SZÉKESFEHÉRVÁRI
SZAKKÉPZÉSI CENTRUM

ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZAT

a személyes adatok jogszerű, átlátható és biztonságos kezelésének belső rendjéről

Adatkezelő:	Székesfehérvári Szakképzési Centrum
Székhely:	8000 Székesfehérvár, Budai út 45. M2 épület
Képviseli:	Horváth Lajos Zoltán főigazgató és Kulcsár Szilvia kancellár
Adatvédelmi tisztviselő:	Adat-Mappa Bt. – adatvedelem@szfszc.hu
Dokumentum azonosítója:	NSZFH/634/ /2026
Hatálybalépés:	2026. június 1.
Kötelező felülvizsgálat:	Évente, továbbá minden lényeges jogi, szervezeti vagy technológiai változáskor

A jóváhagyás dátuma: 2026. június 1. **A jóváhagyó aláírása:** _____

1. A szabályzat célja, hatálya és jogforrásai

1.1. Cél

A szabályzat célja, hogy a Székesfehérvári Szakképzési Centrum, mint adatkezelő valamennyi szervezeti egységében és szakképző intézményében egységes, ellenőrizhető és kockázatarányos rendet állapítson meg a személyes adatok kezelésére. A szabályzat a GDPR szerinti elszámoltathatóság gyakorlati kerete: meghatározza a döntési és felelősségi rendet, az adatkezelések előzetes vizsgálatát, az érintetti jogok és incidensek kezelését, az adatfeldolgozók ellenőrzését, a megőrzés és törlés rendjét, valamint a megfelelés bizonyítékait.

A szabályzat nem teremt önmagában jogalapot. Személyes adat kizárólag konkrét, dokumentált cél, megfelelő GDPR-jogalap és – különleges vagy bűnügyi személyes adat esetén – további jogszabályi feltétel fennállásakor kezelhető. A működési érdek, a technikai lehetőség, a megszokás vagy a tájékoztató aláírása önmagában nem jogalap.

1.2. Személyi, tárgyi és területi hatály

A szabályzat hatálya kiterjed a Centrum központi szervezetére, valamennyi szakképző intézményére és telephelyére, továbbá minden olyan természetes személyre, aki a Centrum nevében vagy utasítása alapján személyes adatot kezel: vezetőre, munkavállalóra, oktatóra, megbízottra, gyakornokra, rendszergazdára, adatfeldolgozói vagy más közreműködői hozzáféréssel rendelkező személyre. A szabályzat alkalmazandó a papíralapú, elektronikus, kép-, hang-, videó-, napló-, helyadat- és más strukturált vagy nem strukturált adatkezelésre is.

A Centrum szakképző intézményei a Centrum szervezetén belül járnak el; önálló adatkezelői minőség csak kifejezett jogszabályi vagy szervezeti kijelölés alapján állapítható meg. Adatátadás előtt mindig tisztázni kell, hogy a címzett adatfeldolgozó, önálló adatkezelő vagy közös adatkezelő. Az elnevezés helyett a tényleges cél- és eszközmeghatározás dönt.

1.3. Irányadó jogi és szakmai keret

- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR);
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.);
- 2019. évi LXXX. törvény a szakképzésről (Szkt.) és a 12/2020. (II. 7.) Korm. rendelet (Szkr.);
- 2013. évi LXXVII. törvény a felnőttképzésről (Fktv.) és a 11/2020. (II. 7.) Korm. rendelet;
- 2018. évi LXXXIX. törvény az oktatási nyilvántartásról (Onytv.);
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.), különösen a személyiségi jogi és munkáltatói ellenőrzési szabályok;
- 2000. évi C. törvény a számvitelről, az adó-, társadalombiztosítási, egészségügyi, munkavédelmi, gyermekvédelmi, levéltári, közbeszerzési és vagyonnyilatkozati tárgyú külön jogszabályok;
- 2003. évi C. törvény az elektronikus hírközlésről, továbbá a Ptk. képmásra, hangfelvételre és igényérvényesítésre vonatkozó rendelkezései;
- a NAIH kötelező hatásvizsgálati jegyzéke, határozatai és ajánlásai, valamint az Európai Adatvédelmi Testület mindenkor irányadó iránymutatásai.

