Az incidens hatását, és az incidenskezelés módját, lépéseit meghatározó szakértői team összehívása. Feladatuk az incidenssel kapcsolatos minden információ felderítése, bizonyítékok további gyűjtése, majd a szükséges technikai és szervezési intézkedések meghatározása és foganatosítása.
- Az adatvédelmi incidens kiértékelésének eredményéről tájékoztatni kell a Hatóságot.

3.8.Adatkezelő igazgatójának további feladatai

Az Adatkezelő mindenkori vezetője köteles:

- megismerni az adatvédelmi incidens minden körülményét (a számára tett jelentést)
- informálódni az adatvédelmi incidensről, amennyiben annak minden körülménye számára nem érthető,
- azonnal elrendelni minden olyan intézkedést, amelyet az adatvédelmi tisztviselő – hatáskör hiányában - nem rendelhet el, de az intézkedés kárenyhítést vagy a jövőbeni újabb adatvédelmi incidens megelőzését szolgálja,
- amennyiben a jogszabályi feltételek fennállnak, feljelentést tenni az illetékes rendőrkapitányságon, illetve hatóságnál.

3.9. Az adatfeldolgozónál bekövetkezett adatvédelmi incidens

Amennyiben Adatkezelő valamelyik adatfeldolgozó partnerénél történik adatvédelmi incidens, úgy az adatfeldolgozó az észlelést (bejelentést) követően a lehető leghamarabb, indokolatlan késedelem nélkül, 24 órán belül értesíti az adatkezelőt, továbbá megteszi az adatvédelmi rendelkezéseknek megfelelő és kötelező intézkedéseket (az adatfeldolgozói tevékenységről szóló megállapodás alapján).

4. Az eljárás eredménye, intézkedési javaslat

Az eljárás eredménye lehet:

- annak megállapítása, hogy nem történt adatvédelmet sértő esemény és az eljárás intézkedés nélküli megszüntetése (pl.: hibás észlelés);
- adatvédelmet sértő esemény megtörténtét megállapító és intézkedést elrendelő döntés;
- további eljárás elrendelése, amely a felelősség megállapítása vagy hasonló esetek megelőzése érdekében szükséges.

Belső vagy külső ellenőrzés eredménye alapján szükséges intézkedés:

Belső szakmai ellenőrzés, az adatvédelmi tisztviselő vagy a belső adatvédelmi felelős által megállapított szabálytalanság, informatikai incidens esetén a szabálytalansággal, illetve incidenssel érintett szervezeti egység vezetőjének a vonatkozó belső szabályzat előírása alapján intézkednie kell a megállapítások hatásos kezelésére.

Külső ellenőrzési szerv által megállapított szabálytalanság esetén szükséges intézkedés:

Az eljárási jelentésben foglalt szabálytalanságokra vonatkozó, az ellenőrzéssel érintett szakterület által kidolgozott intézkedési tervet végre kell hajtani.

5. Jogkövetkezmények

A jogkövetkezményekről való döntés kezdeményezése az adatvédelmet sértő esemény megszüntetésére hatáskörrel rendelkező szervezeti egység vezetői, kiemelt jelentőségű ügyben a Adatkezelő igazgatójának feladata.

A jogkövetkezmény jellege szerint a következő lehet:

- jogi jellegű (kártérítési eljárás megindítása, szabálysértési vagy büntetőeljárás kezdeményezése az arra feljogosított hatóságnál);
- munkajogi (figyelmeztetés, felmondással, azonnali hatállyal történő megszüntetése);
- pénzügyi jellegű (pénzbeli juttatás, kifizetés részben vagy egészben történő felfüggesztése, visszakövetelése, behajtása)
- szakmai jellegű (belső szabályozás módosítása, szigorításának kezdeményezése, betartásának fokozott ellenőrzése stb.)

Amennyiben büntető- vagy szabálysértési eljárás kezdeményezésének szükségessége merül fel, a szükséges intézkedések meghozatala az arra illetékes szervek értesítését is jelenti annak érdekében, hogy megalapozottság esetén az illetékes szerv a megfelelő eljárásokat megindítsa. Az eljárások megindításának kezdeményezésére a Szeretetszolgálat igazgatója jogosult.

Ha nyilvánvalóvá vált, hogy az adatvédelmet sértő eseményt bejelentő személy rosszhiszeműen járt el és alaposan feltehető, hogy ezzel bűncselekményt vagy szabálysértést követett el, másnak kárt vagy egyéb jogsérelmet okozott, adatai az eljárás kezdeményezésére, valamint lefolytatására jogosult részére átadhatók.

6. Az adatvédelmi tisztviselő

Az adatvédelmi tisztviselő elérhetőségei:

Név: dr. Olajos József
E-mail: info@drolajosjozsef.hu
Telefonszám: +36 30 8171 741

Az adatvédelmi tisztviselő jogállása:

(GDPR 38. cikk) alapján:

(1) Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

(2) Az adatkezelő és az adatfeldolgozó támogatja az adatvédelmi tisztviselőt a jogszabályban előírt feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

(3) Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. Az adatkezelő vagy az adatfeldolgozó az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az adatkezelő vagy az adatfeldolgozó legfelső vezetésének tartozik felelősséggel.

(4) Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

(5) Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

(6) Az adatvédelmi tisztviselő más feladatokat is elláthat. Az adatkezelő vagy az adatfeldolgozó biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség

Az adatvédelmi tisztviselő feladatai:

(1) Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

- tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó, továbbá az adatkezelést végző alkalmazottak részére az e rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

- ellenőrzi az e rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is;

- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a GDPR szerinti hatásvizsgálat elvégzését;

- együttműködik a felügyeleti hatósággal;

- az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

(2) Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

7. Záró rendelkezések

Jelen szabályzat 2026. február 15. napján lép hatályba, a benne foglaltak a munkavállalók és egyéb közreműködők részére történő ismertetése a Szeretetszolgálat igazgatója, valamint az intézmények vezetőinek a feladata. A szabályzatban foglaltak megismerését a munkavállalók aláírásukkal igazolják (Megismerési nyilatkozat: szabályzat 2. számú melléklete).

Hajdúböszörmény, 2026. február

Dr. Erdős András
intézményvezető