

SZÉKESFEHÉRVÁRI SZAKKÉPZÉSI CENTRUM

MUNKAVÁLLALÓI ADATKEZELÉSI TÁJÉKOZTATÓ

1. A tájékoztató célja és hatálya

A Székesfehérvári Szakképzési Centrum (a továbbiakban: Centrum, Munkáltató vagy Adatkezelő) a jelen tájékoztatóban a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről szóló (EU) 2016/679 rendelet (GDPR) 12–14. cikke, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint a munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.) alapján közérthető, átlátható és részletes tájékoztatást ad a munkaviszonnyal összefüggő személyesadat-kezelésekről.

A tájékoztató a Centrum jelenlegi és volt munkavállalóira, továbbá – az adott adatkezeléshez szükséges mértékben – a munkavállaló hozzátartozóira, kedvezményezettjeire, vészhelyzeti kapcsolattartóira, tanúkra és más érintett személyekre terjed ki. Az állásra jelentkezők adatkezeléséről külön tájékoztató rendelkezik.

A jelen dokumentum a munkaviszony létesítésétől a megszűnését követő iratmegőrzésig terjedő életciklust, továbbá a munkáltatói ellenőrzés egyes formáit is lefedi.

Fontos:

A tájékoztató átvételének vagy megismerésének aláírással történő igazolása nem jelenti az adatkezeléshez adott hozzájárulást. A Centrum a munkaviszonyban hozzájárulásra csak kivételes, valóban önkéntes helyzetben támaszkodik.

2. Az adatkezelő és az adatvédelmi tisztviselő

Adatkezelő neve:	Székesfehérvári Szakképzési Centrum
Székhely és postacím:	8000 Székesfehérvár, Budai út 45. M2 épület
Központi telefon:	+36 22 514 060
Központi e-mail:	titkarsag@szfszc.hu
Honlap:	https://www.szfszc.hu
Képviseli:	Horváth Lajos Zoltán főigazgató és Kulcsár Szilvia kancellár
Adatvédelmi tisztviselő:	Adat-Mappa Bt.
Adatvédelmi kapcsolattartás:	adatvedelem@szfszc.hu

A munkavállaló személyes adatainak kezelésével kapcsolatos kérdéssel, kérelemmel vagy tiltakozással közvetlenül az Adatkezelőhöz vagy az adatvédelmi tisztviselőhöz fordulhat. Az adatvédelmi tisztviselő feladatával összefüggésben titoktartási kötelezettség alatt áll.

3. Alapelvek és jogalapok

A Centrum a személyes adatokat jogszerűen, tisztességesen és átláthatóan, meghatározott és jogszerű célból, a szükséges adatkörre korlátozva, pontosan, a szükséges ideig, megfelelő biztonság mellett és elszámoltatható módon kezeli. Az adatokat új, az eredeti céllal össze nem egyeztethető célra csak külön jogalap és előzetes tájékoztatás mellett használja fel.

Jogalap	Mikor alkalmazza a Centrum?	Munkavállalói példa
GDPR 6. cikk (1) b)	A munkaszerződés teljesítéséhez vagy a munkavállaló kérésére a szerződéskötést megelőző lépéshez szükséges adatkezelés.	A munkaszerződés lényeges adatainak kezelése.
GDPR 6. cikk (1) c)	A Centrumra vonatkozó uniós vagy magyar jogi kötelezettség teljesítése.	Munkaidő-nyilvántartás, bérszámfejtés, adó- és társadalombiztosítási adatszolgáltatás, munkavédelem.
GDPR 6. cikk (1) e)	A Centrumra ruházott közérdekű vagy közhatalmi feladat végrehajtásához szükséges adatkezelés.	A szakképzési közfeladat ellátásához szükséges szervezési és alkalmazotti nyilvántartás.
GDPR 6. cikk (1) f)	A Centrum vagy harmadik személy valós és aktuális jogos érdeke, dokumentált érdekmérlegeléssel; közfeladat ellátása során erre a jogalapra a Centrum nem támaszkodik.	Vagyon- és információbiztonság, célhoz kötött eszköz-, e-mail-, internet-, GPS- vagy kamerás ellenőrzés.
GDPR 6. cikk (1) a)	Kivételesen, ha a döntés valóban önkéntes, konkrét, tájékozott, egyértelmű és hátrány nélkül visszavonható.	Egyedi portré vagy név önkéntes, nyilvános kommunikációs felhasználása.

Különleges személyes adat – így különösen egészségi adat, szakszervezeti tagságra utaló adat vagy más, a GDPR 9. cikke alá tartozó adat – csak akkor kezelhető, ha a GDPR 6. cikke szerinti jogalap mellett a 9. cikk (2) bekezdésének valamely feltétele is fennáll. A foglalkoztatási, társadalombiztosítási és szociális jogi kötelezettségek körében jellemzően a GDPR 9. cikk (2) bekezdés b) pontja; foglalkozás-egészségügyi ellátásnál a h) pont; jogi igényeknél az f) pont alkalmazható.

A Centrum a GDPR 6. cikk (1) f) pontján alapuló ellenőrzési célú adatkezeléseket csak előzetes érdekmérlegelés, szükségességi és arányossági vizsgálat, írásbeli szabályozás és előzetes munkavállalói tájékoztatás mellett végezheti. A lényegi mérlegelési szempontokról a munkavállaló további tájékoztatást kérhet.

4. Az adatok forrása és az adatszolgáltatás jellege

A személyes adatok elsődleges forrása a munkavállaló és az általa benyújtott okirat. További forrás lehet a munkaszerződés és más munkáltatói okirat, a közvetlen vezető, a munkaidő- és szabadságnylvántartás, a KIRA, SAP, KRÉTA vagy más jogszerűen használt ügyviteli rendszer, a Magyar Államkincstár, a NAV, társadalombiztosítási és egészségbiztosítási szerv, a foglalkozás-egészségügyi szolgáltató alkalmassági véleménye, pályázati vagy hatósági dokumentum, munkabaleset tanúja, informatikai és biztonsági napló, GPS-rendszer, beléptetési nyilvántartás és kamerafelvétel.

A jogszabályon vagy a munkaszerződés teljesítésén alapuló adatok megadása kötelező lehet. A szükséges adat hiányában a Centrum a munkaviszonyt nem tudja létesíteni vagy teljesíteni, a munkabért, ellátást vagy kedvezményt nem tudja megállapítani, illetve jogszabályi kötelezettségét nem tudja teljesíteni. Az önkéntes adatkezelésnél a megtagadás vagy a

hozzájárulás visszavonása nem járhat munkajogi hátránnyal. A munkavállaló csak a célhoz szükséges adatot köteles megadni, és a változást a vonatkozó belső szabály szerint jelzi.

5. A munkaviszonyhoz kapcsolódó adatkezelési műveletek

Az alábbi adatkezelési lapok a csatolt adatkezelési folyamatnyilvántartás munkavállalókat érintő műveleteit foglalják össze. Ha ugyanaz az irat több célhoz is kapcsolódik, az egyes célokhoz tartozó jogalapot és megőrzési időt külön kell értelmezni; a hosszabb megőrzés csak az arra kötelezett iratpéldányra vagy adatkörre alkalmazható.