Jogszabályváltozás esetén a közvetlenül alkalmazandó vagy kötelező új szabály elsőbbséget élvez. A folyamatgazda és az adatvédelmi tisztviselő haladéktalanul kezdeményezi a szabályzat, a nyilvántartás, a tájékoztató és a technikai beállítás összehangolását.

2. Fogalmak és értelmezési szabályok

Személyes adat:	Azonosított vagy azonosítható természetes személyre vonatkozó bármely információ, ideértve az online azonosítót, helyadatot, képet, hangot, véleményt és következtetést is.

Adatkezelés:	A személyes adaton végzett bármely művelet, így a gyűjtés, rögzítés, rendszerezés, tárolás, megtekintés, továbbítás, összekapcsolás, közzététel, korlátozás, törlés és megsemmisítés.
Különleges személyes adat:	A GDPR 9. cikk (1) bekezdése szerinti adat, különösen egészségi, biometrikus azonosítási, vallási, politikai, szakszervezeti, faji vagy etnikai eredetre, szexuális életre vagy irányultságra vonatkozó adat.
Bűnügyi személyes adat:	Büntetőjogi felelősség megállapítására, bűncselekményre vagy kapcsolódó biztonsági intézkedésre vonatkozó adat; csak a GDPR 10. cikke és magyar jogi felhatalmazás szerint kezelhető.
Adatkezelő:	A Centrum, amely az adatkezelés céljait és eszközeit meghatározza, és e döntéseiért felel.
Adatfeldolgozó:	A Centrum nevében, dokumentált utasítás alapján személyes adatot kezelő külső szervezet vagy személy.
Folyamatgazda:	Az a vezető vagy kijelölt munkatárs, aki az adott adatkezelési folyamat szakmai céljáért, jogszerű működtetéséért és dokumentálásáért felel.
Rendszergazda / rendszerfelelős:	A technikai működésért, hozzáférés-kezelésért, naplózásért, mentésért és biztonsági intézkedésekért feladatkörében felelős személy; adatkezelési célt önállóan nem bővíthet.
Adatvédelmi incidens:	A biztonság olyan sérülése, amely személyes adat véletlen vagy jogellenes megsemmisülését, elvesztését, megváltoztatását, jogosulatlan közlését vagy hozzáférését eredményezi.
Anonimizálás:	Vissza nem fordítható művelet, amely után az adat észszerűen alkalmazható eszközökkel nem kapcsolható természetes személyhez. Az álnevesített adat továbbra is személyes adat.

3. Adatvédelmi alapelvek és tiltott gyakorlatok

Alapelv	Kötelező működési szabály	Bizonyíték
Jogszerűség, tisztességesség, átláthatóság	Minden célhoz jogalap és közérthető tájékoztatás; rejtett vagy megtévesztő adatgyűjtés tilos.	Nyilvántartás, tájékoztató, jogalap-elemzés.
Célhoz kötöttség	Az adat csak előre meghatározott, kifejezett célra használható; új cél előtt összeegyeztethetőségi vizsgálat kell.	Célleírás, változásengedély, szükség esetén új tájékoztató.
Adattakarékosság	Csak a célhoz ténylegesen szükséges adat kérhető; teljes okmánymásolat és teljes egészségügyi irat csak kifejezett indokkal.	Űrlap- és mezőlista-felülvizsgálat, minimalizálási döntés.
Pontosság	Az adatot észszerűen naprakészen kell tartani; a vitatott vagy téves adatot jelölni és helyesbíteni kell.	Helyesbítési napló, adatminőségi ellenőrzés.
Korlátozott tárolhatóság	Minden adatkörhöz konkrét törlési vagy felülvizsgálati esemény tartozik; a „korlátlan” vagy „szükség szerint” határidő nem elegendő.	Megőrzési jegyzék, törlési napló, selejtezési jegyzőkönyv.
Integritás és bizalmas jelleg	Kockázatarányos szervezési és technikai intézkedések; legkisebb jogosultság; incidensek azonnali jelzése.	Jogosultsági lista, napló, mentési és tesztjegyzőkönyv.
Elszámoltathatóság	A Centrum nemcsak megfelel, hanem ezt döntési és végrehajtási bizonyítékokkal igazolja.	Jóváhagyások, oktatás, audit, szerződések.

Kifejezetten tilos:
„Biztonság kedvéért” többletadatot gyűjteni; üres vagy általános hozzájárulást kérni; kötelező adatkezelést hozzájárulásként feltüntetni; magán e-mailre vagy jóvá nem hagyott felhőbe személyes adatot továbbítani; közös felhasználói azonosítót használni; jelszót megosztani; nyilvános címzettlistával tömeges e-mailt küldeni; személyes adatot tesztadatként kontroll nélkül használni; engedély nélkül külső adathordozóra másolni; adatvédelmi tisztviselői véleményt elhallgatni vagy utólagosan beszerezni egy már megkezdett magas kockázatú adatkezeléshez.

4. Szervezet, felelősségek és döntési rend

4.1. A vezetés felelőssége

A főigazgató és a kancellár a hatáskörük és a Centrum belső irányítási rendje szerint gondoskodnak az adatvédelmi megfeleléshez szükséges szervezetről, erőforrásról, szabályozásról és végrehajtásról. Biztosítják az adatvédelmi tisztviselő függetlenségét, megfelelő és kellő idejű bevonását, hozzáférését a szükséges információkhoz, továbbá azt, hogy feladatai ellátása miatt utasítás, hátrány vagy összeférhetetlenség ne érje.
A vezetés adatkezelési döntését nem ruházhatja át az adatvédelmi tisztviselőre. Ha a vezetés a tisztviselő dokumentált szakmai véleményétől eltér, az eltérés okát, a vállalt kockázatot és a kompenzáló intézkedést írásban rögzíteni kell.

4.2. Szerepkörök

Szereplő	Fő feladat	Kötelező bizonyíték / eredmény
Főigazgató / kancellár	Szabályozás, erőforrás, magas kockázatú döntés, incidensbejelentés és hatósági együttműködés jóváhagyása a belső hatásköri rend szerint.	Jóváhagyás, vezetői döntés, erőforrás- és intézkedési terv.
Intézményvezető	A szabályzat helyi végrehajtása, helyi folyamatok és hozzáférések ellenőrzése, incidens és változás jelzése.	Helyi felelőslista, éves igazolás, intézkedési jegyzőkönyv.
Adatvédelmi tisztviselő	Tanácsadás, ellenőrzés, DPIA (adatvédelmi hatásvizsgálat) szükségességének ellenőrzése, oktatási és auditjavaslat, NAIH-kapcsolattartás; döntési felelősség átvétele nélkül.	Írásbeli vélemény, ellenőrzési jelentés, DPIA-tanács, éves beszámoló.
Adatvédelmi koordinátor	Központi nyilvántartások, kérelmek, incidensek, határidők és dokumentumverziók operatív koordinációja.	Nyilvántartás, határidőnapló, dokumentumcsomag.
Folyamatgazda	Cél, adatkör, jogalap, címzett, megőrzés, tájékoztatás és tényleges gyakorlat megfelelése.	Folyamatlap, felülvizsgálat, törlési és hozzáférési igazolás.
Rendszerfelelős / IT	Biztonságos konfiguráció, jogosultság, napló, mentés, sérülékenység-kezelés, törlés technikai végrehajtása.	Rendszerleltár, jogosultsági napló, mentési és törlési jegyzőkönyv.
HR, tanügy, pénzügy, beszerzés	Szakmai folyamat és iratkezelés, adatminimalizálás, határidő, címzettek és adatszolgáltatások ellenőrzése.	Ügyirat, ellenőrző lista, jogszabályi hivatkozás, átadás igazolása.
Minden hozzáférő személy	Utasítás, célhoz kötöttség, titoktartás, biztonság, pontosság, incidens és kérelem azonnali jelzése.	Oktatási és megismerési igazolás; szükség esetén eseményjelentés.