5.1. Személyügyi nyilvántartás és a munkaviszony kezelése

Cél:	A munkaviszony létesítése, fenntartása, módosítása és megszüntetése; besorolás, előmenetel, munkakör és jogosultságok kezelése; jogszabályi nyilvántartások vezetése.
Adatok és forrás:	Név, születési adatok, anyja neve, lakcím, elérhetőség, adóazonosító jel, TAJ, bankszámlaszám, állampolgárság és tartózkodási jogosultság szükség szerint, végzettség, szakképzettség, munkakör, jogviszony, besorolás, munkáltatói intézkedések és okiratok. Forrás: munkavállaló, igazoló okirat, vezetői döntés, KIRA/SAP/KRÉTA, jogszabály szerinti nyilvántartás.
Jogalap:	GDPR 6. cikk (1) b), c) és e); Mt.; a szakképzésről szóló 2019. évi LXXX. törvény (Szt.) és végrehajtási rendeletei; a vonatkozó nyilvántartási szabályok.
Különleges adat:	Csak foglalkoztatási vagy szociális jogi kötelezettséghez szükséges körben, GDPR 9. cikk (2) b).
Címzettek szolgáltatók:	/ Humánerőforrás, feladatkör szerinti vezetők, pénzügy; Magyar Államkincstár, NAV, Oktatási Hivatal vagy más jogszabályban kijelölt szerv; KIRA, SAP, KRÉTA és iratkezelő rendszer szolgáltatói a szerződés szerinti szerepükben.
Megőrzés:	A jogviszony fennállása alatt, majd az irattári terv és az adott irat jogcíme szerint. A 2024. december 31-éig keletkezett, szolgálati időre vagy nyugdíj-megállapításnál figyelembe veendő keresetre/jövedelemre adatot tartalmazó munkaügyi irat a munkavállalóra irányadó öregségi nyugdíjkorhatár betöltését követő 5 évig őrzendő a Tny. 99/A. § alapján. Más irat csak a rá irányadó rövidebb vagy külön törvényi határidőig tartható meg.

5.2. Bérszámfejtés, bérjegyzék, adó-, járulék- és kifizetői kötelezettségek

Cél:	Munkabér, illetmény, pótlék, egyéb járandóság és levonás megállapítása, kifizetése és közlése; adó-, járulék-, társadalombiztosítási és számviteli kötelezettségek teljesítése.
Adatok és forrás:	Azonosító adatok, adóazonosító jel, TAJ, bankszámlaszám, munkabér és juttatások, munkaidő- és távolléti adatok, levonások, végrehajtások, adó- és családi kedvezményhez szükséges adatok, eltartott vagy kedvezményezett szükséges adatai. Forrás: munkavállaló, munkáltatói nyilvántartások, KIRA/SAP, hatósági vagy végrehajtói irat.

Jogalap:	GDPR 6. cikk (1) c) és e); Mt. 155. §; az adózás rendjéről szóló 2017. évi CL. törvény; a személyi jövedelemadóról szóló 1995. évi CXVII. törvény; a 2019. évi CXXII. törvény (Tbj.); a számvitelről szóló 2000. évi C. törvény.
Különleges adat:	GDPR 9. cikk (2) b), ha kedvezményhez, ellátáshoz vagy levonáshoz egészségi vagy szakszervezeti tagságra utaló adat feltétlenül szükséges.
Címzettek szolgáltatók:	/ HR, bérszámfejtés, pénzügy; Magyar Államkincstár, NAV, társadalombiztosítási szervek, végrehajtó vagy más hatóság; KIRA, SAP, MÁK-rendszerek és banki szolgáltató.
Megőrzés:	A számviteli bizonylatok legalább 8 évig; a munkajogi igényhez szükséges, más kötelező megőrzés alá nem tartozó iratok főszabály szerint 3 évig; a Tny. 99/A. § hatálya alá tartozó, 2024. december 31-éig keletkezett iratok az ott meghatározott hosszabb ideig.

5.3. Munkaidő, jelenlét és szabadság nyilvántartása

Cél:	A rendes és rendkívüli munkaidő, készenlét, szabadság és egyéb távollét jogszerű nyilvántartása, a munkaszervezés és bérszámfejtés alátámasztása.
Adatok és forrás:	Név, munkakör, munkavégzés kezdő és befejező időpontja, munkaidő-beosztás, jelenlét, aláírás, távollét jogcíme és ideje, szabadságkeret és vezetői jóváhagyás. Forrás: munkavállaló, vezető, jelenléti és munkaidő-nyilvántartás, KIRA/SAP.
Jogalap:	GDPR 6. cikk (1) c) és e); Mt. 122–134. §, különösen 134. §.
Címzettek szolgáltatók:	/ HR, közvetlen vezető, pénzügy; MÁK/NAV vagy ellenőrző hatóság jogszabály alapján; KIRA/SAP vagy belső munkaidő-nyilvántartás szolgáltatója.
Megőrzés:	Főszabály szerint az Mt. szerinti munkajogi igény elévüléséig, 3 évig; bér- vagy számviteli bizonylattá váló iratrésznel 8 évig; a Tny. 99/A. § alá tartozó régi iratoknál az ott meghatározott ideig.

5.4. Betegszabadság, táppénz, CSED, GYED és családi távollétek

Cél:	Keresőképtelenség, betegszabadság, táppénz, gyermekgondozási és más törvényi távollét, valamint pénzbeli ellátás megállapítása, nyilvántartása és kifizetése.
Adatok és forrás:	Munkavállaló azonosítói és TAJ-száma, távollét jogcíme és időtartama, orvosi igazolás adminisztratív adatai, ellátási adatok; gyermek vagy hozzátartozó neve, születési adatai és TAJ-száma kizárólag a jogosultsághoz szükséges körben. Forrás: munkavállaló, igazolás, egészségbiztosítási/MÁK-dokumentum, KIRA/SAP.
Jogalap:	GDPR 6. cikk (1) c) és e); Mt.; a kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény; Tbj.; családtámogatási és adózási szabályok.
Különleges adat:	GDPR 9. cikk (2) b), szükség szerint h). A Centrum diagnózist csak akkor kezelhet, ha azt jogszabály kifejezetten megköveteli; általános esetben a keresőképtelenség ténye és időtartama elegendő.

Címzettek szolgáltatók:	/	HR, bérszámfejtés, Magyar Államkincstár, egészségbiztosítási szerv, NAV; KIRA/SAP.
Megőrzés:		Ellátási, adó- és bérszámfejtési iratként főszabály szerint 8 évig, illetve az adott ellátási jogszabály vagy irattári terv szerinti ideig; a Tny. 99/A. § hatálya alá tartozó régi iratnál az ott meghatározott hosszabb ideig.