4.3. Kötelező eszkaláció

A munkatárs haladéktalanul, de legkésőbb az észleléstől számított 4 munkaórán belül jelzi a közvetlen vezetőnek, az adatvédelmi koordinátornak és az erre kijelölt informatikai elérhetőségen: az adatvesztést vagy jogosulatlan hozzáférést; téves címzettet; elveszett eszközt; kártékony kódot; tömeges vagy különleges adatot érintő hibát; érintetti kérelmet; hatósági megkeresést; új adatgyűjtési igényt; új szolgáltatót, rendszert, kamerát, biometrikus vagy MI-megoldást; továbbá a szabályzat és a tényleges gyakorlat bármely eltérését. Az eszkaláció nem várhat vezetői aláírásra vagy teljes kivizsgálásra.

5. Az adatkezelési nyilvántartás és az elszámoltathatóság bizonyítékai

A Centrum a GDPR 30. cikke szerinti adatkezelési tevékenységek nyilvántartását központilag vezeti. Az intézmények és folyamatgazdák adatot szolgáltatnak, a változásokat öt munkanapon belül bejelentik, és legalább évente tételesen igazolják a rájuk vonatkozó bejegyzések pontosságát. A nyilvántartás nem puszta lista: egyeznie kell a tájékoztatókkal, űrlapokkal, szerződésekkel, rendszerbeállításokkal, hozzáférésekkel és törlési gyakorlattal.

- minden folyamat egyedi azonosítója, megnevezése, célja és folyamatgazdája;
- érintettek, adatkategóriák, adatok forrása és az adatszolgáltatás kötelező vagy önkéntes jellege;
- jogalap célonként, különleges és bűnügyi adat további feltétele, valamint a pontos jogszabályhely;
- címzettek és az adatkezelői szerep, adatfeldolgozó és al-adatfeldolgozó, rendszer és tárolási hely;
- EGT-n kívüli továbbítás, ország, címzett, mechanizmus, adattovábbítási hatásvizsgálat és kiegészítő garancia;
- konkrét megőrzési idő vagy törlési esemény, irattári tétel, mentési ciklus és a törlés felelőse;
- technikai és szervezési intézkedések, hozzáférő szerepkörök, naplózás és rendszeres felülvizsgálat;
- tájékoztató, hozzájárulás, érdekmérlegelés, DPIA, szerződés és vezetői döntés verziója és helye.

> Nyilvántartási minőségi szabály:
> A „szabályzat szerint”, „jogszabály szerint”, „ha van”, „szükség szerint” vagy kérdőjeles megjegyzés csak ideiglenes hibajelzés lehet, végleges nyilvántartási adat nem. A folyamatgazda köteles konkrét határidőt, szolgáltatót, szerepet, rendszernevet vagy pontos jogszabályhelyet rögzíteni. Az ismert, de még nem igazolt adatot „ellenőrzés alatt” státusszal és határidős intézkedéssel kell kezelni.

A bizonyítási csomag legalább a hatályos szabályzatból, folyamatnyilvántartásból, tájékoztatókból, szerződésekből, LIA/DPIA-dokumentumokból, jogosultsági és törlési jegyzőkönyvekből, oktatási nyilvántartásból, incidens- és jogkérelmi naplóból, valamint a legutóbbi audit és vezetői felülvizsgálat eredményéből áll.

6. Új vagy megváltozó adatkezelés előzetes engedélyezése

6.1. Bejelentési kötelezettség és adatvédelem a tervezéskor

Új adatkezelés, űrlap, kérdőív, rendszer, alkalmazás, felhőszolgáltatás, külső adattovábbítás, megfigyelés, elemzés, beágyazott webes elem, MI-funkció vagy a meglévő cél, adatkör, címzett, megőrzés, technológia, érintetti kör lényeges változása csak előzetes adatvédelmi kontroll után indítható. A folyamatgazda a tervezett indulás előtt legalább 20 munkanappal benyújtja az A. melléklet szerinti változáslapot; sürgősség nem igazolja a kontroll mellőzését.

1. A folyamatgazda meghatározza a célt, szükségességet, érintetteket, adatmezőket, forrást, jogalapot, címzetteket, megőrzést, rendszert és felelősöket.
2. Az IT/rendszerfelelős elvégzi a biztonsági, hozzáférési, naplózási, mentési, törlési, integrációs és beszállítói vizsgálatot.
3. A beszerzés vagy szerződésgazda tisztázza a szolgáltatói szerepet, Adatfeldolgozókat, adatkezelési helyeket és szerződéses garanciákat.
4. Az adatvédelmi tisztviselő véleményezi a jogalapot, minimalizálást, átláthatóságot, érintetti kockázatot, LIA/DPIA szükségességét és adattovábbítást.

5. A jóváhagyásra jogosult vezető a vélemények és a fennmaradó kockázat alapján dönt; magas kockázat elfogadása kizárólag írásban történhet.
6. Indulás előtt frissül a nyilvántartás, tájékoztató, megőrzési és jogosultsági rend, valamint megtörténik a technikai teszt és az érintett munkatársak oktatása.

6.2. Érdekmérlegelési teszt

GDPR 6. cikk (1) f) pont csak akkor alkalmazható, ha a Centrum az adott műveletnél nem közfeladatot ellátó szervként jár el, az érdek jogszerű, valós és kellően konkrét, az adatkezelés szükséges, nincs kevésbé beavatkozó alternatíva, és az érintett jogai nem élveznek elsőbbséget. A tesztnek ki kell térnie az érintett észszerű elvárására, kiszolgáltatottságára, gyermekekre, adatok jellegére, hatókörére, megőrzésére, tiltakozásra és garanciákra. A B. melléklet szerinti tesztet az adatkezelés előtt jóvá kell hagyni és változáskor meg kell ismételni.

6.3. Adatvédelmi hatásvizsgálat és előzetes konzultáció

A C. melléklet szerinti DPIA-előszűrés minden új vagy lényegesen változó adatkezelésnél kötelező. Hatásvizsgálatot kell végezni, ha az adatkezelés – különösen új technológia, módszeres megfigyelés, gyermekek vagy más kiszolgáltatott személyek, nagy számú különleges adat, biometria, helyadat, profilalkotás, összekapcsolt adatállomány vagy automatizált jelentős döntés miatt – valószínűsíthetően magas kockázattal jár, illetve ha a NAIH kötelező jegyzéke ezt előírja.
A DPIA rögzíti a műveletek rendszeres leírását, célját, szükségességét és arányosságát, a jogokra és szabadságokra leselkedő kockázatokat, az intézkedéseket, a fennmaradó kockázatot, a DPO véleményét és az érintettek véleményének kezelését. Ha a magas fennmaradó kockázat megfelelően nem mérsékelhető, az adatkezelés nem kezdhető meg; a Centrum a GDPR 36. cikke szerint előzetesen konzultál a NAIH-hal.