5.5. Foglalkozás-egészségügyi alkalmasság

Cél:	A munkaköri alkalmasság megállapítása és a biztonságos foglalkoztatás feltételeinek biztosítása.
Adatok és forrás:	A Centrum a beutaláshoz szükséges munkaköri és expozíciós adatokat, továbbá az alkalmas, korlátozással alkalmas, ideiglenesen nem alkalmas vagy nem alkalmas minősítést és a munkáltatóval jogszerűen közölhető korlátozásokat kezeli. A részletes egészségügyi dokumentációt a foglalkozás-egészségügyi szolgáltató kezeli.
Jogalap:	GDPR 6. cikk (1) c) és e); Mvt.; 33/1998. (VI. 24.) NM rendelet és a munkakörre alkalmazandó ágazati szabályok.
Különleges adat:	GDPR 9. cikk (2) b) és h). A munkáltató főszabály szerint nem ismerheti meg a diagnózist vagy az alkalmatlanság egészségügyi okát.
Címzettek szolgáltatók:	/ Foglalkozás-egészségügyi szolgáltató – az orvosi dokumentáció tekintetében jellemzően önálló adatkezelő –, HR és a szükséges munkáltatói jogkör gyakorlója kizárólag az alkalmassági eredmény szükséges körében.
Megőrzés:	A Centrum által őrzött alkalmassági vélemény a munkaviszony alatt, majd főszabály szerint a munkajogi igény elévüléséig, 3 évig; a szolgáltató egészségügyi dokumentációja a rá irányadó egészségügyi megőrzési szabályok szerint.

5.6. Munkabalesetek, munkavédelem és tűzvédelem

Cél:	Munkabaleset kivizsgálása, nyilvántartása, bejelentése, baleseti ellátás; munkavédelmi és tűzvédelmi oktatás megtartásának, részvételének és eredményének igazolása.
Adatok és forrás:	Név, azonosítók, TAJ, munkakör, baleset időpontja, helye, körülményei, sérülés és ellátás szükséges adatai, tanúnyilatkozat; oktatásnál név, munkahelyi e-mail, aláírás, időpont és teszteredmény. Forrás: munkavállaló, tanú, munkavédelmi felelős, orvosi és hatósági irat, Microsoft 365/Forms vagy papírajegyzőkönyv.
Jogalap:	GDPR 6. cikk (1) c); Mvt., különösen a munkabaleseti nyilvántartásra vonatkozó szabályok; az 1996. évi XXXI. törvény a tűz elleni védekezésről; Ebtv.; Mt.
Különleges adat:	Munkabalesetnél és ellátásnál GDPR 9. cikk (2) b) és h).

Címzettek szolgáltatók:	/ Munkavédelmi/tűzvédelmi felelős vagy megbízott, HR, vezető; munkavédelmi és tűzvédelmi hatóság, MÁK/egészségbiztosítás, NAV, szükség esetén rendőrség; Microsoft 365 és a megbízott szolgáltató.
Megőrzés:	A munkabaleseti nyilvántartás adatai 5 évig az Mvt. 64. § (4) bekezdése szerint; oktatási iratok az irattári tervben rögzített, legalább az ellenőrizhetőséghez szükséges ideig; bér- vagy ellátási bizonylatnál 8 évig.

5.7. Pályázatok, projektek és kiküldetések

Cél:	Támogatási forrás igénylése, projekt megvalósítása és elszámolása; kiküldetés engedélyezése, útiköltség, napidíj és más költség elszámolása.
Adatok és forrás:	Név, munkakör, jogviszony, azonosítók, részvételi és teljesítési adatok, aláírás, úticél, időpont, útvonal, gépjármű/rendszám, költség- és kifizetési adatok. Forrás: munkavállaló, projektirát, kiküldetési rendelvénnyel, KIRA/KRÉTA/SAP.
Jogalap:	GDPR 6. cikk (1) c) és e), szükség szerint b); támogatási szerződés és pályázati felhívás; Mt.; Szja tv.; számviteli és adózási szabályok.
Címzettek szolgáltatók:	/ Projekt- és pénzügyi munkatársak, vezetők; támogató, irányító hatóság, közreműködő és auditáló szerv; MÁK/NAV; SAP, KIRA, KRÉTA, banki és projektadminisztrációs szolgáltató.
Megőrzés:	Projektirát a pályázati/támogatási előírás szerinti ideig, jellemzően a projekt lezárását követő legalább 5 évig; kiküldetési és számviteli bizonylat 8 évig; jogvita esetén a szükséges irat az ügy jogerős lezárásáig és az igényérvényesítés végéig.

5.8. Eszköznyilvántartás, mobiltelefon, SIM-kártya és külső adathordozó

Cél:	Munkáltatói eszközök kiadása, visszavétele, leltározása, biztonságos használata, költségelszámolása és védelme.
Adatok és forrás:	Név, szervezeti egység, eszköz- és SIM-azonosító, leltári/gyári szám, telefonszám, átadás és visszavétel dátuma, aláírás; indokolt esetben forgalmi vagy híváslista-adat a tartalom megismerése nélkül és a szükséges körre szűkítve. Forrás: átadási jegyzőkönyv, leltár, távközlési számla, rendszer- és eszköznyilvántartás.
Jogalap:	GDPR 6. cikk (1) c), e) és – eszköz-, költség- vagy információbiztonsági célhoz – f), dokumentált érdekmérlegeléssel; Mt. 11/A. §; számviteli és belső információbiztonsági szabályok.
Címzettek szolgáltatók:	/ IT/rendszergazda, leltárfelelős, pénzügy, szükséges vezető; távközlési szolgáltató, szerviz, leltár- és pénzügyi rendszer szolgáltatója.
Megőrzés:	Az eszköz használatának és elszámolásának lezárásáig, majd az igényérvényesítéshez szükséges 3 évig; számviteli bizonylat 8 évig. Visszavételkor vagy selejtezéskor az adattárolót dokumentáltan törölni vagy megsemmisíteni kell.

Garanciák:	Személyre szóló átadás, készülékszár és lehetőség szerint titkosítás; külső adathordozó csak engedélyezetten; javítás/selejtezés előtt adattörlés; ellenőrzéskor fokozatosság és magánadatok védelme.
-------------------	---

5.9. E-mail-rendszer és hivatalos levelezés

Cél:	Hivatalos kommunikáció, munkafolyamatok és intézményi iratok kezelése, üzletmenet-folytonosság, információbiztonság és az e-mail-használati szabályok betartásának célhoz kötött ellenőrzése.
Adatok és forrás:	Név, munkahelyi e-mail-cím, feladó, címzett, tárgy, időpont, csatolmány, naplóadat; a levéltartalom csak akkor, ha a fokozatos ellenőrzés kevésbé beavatkozó lépései nem elegendők és a konkrét munkáltatói célhoz szükséges. Forrás: Microsoft 365/e-mail-rendszer, munkavállaló, levelezőpartner.
Jogalap:	A hivatalos kommunikáció és közfeladati működés körében GDPR 6. cikk (1) e), jogi kötelezettségnél c); ellenőrzésnél GDPR 6. cikk (1) f) dokumentált érdekmérlegeléssel és Mt. 11/A. § alapján. Hozzájárulás nem jogalap.
Címzettek szolgáltatók:	/ A munkakör szerint jogosult munkatárs és vezető; ellenőrzéskor kizárólag írásban kijelölt személy, szükség esetén IT és adatvédelmi tisztviselő; Microsoft 365/e-mail-szolgáltató és rendszergazda.
Megőrzés:	A hivatalos ügyirat az irattári terv szerinti ideig; rendszer- és biztonsági naplók legfeljebb 90 napig, kivéve dokumentált incidenst; ellenőrzési jegyzőkönyv főszabály szerint 3 évig. A munkaviszony megszűnésekor a fiók hozzáférését haladéktalanul meg kell szüntetni, a hivatalos iratokat szabályozottan át kell adni, a magánjellegű tartalmat pedig a lehető legkisebb megismerés mellett rendezni kell.
Garanciák:	Előzetes írásbeli tájékoztatás; konkrét cél, időszak és keresési feltétel; fokozatosság; a munkavállaló jelenlétének vagy képviselőjének biztosítása, ha lehetséges; magánjellegű levél tárgyának és címzettjének észlelésekor tartalmi megismerés mellőzése; minden hozzáférés dokumentálása.

5.10. Munkahelyi internethasználat és hálózati naplók

Cél:	Munkaköri internet-hozzáférés, hálózat- és információbiztonság, kártékony vagy tiltott használat észlelése, a használati szabályok betartásának ellenőrzése.
Adatok és forrás:	Felhasználói azonosító, IP-cím, eszközazonosító, kapcsolódás ideje, forgalmi mennyiség, látogatott domain vagy – csak különösen indokolt esetben – URL. A Centrum főszabály szerint nem figyeli a kommunikáció tartalmát és nem készít általános érdeklődési profilt.
Jogalap:	GDPR 6. cikk (1) e) a közfeladati információbiztonsághoz, illetve f) a dokumentált munkáltatói jogos érdekhez; Mt. 11/A. §; belső IT-biztonsági szabályzat.
Címzettek szolgáltatók:	/ IT/rendszergazda, konkrét ügyben írásban kijelölt vezető és szükség esetén adatvédelmi tisztviselő; internetszolgáltató, tűzfal/proxy és biztonsági szolgáltató.

Megőrzés:	Részletes hálózati napló legfeljebb 90 napig; incidens vagy jogvita esetén a releváns rész elkülönítve az ügy lezárásáig; hosszabb statisztika csak anonimizált formában.
Garanciák:	Elsőként aggregált vagy kategóriaalapú ellenőrzés; egyéni azonosítás csak konkrét és dokumentált okból; célhoz és időszakhoz szűkített lekérdezés; indokolatlan tartalommegfigyelés tilalma; hozzáférési napló.

5.11. Számítógép, laptop és tablet ellenőrzése

Cél:	Munkáltatói eszköz és intézményi adat védelme, információbiztonsági esemény kivizsgálása, munkaköri irat visszakeresése, az eszközhasználati szabály betartásának ellenőrzése.
Adatok és forrás:	Felhasználói azonosító, fájl- és naplóadat, telepített szoftver, konfiguráció, munkavégzési dokumentum. Magánjellegű fájl tartalma csak kivételesen, elkerülhetetlen és jogszerű helyzetben ismerhető meg.
Jogalap:	GDPR 6. cikk (1) e) és f) dokumentált érdekmérlegeléssel; Mt. 11/A. §; információbiztonsági és eszközhasználati szabályzat.
Címzettek szolgáltatók:	/ Kijelölt vezető, IT/rendszergazda, szükség esetén adatvédelmi tisztviselő; szerződött szerviz adatvédelmi feltételek mellett.
Megőrzés:	Rendszer- és biztonsági naplók legfeljebb 90 napig, az ellenőrzési jegyzőkönyv 3 évig; incidens vagy jogvita bizonyítéka az ügy lezárásáig. Visszavételkor/selejtezéskor dokumentált adattörlés.
Garanciák:	Előzetes írásbeli tájékoztatás; ellenőrzési terv és jegyzőkönyv; fokozatosság; a munkavállaló jelenléte vagy képviselte, ha lehetséges; munkaköri mappa/keresés elsőbbsége a teljes eszköz átvizsgálásával szemben; magánadatok lehető legkisebb megismerése.

5.12. Informatikai jogosultságok és hozzáférési naplók

Cél:	Felhasználói fiókok és jogosultságok kiadása, módosítása, visszavonása; információbiztonsági megfelelés, elszámoltathatóság és incidenskivizsgálás.
Adatok és forrás:	Név, felhasználói azonosító, szerepkör, jogosultság, hozzáférés kezdete és vége, hitelesítési és műveleti napló. Jelszó nem olvasható formában kezelendő.
Jogalap:	GDPR 6. cikk (1) c) a GDPR 32. cikke szerinti biztonsági kötelezettséghez; 6. cikk (1) e) a közfeladati információbiztonsághoz; szükség szerint f), érdekmérlegeléssel.
Címzettek szolgáltatók:	/ IT/rendszergazda, kijelölt vezetők és adatvédelmi tisztviselő a szükséges körben; IT-, felhő- és rendszerüzemeltető szolgáltatók.
Megőrzés:	Jogosultsági adat a jogosultság fennállásáig és visszavonását követően 3 évig; hozzáférési napló legfeljebb 12 hónapig, kivéve elkülönített incidens- vagy jogvitai bizonyíték.

Garanciák:	Személyre szóló fiók, legkisebb jogosultság elve, erős hitelesítés és ahol elérhető többtényezős azonosítás, rendszeres és személyi változásokor azonnali jogosultság-felülvizsgálat, naplóvédelem.
-------------------	---

5.13. Céges gépjárművek GPS-adatai

Cél:	Gépjármű- és vagyonvédelem, munkaszervezés, logisztika, út- és költségelszámolás, konkrét rendellenesség kivizsgálása.
Adatok és forrás:	Gépjármű rendszáma, használó neve, hely, útvonal, időpont, távolság és menetadat. Forrás: GPS-rendszer és gépjárműhasználati nyilvántartás.
Jogalap:	GDPR 6. cikk (1) f), dokumentált érdekmérlegeléssel; közfeladati flottaüzemeltetésnél 6. cikk (1) e) megfelelő indokolással; Mt. 11/A. §; gépjárműhasználati szabályzat.
Címzettek szolgáltatók:	/ Kijelölt vezető, pénzügy, flottakezelő/bérbeadó és GPS-szolgáltató; hatóság jogszabály alapján.
Megőrzés:	Részletes GPS-adat legfeljebb 90 napig; menetlevél, kiküldetési és számviteli bizonylat 8 évig; konkrét ügy releváns adata az ügy lezárásáig.
Garanciák:	Munkaidőn kívüli és engedélyezett magánhasználat alatti követés tilalma vagy kikapcsolhatósága; hozzáférés csak kijelölt személynek; lekérdezés célhoz és időszakhoz kötése, naplózás; folyamatos teljesítményértékelésre nem használható.

5.14. Munkahelyi be- és kiléptetés, portanyilvántartás

Cél:	Épületbiztonság, vagyonvédelem, belépések és vendégek kezelése, rendkívüli esemény kivizsgálása.
Adatok és forrás:	Név, szervezeti egység vagy látogatott személy, belépés és kilépés ideje, szükség esetén gépjármű rendszáma. Forrás: munkavállaló, portaszolgálat, beléptetési nyilvántartás.
Jogalap:	GDPR 6. cikk (1) f), dokumentált biztonsági és vagyonvédelmi jogos érdekekkel; megfelelően indokolt közfeladati intézménybiztonságnál e); Mt. 11/A. §.
Címzettek szolgáltatók:	/ Portaszolgálat, kijelölt vezető és biztonsági felelős; hatóság/rendőrség jogszerű megkeresésre; szerződött portaszolgálat vagy vagyonvédelmi szolgáltató, ha van.
Megőrzés:	Legfeljebb 6 hónap, amennyiben ezt a beléptetési szabályzatban dokumentált szükségesség alátámasztja; konkrét incidens vagy jogvita adata elkülönítve az ügy lezárásáig.

5.15. Fénykép, videó, évkönyv és rendezvényi kommunikáció

Cél:	Rendezvény megszervezése és dokumentálása; intézményi kommunikáció; évkönyv; egyedi képmás, hang vagy név honlapon, sajtóban vagy közösségi médiában történő közzététele.
Adatok és forrás:	Név, munkakör, elérhetőség, részvételi adat, képmás, hang, videó és szereplés. Forrás: munkavállaló, rendezvényregisztráció, fotós/videós.

Jogalap:	Rendezvényszervezésnél GDPR 6. cikk (1) e), b) vagy c) az eseménytől függően. Azonosítható munkavállalói portré, névvel összekapcsolt vagy marketingcélú közzététel főszabály szerint GDPR 6. cikk (1) a) pont szerinti önkéntes hozzájárulással; tömegfelvétel vagy nyilvános közéleti szereplés esetén a Ptk. 2:48. § és a körülmények szerinti más jogalap alkalmazható.
Címzettek szolgáltatók:	/ Kommunikációs munkatársak, rendezvényszervező, fotós/videós, nyomda, honlap- és közösségimédia-szolgáltató; közzététel esetén a nyilvánosság.
Megőrzés:	Szervezési adat a rendezvény lezárásáig, illetve számviteli iratként 8 évig; közzétett anyag a dokumentált cél fennállásáig vagy a hozzájárulás visszavonásáig. A már kiadott nyomtatott évkönyv visszahívása nem mindig lehetséges, de a jövőbeni felhasználást meg kell szüntetni.
Garanciák:	A hozzájárulás megtagadása vagy visszavonása nem járhat munkajogi hátránnyal; a külön felhasználási felületeket és célokat előre meg kell nevezni; a tömegfelvételtől előzetesen tájékoztatni kell; különleges vagy kiszolgáltatott helyzetet ábrázoló felvétel nem tehető közzé megfelelő jogalap nélkül.

5.16. Vagyonnyilatkozatok

Cél:	A jogszabályban meghatározott vagyonnyilatkozat-tételi kötelezettség teljesítése és ellenőrzése.
Adatok és forrás:	A nyilatkozatban szereplő vagyoni, jövedelmi és érdekeltségi adatok, átvételi és borítékazonosító; ha jogszabály előírja, hozzátartozói adatok. Forrás: kötelezett munkavállaló és a jogszabály szerinti nyilatkozat.
Jogalap:	GDPR 6. cikk (1) c) és e); az egyes vagyonnyilatkozat-tételi kötelezettségekről szóló 2007. évi CLII. törvény és az adott munkakörre irányadó szabály.
Címzettek:	Kizárólag a jogszabályban ellenőrzésre jogosult személy vagy szerv, a szükséges vezetői körben.
Megőrzés:	A vonatkozó törvény szerinti időtartam; a kötelezettség megszűnésekor visszaadás vagy megsemmisítés a jogszabály szerint.
Garanciák:	Zárt boríték, külön nyilvántartás, pánccs szekrény vagy egyenértékű fizikai védelem, különösen korlátozott hozzáférés; a boríték felnyitása csak törvényi feltételekkel.

5.17. Jogi igények, hatósági eljárások és belső vizsgálatok

Cél:	Munkajogi, kártérítési, fegyelmi, adatvédelmi vagy más jogvita és vizsgálat kezelése, tényállás tisztázása, jogi igény előterjesztése, érvényesítése vagy védelme.
Adatok és forrás:	Az ügyhöz szükséges azonosító, elérhetőségi, munkaviszonyi, teljesítési, pénzügyi, kommunikációs, tanú-, kép-, napló- és bizonyítási adatok. Forrás: érintett, belső irat, tanú, rendszer, hatóság, bíróság, jogi képviselő.

Jogalap:	GDPR 6. cikk (1) c), e) vagy f) az ügy természetétől függően; Mt., Ptk. és eljárási jogszabályok.
Különleges adat:	GDPR 9. cikk (2) f), ha jogi igényhez különleges adat szükséges.
Címzettek szolgáltatók:	/ Kijelölt vezető, HR, adatvédelmi tisztviselő, jogi képviselő, biztosító, bíróság, hatóság, ellenérdekű fél a jogszabály szerinti körben.
Megőrzés:	Az ügy lezárását követően az alkalmazandó elévülési és irattári határidőig; folyamatban lévő ügyben a jogerős befejezésig és a végrehajthatóság/igényérvényesítés végéig, rendszeres szükségességi felülvizsgálattal.

5.18. Adatvédelmi incidensek és érintetti kérelmek

Cél:	Adatvédelmi incidens bejelentése, kivizsgálása és dokumentálása; hozzáférési, helyesbítési, törlési, korlátozási, tiltakozási és más érintetti kérelem kezelése.
Adatok és forrás:	Név, elérhetőség, kérelem vagy incidens tartalma, érintett adat és rendszer, időpont, intézkedés, válasz, bejelentő és intézkedő személy adatai. Forrás: munkavállaló, bejelentő, érintett rendszer, IT, vezető, adatvédelmi tisztviselő.
Jogalap:	GDPR 6. cikk (1) c); GDPR 12–22. és 33–34. cikk; Infotv.
Címzettek szolgáltatók:	/ Adatvédelmi tisztviselő, kijelölt vezető, érintett szervezeti egység, IT, jogi képviselő; szükség esetén NAIH, más hatóság és érintettek; e-mail- és iratkezelő szolgáltató.
Megőrzés:	Incidensnyilvántartás a belső szabályzat szerint 5 évig; érintetti kérelem és válasz főszabály szerint a lezárástól számított 5 évig a megfelelés és igényérvényesítés igazolására, jogvita esetén annak lezárásáig.

5.19. Iratkezelés, levéltári és maradandó értékű iratok

Cél:	Közziratok szabályos kezelése, megőrzése, selejtezése és a maradandó értékű iratok közlevéltári átadása.
Adatok és forrás:	Az adott ügyiratban szereplő munkavállalói és más személyes adatok; forrás a Centrum és intézményei irattára, ügyviteli rendszere és papíriratai.
Jogalap:	GDPR 6. cikk (1) c) és e); a közziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény; iratkezelési szabályzat és irattári terv.
Különleges adat:	GDPR 9. cikk (2) j) közérdekű archiválásnál, megfelelő garanciák mellett, illetve az eredeti ügy jogalapja.
Címzettek szolgáltatók:	/ Irattáros, feladatkör szerint jogosult munkatárs, közlevéltár, ellenőrző szerv; iratkezelő rendszer szolgáltatója.
Megőrzés:	Az irattári terv szerinti selejtezési határidőig; maradandó értékű irat esetén közlevéltári átadásig, majd a levéltári szabályok szerint tartósan.

6. Munkáltatói ellenőrzés közös garanciái

A munkavállaló az Mt. 11/A. § alapján kizárólag a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. A technikai eszköz alkalmazásáról a munkavállalót előzetesen írásban tájékoztatni kell. Az ellenőrzés nem lehet titkos, állandó, készletező vagy általános „hátha szükség lesz rá” jellegű, és nem irányulhat a munkavállaló magánéletének feltárására.

- minden ellenőrzéshez előre meghatározott, valós és jogszerű cél, jogalap és írásban kijelölt hozzáférő szükséges;
- elsőként a legkevésbé beavatkozó, összesített vagy technikai adatot kell vizsgálni; tartalomhoz csak indokolt esetben lehet hozzáférni;
- az ellenőrzést konkrét személyre, eszközre, adatkörre és időszakra kell szűkíteni, és jegyzőkönyvben dokumentálni kell;
- a munkavállaló jelenlétét vagy képviseletét lehetőség szerint biztosítani kell; távollétében ellenőrzés csak objektív, dokumentált okból történhet;
- magánjellegű adat és kommunikáció tartalma főszabály szerint nem ismerhető meg; ha a magánjelleg felismerhető, az ellenőrzést e tartalom tekintetében meg kell állítani;
- az ellenőrzési adat nem használható új, előre nem közölt célra; a hozzáférés és a másolatkészítés naplózandó;
- a jogos érdek megszűnésekor vagy a megőrzési idő végén az adatot törölni, illetve az ügryhöz szükséges részt elkülöníteni kell.

7. Elektronikus megfigyelőrendszer – munkavállalók

A Centrum székhelyén 11 kamerából álló, IP-alapú, zártláncú elektronikus megfigyelőrendszer működik. A kamerás adatkezelés munkavállalók tekintetében is kizárólag személy- és vagyonvédelmi, jogosulatlan belépés megelőzési, rendkívüli esemény kivizsgálási és jogi igény-értvényesítési célokat szolgál. Nem szolgál jelenléti, munkaidő-, teljesítmény- vagy általános magatartás-ellenőrzésre; rejtett megfigyelés nem történik.

Rendszer:	11 darab IP-alapú kamera, helyi hálózati videórögzítő
Rögzített adatok:	Képmás, mozgás és cselekvés képi megjelenése, jelenlét helye és időpontja, mozgás iránya, kameraazonosító
Hang:	Hangfelvétel nem készül
Biometria arcfelismerés:	/ Nincs; biometrikus sablon és automatikus személyazonosítás nem készül
Élőkép:	Rendszeres vagy folyamatos élőképfigyelés nincs
Tárolás:	Helyi rögzítőn; kamerafelvételhez hozzáférő külső adatfeldolgozó a rendelkezésre álló adatok szerint nincs
Automatizált döntés / profilalkotás:	Nincs

7.1. Cél és jogalap

A személy- és vagyonvédelmi, valamint eseménykivizsgálási adatkezelés jogalapja a GDPR 6. cikk (1) bekezdés f) pontja: a Centrum, az általa használt vagyon és az épületben tartózkodó személyek védelméhez, továbbá jogi igény előterjesztéséhez, érvényesítéséhez vagy védelméhez fűződő jogos érdek. A Centrum e jogos érdekekre nem közfeladata ellátásának részeként, hanem az attól elkülönülő munkáltatói, személy- és vagyonvédelmi tevékenység körében támaszkodik. Kötelező hatósági vagy bírósági megkeresés teljesítésének jogalapja a GDPR 6. cikk (1) c) pontja és az adott megkeresésre irányadó jogszabály. A belépés nem minősül hozzájárulásnak.

A dokumentált érdekmérlegelés szerint az incidensek utólagos tisztázásához a záruk, beléptetés, világítás és szervezési intézkedések önmagukban nem minden esetben elegendők. Az érintetti beavatkozást a szűk látómező, rövid megőrzés, rendszeres élőképfelügyelés hiánya, névre szóló hozzáférés, dokumentált visszanezés és a hang-/biometrikus adatkezelés tilalma csökkenti. A jogos érdek csak e garanciák folyamatos fennállása mellett élvez elsőbbséget.

7.2. A kamerák helye és látómezeje

Kamera / hely	Megfigyelt terület	Közvetlen cél	Korlátozás
1. Külső bejárat	Külső megközelítési és belépési pont szükséges sávja	Jogosulatlan behatolás, személy- és vagyon elleni esemény	Közterület csak elkerülhetetlen, minimális mértékben
2. Belső bejárat	Belépők és kilépők közvetlen útvonala	Belépési incidens és biztonsági esemény tisztázása	Látómező a bejárat zónára korlátozott
3. Aula – ügyfél- és vendégfogadó tér	A bejáratot követő fogadótér és közlekedési csomópont szükséges része	Belépési, személy- és vagyonvédelmi esemény	Csak a bejárat, várakozási és közlekedési zóna szükséges része
4. Folyosó	Közlekedési útvonal és irodai bejáratok környezete	Incidens helye, ideje és mozgási iránya	Célhoz nem szükséges ajtó- és háttérterület kizárandó
5. Vezetői irodák előtere – folyosó	Vezetői irodák megközelítése és közlekedési csomópont	Iratok, intézményi vagyon és útvonal védelme	Csak az ajtók és átjáró szükséges része
6. Vezetői iroda előtere és hátsó bejárat	Irodaajtó előtere, bejárat és hátsó belépési útvonal	Jogosulatlan belépés és vagyonvédelmi esemény	Belépési pontokra és közvetlen előterükre korlátozott
7. Hátsó „B” bejárat kívülről	Hátsó külső belépési pont és közvetlen megközelítése	Jogosulatlan behatolás, rongálás, károkozás	Közterület csak elkerülhetetlen, minimális mértékben
8. Tárgyalói külső bejárat	Új épületszárny és tárgyaló külső megközelítési pontja	Jogosulatlan belépés és vagyonvédelmi esemény	Csak a belépési zóna; a helyiség belső tere nem
9. Új épületszárny – tárgyalói folyosó	Közlekedési útvonal és tárgyalói megközelítés	Belépési vagy vagyonvédelmi esemény	Közlekedési csomópont szükséges része
10. Parkoló	A Centrum használatában álló parkoló rész és járműközlekedési terület	Rongálás, károkozás, lopás vagy személyi sérülés	A Centrum által használt területre korlátozott
11. Kerékpártároló	Kerékpártároló és közvetlen megközelítése	Lopás és rongálás megelőzése, bizonyítása	Csak a tároló és közvetlen megközelítése

A látómező nem irányulhat olyan területre, ahol a megfigyelés az emberi méltóságot sértene vagy a munkavállaló magánéletejébe aránytalanul beavatkozna. A célhoz nem szükséges

területet fizikai átállítással vagy adatvédelmi maszkkal ki kell zárni. Egy adott kamera felvétele csak az adott hely védelméhez meghatározott célból használható fel.

7.3. Megőrzési idő és felhasználás

Megőrzési idő:

A 2026. június 1. napját megelőzően rögzített felvételek felhasználás hiányában legfeljebb 30 napig kerültek megőrzésre. A 2026. június 1. napjától rögzített felvételek felhasználás hiányában legfeljebb 7 naptári napig (168 óráig) őrződnek; ezt követően a rendszer a legrégebbi felvételt automatikusan és helyreállíthatatlanul felülírja. A módosított időtartamot az elvégzett érdekmérlegelési teszt és az adattakarékosság elve alapján határozták meg.

Rögzített felvétel csak konkrét, dokumentált biztonsági esemény, érintetti hozzáférési vagy megőrzési kérelem, jogi igény, illetve jogszerű hatósági vagy bírósági megkeresés alapján tekinthető vissza. A felvétel kizárólag annál a kameránál és abban a legrövidebb időtartományban vizsgálható, amely a konkrét eseményhez szükséges; a teljes rendszer általános, kereső jellegű visszanezése tilos.

Ha a 7 napos időn belül konkrét ügy miatt szükséges, a releváns képsor elkülöníthető és zárolható. A cél megszűnésekor haladéktalanul törlendő. Jogi vagy hatósági eljárás esetén legfeljebb az eljárás jogerős befejezéséig, illetve a kapcsolódó jogi igény érvényesíthetőségének vagy végrehajthatóságának megszűnéséig tartható meg, rendszeres felülvizsgálat mellett. A megőrzési kérelmet az automatikus felülírás miatt haladéktalanul, lehetőleg 7 napon belül kell benyújtani.

7.4. Hozzáférés és adatbiztonság

A felvételekhez kizárólag a főigazgató által írásban kijelölt, névre szóló jogosultsággal rendelkező személy férhet hozzá a feladatához szükséges mértékben. A belső rendszergazda a Centrum utasítása és titoktartási szabályai szerint jár el; önálló felhasználási joga nincs. Minden megtekintést, mentést, korlátozást, továbbítást és törlést naplózni kell a személy, időpont, cél, jogalap, kamera, időszak és eredmény feltüntetésével. A rögzítő fizikailag védett; az elérés korlátozott; erős, egyedi hitelesítés, rendszeres jogosultság-felülvizsgálat, frissítés és incidenskezelési eljárás alkalmazandó.

8. Címzettek, adatfeldolgozók és adattovábbítás

A személyes adatokhoz a Centrumon belül kizárólag az a munkavállaló vagy vezető férhet hozzá, akinek feladatellátásához az adat szükséges. Tipikus belső címzett a HR, bérszámfejtés, pénzügy, közvetlen vagy munkáltatói jogkört gyakorló vezető, IT/rendszergazda, iratkezelő, munkavédelmi felelős, adatvédelmi tisztviselő és jogi ügyintéző. A jogosultság nem jelent korlátlan hozzáférést; az adatokat feladatonként el kell különíteni.

Külső címzett lehet jogszabály alapján különösen a Magyar Államkincstár, NAV, társadalombiztosítási és egészségbiztosítási szerv, Oktatási Hivatal, fenntartó, támogató vagy auditáló szervezet, levéltár, munkavédelmi és más hatóság, rendőrség, ügyészség, bíróság, végrehajtó, jogi képviselő, biztosító és bank. Adat csak ellenőrzött hatáskör, azonosított címzett, megfelelő jogalap és szükséges adatkör mellett adható át.

Az adatkezelési nyilvántartásban megjelölt rendszerek és szolgáltatói kategóriák különösen: KIRA és Magyar Államkincstár, SAP, KRÉTA, Microsoft 365/Outlook/Forms, iratkezelő, pénzügyi és pályázati rendszer, banki, távközlési, internetszolgáltató, GPS/flottakezelő, IT- és

szervizszolgáltató, munkavédelmi/tűzvédelmi megbízott, fotós, videós, nyomda és honlapüzemeltető. Az egyes szervezetek adatkezelői vagy adatfeldolgozói minőségét nem a rendszer neve, hanem a jogszabály és a tényleges szerződéses feladat határozza meg. Az aktuális adatfeldolgozói jegyzék az adatvédelmi tisztviselőtől kérhető.

A kamerafelvételek helyi rögzítőn tárolódnak, és a rendelkezésre álló információk alapján harmadik országba nem kerülnek. Más munkavállalói adatnál a Centrum közvetlenül nem tervez harmadik országba továbbítást. Ha valamely globális informatikai szolgáltatás működése mégis harmadik országbeli hozzáférést vagy továbbítást eredményez, arra csak a GDPR 44–49. cikke szerinti megfelelési határozat, általános adatvédelmi kikötés vagy más megfelelő garancia, kockázatértékelés és előzetes tájékoztatás mellett kerülhet sor. A konkrét ország és garancia az adatvédelmi tisztviselőtől megismerhető.

9. Adatbiztonság és hozzáférés-szabályozás

- papíriratok zárt szekrényben vagy korlátozott irattárban, különösen érzékeny iratok elkülönítve;
- névre szóló, szerepkörhöz és legkisebb szükséges jogosultsághoz kötött elektronikus hozzáférés;
- erős hitelesítés, ahol elérhető többszörös azonosítás, képernyőzár és jogosultságok rendszeres felülvizsgálata;
- tűzfal, kártevővédelem, biztonsági frissítés, naplózás, mentés és helyreállítási eljárás;
- titoktartás, adatvédelmi és információbiztonsági oktatás, incidensbejelentési és jogosultság-visszavonási folyamat;
- adathordozók titkosítása vagy jelszóvédelme, visszavételkor és selejtezéskor dokumentált adattörlés;
- különleges adatokhoz és béradatokhoz szűkített hozzáférés, továbbításkor megfelelő védelem;
- adatfeldolgozói szerződések, szolgáltatói jogosultságok és biztonsági feltételek rendszeres ellenőrzése.

10. A munkavállaló adatvédelmi jogai

A munkavállaló kérelmét a 2. pontban megjelölt elérhetőségeken nyújthatja be. A Centrum a kérelmező személyazonosságát csak a szükséges és arányos módon ellenőrzi; személyazonosító okmány másolatát rutinszerűen nem kéri. A kérelemre indokolatlan késedelem nélkül, de legkésőbb egy hónapon belül válaszol. A határidő a kérelem összetettsége vagy száma miatt további két hónappal meghosszabbítható, amelyről egy hónapon belül, indokolással tájékoztatást ad. Az eljárás főszabály szerint díjmentes.

Tájékoztatás hozzáférés	és	Visszajelzés kérhető arról, hogy a Centrum kezel-e személyes adatot, továbbá másolat és a GDPR 15. cikke szerinti kiegészítő információ kérhető. A másolat nem sértheti mások jogait és szabadságait.
Helyesbítés kiegészítés	és	A pontatlan adat kijavítása és a hiányos adat kiegészítése kérhető. A felvétel tartalma nem módosítható, de a kapcsolt leíró adat helyesbíthető.
Törlés		A törvényben meghatározott esetben kérhető. Nem teljesíthető például, ha jogi kötelezettség, közérdekű feladat, közérdekű archiválás vagy jogi igény miatt a további kezelés szükséges.
Korlátozás		Kérhető többek között vitatott pontosság, vitatott jogszerűség, saját jogi igényhez szükséges adat vagy tiltakozás elbírálása esetén.

Tiltakozás	A munkavállaló saját helyzetével kapcsolatos okból tiltakozhat a GDPR 6. cikk (1) e) vagy f) pontján alapuló adatkezelés ellen. A Centrum csak kényszerítő erejű jogos ok vagy jogi igény esetén kezelheti tovább az adatot.
Adathordozhatóság	A jog csak az érintett hozzájárulásán vagy szerződésen alapuló, automatizált adatkezelésnél és az érintett által rendelkezésre bocsátott adatokra alkalmazható; a legtöbb munkáltatói adatkezelésre nem terjed ki.
Hozzájárulás visszavonása	Az önkéntes hozzájárulás bármikor, hátrány nélkül visszavonható; ez nem érinti a visszavonás előtti adatkezelés jogszerűségét.
Emberi felülvizsgálat	Ha a jövőben automatizált egyedi döntés történne, az érintett jogosult lenne emberi beavatkozást, álláspontjának kifejtését és a döntés megtámadását kérni. Jelenleg ilyen döntéshozatal nincs.

A munkavállalói jogok gyakorlása miatt hátrányos intézkedés nem alkalmazható. A kérelem teljesítésének esetleges korlátozását a Centrum egyedileg, írásban és jogalappal indokolja. Nyilvánvalóan megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó kérelem esetén a GDPR feltételei szerint észszerű díj számítható fel vagy az intézkedés megtagadható.

11. Panasz, hatósági és bírósági jogorvoslat

A Centrum kéri, hogy a munkavállaló elsőként az adatvédelmi tisztviselőhöz forduljon, hogy a kérdést vagy panaszt közvetlenül kivizsgálhassa. Ez nem feltétele a hatósági vagy bírósági jogorvoslat igénybevételének.

Hatóság:	Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
Székhely:	1055 Budapest, Falk Miksa utca 9–11.
Levelezési cím:	1363 Budapest, Pf. 9.
Telefon:	+36 1 391 1400
E-mail:	ugyfelszolgalat@naih.hu
Honlap:	https://www.naih.hu

A munkavállaló a GDPR 79. cikke és az Infotv. alapján bírósághoz fordulhat. A pert – választása szerint – az Adatkezelő tevékenységi helye vagy a saját lakóhelye, ennek hiányában tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja. A feltételek fennállása esetén kártérítés vagy sérelemdíj is igényelhető.

12. Automatizált döntéshozatal és profilalkotás

A Centrum a jelen tájékoztató szerinti munkavállalói adatok alapján nem hoz kizárólag automatizált adatkezelésen alapuló, a munkavállalóra nézve joghatással járó vagy hasonlóan jelentős döntést, és nem végez profilalkotást. A kamerarendszer nem alkalmaz arcfelismerést, biometrikus elemzést vagy viselkedéértékelést. Ilyen technológia bevezetése előtt külön jogalap-, szükségességi, kockázati és – ha szükséges – adatvédelmi hatásvizsgálatot kell végezni, és a munkavállalókat előzetesen tájékoztatni kell.

13. A tájékoztató elérhetősége és felülvizsgálata

A tájékoztató elektronikusan a Centrum belső vagy honlapi felületén, papíralapon pedig a HR-nél vagy az adatvédelmi kapcsolattartási ponton érhető el. Kérésre hozzáférhető formátumban is rendelkezésre bocsátható. A Centrum a tájékoztatót legalább évente, továbbá új adatkezelés

vagy technológia, cél-, jogalap-, adatkör-, címzett-, megőrzési idő- vagy szolgáltatói változás, incidens, panasz, hatósági megállapítás vagy jogszabályváltozás esetén soron kívül felülvizsgálja. A lényeges változásról annak hatálybalépése előtt, igazolható módon tájékoztatást ad.

14. Irányadó jogi és szakmai keret

- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR), különösen az 5–6., 9., 12–22., 24–25., 28., 30., 32–35., 44–49. és 77–82. cikk;
- 2011. évi CXII. törvény (Infotv.);
- 2012. évi I. törvény (Mt.), különösen a 9–11/A., 134., 155. és 286. §;
- 2019. évi LXXX. törvény (Szkt.) és a 12/2020. (II. 7.) Korm. rendelet;
- 1993. évi XCIII. törvény (Mvt.) és 33/1998. (VI. 24.) NM rendelet;
- 1997. évi LXXXIII. törvény (Ebtv.), 2019. évi CXXII. törvény (Tbj.), 1997. évi LXXXI. törvény (Tny.);
- 2017. évi CL. törvény (Art.), 1995. évi CXVII. törvény (Szja tv.) és 2000. évi C. törvény (Számviteli tv.);
- 1995. évi LXVI. törvény (Levéltári tv.), 2007. évi CLII. törvény (Vnytv.) és 2013. évi V. törvény (Ptk.);
- az Európai Adatvédelmi Testület 3/2019. iránymutatása a személyes adatok videoeszközökkel történő kezeléséről;
- a NAIH munkahelyi adatkezelésre, munkavállalói e-mail-fiókok és munkaeszközök ellenőrzésére, valamint kamerás megfigyelésre vonatkozó határozatai és tájékoztatói.

MELLÉKLET

MEGISMERÉSI NYILATKOZAT

Alulírott munkavállaló kijelentem, hogy a Székesfehérvári Szakképzési Centrum „Munkavállalói adatkezelési tájékoztató” című, 2026. június 1. napjától hatályos dokumentumát átvettem, annak tartalmát megismerhettem, kérdéseim feltételére és az adatvédelmi tisztviselő megkeresésére lehetőséget kaptam.

A nyilatkozat jelentése:

A jelen nyilatkozat kizárólag a tájékoztatás megtörténtének igazolására szolgál. Nem minősül a GDPR 6. cikk (1) a) pontja szerinti hozzájárulásnak, nem tesz jogszerűvé hozzájárulást igénylő adatkezelést, és nem korlátozza az érintetti jogok gyakorlását.

Munkavállaló neve:	Munkakör	Átvétel / megismerés dátuma:	Munkavállaló aláírása:

A munkavállaló a tájékoztató egy példányát vagy elektronikus elérhetőségét megkapta.

A későbbi lényeges módosításokról a Székesfehérvári Szakképzési Centrum külön, igazolható módon tájékoztat