7. Jogalap, különleges és bűnügyi személyes adatok

Jogalap	Alkalmazási szabály	Tipikus centrumi kör
GDPR 6. cikk (1) c)	A Centrumra vonatkozó konkrét uniós vagy magyar jogi kötelezettség; a jogszabályhelyet és kötelező adatkört rögzíteni kell.	Adó, számvitel, bér, tanügyi és felnőttképzési nyilvántartás, irattár, incidens.
GDPR 6. cikk (1) e)	A jogszabályon alapuló közérdekű feladat végrehajtásához szükséges; meg kell nevezni a közfeladatot és a szükségességet.	Szakképzés, tanulói ügyintézés, intézményi tájékoztatás, biztonságos működés.
GDPR 6. cikk (1) b)	Az érintettel kötött szerződés teljesítése vagy az érintett kérésére szerződés előtti lépés; csak elengedhetetlen adatokra.	Felnőttképzési és terembérleti szerződés, természetes személy partner, álláspályázat.
GDPR 6. cikk (1) f)	Csak nem közfeladati működésben, dokumentált érdekmérlegeléssel és hatékony tiltakozási lehetőséggel.	Kivételes vagyonvédelem, jogi igény, partnerkapcsolat; nem használható kényelmi rövidítésként.
GDPR 6. cikk (1) a)	Valóban önkéntes, konkrét, célonként külön, tájékozott, aktív és bizonyítható; ugyanolyan könnyen visszavonható.	Pályázói adatbázis, nem szükséges süti, egyedi promóciós portré, külön marketing.

Különleges személyes adat csak egy 6. cikk szerinti jogalap és a GDPR 9. cikk (2) bekezdésének konkrét feltétele együttes fennállásakor kezelhető. Foglalkoztatási, szociális, oktatási vagy egészségügyi kötelezettségnél különösen a b), g) vagy h) pont jöhet szóba; jogi igénynél az f), közérdekű archiválásnál a j) pont. Kifejezett hozzájárulás csak valóban szabad választási helyzetben alkalmazható. Diagnózis

vagy teljes orvosi dokumentáció helyett főszabály szerint csak az alkalmasság, kedvezmény vagy szükséges korlátozás ténye kezelhető.
Bűnügyi személyes adat csak uniós vagy magyar jogi felhatalmazás és megfelelő garanciák alapján kezelhető. Erkölcsi bizonyítványról másolat csak akkor őrizhető, ha jogszabály ezt kifejezetten szükségessé teszi; egyébként a bemutatás, érvényesség és a releváns feltétel teljesülésének rögzítése elegendő. Fegyelmi vagy magatartási adat nem automatikusan bűnügyi adat, de fokozottan bizalmas.

8. Tájékoztatás, hozzájárulás és gyermekek adatainak kezelése

8.1. Tájékoztatás
A GDPR 13–14. cikke szerinti tájékoztatást az adatgyűjtéskor, közvetett adatgyűjtésnél legkésőbb a GDPR 14. cikkében meghatározott időben, közérthetően és az érintetti körhöz igazodva kell megadni. A hosszú tájékoztató rétegzett rövid tájékoztatóval egészíthető ki, de a lényeges információ nem rejthető el. Az „elolvastam” vagy „tudomásul vettem” nyilatkozat a tájékoztatás igazolása, nem hozzájárulás.
A Centrum külön tájékoztatót tart fenn legalább a munkavállalók, álláspályázók, tanulók és felnőttképzésben részt vevők, törvényes képviselők, üzleti partnerek és kapcsolattartók, weboldallátogatók, valamint a kamerával megfigyelt személyek részére. Egyedi projekt, rendezvény, kutatás, űrlap, pályázat vagy új technológia további rétegzett tájékoztatást igényelhet.

8.2. Hozzájárulás
- a hozzájárulás célonként külön, aktív nyilatkozattal történik; előre bejelölt négyzet, hallgatás vagy továbbhasználat nem elfogadás;
- a teljesítéshez nem szükséges adatkezelés nem tehető szolgáltatás, oktatás, munkaviszony vagy előny feltételévé;
- a Centrum bizonyítja, ki, mikor, milyen tájékoztató-verzió és cél alapján adott hozzájárulást;
- a visszavonás legalább olyan egyszerű, mint a megadás; a visszavonást haladéktalanul továbbítani kell minden végrehajtó rendszer és címzett felé;
- munkavállalói és tanulói alá-fölérendeltségben a hozzájárulás önkéntességét különösen szigorúan kell vizsgálni; hátrány nem kapcsolódhat a megtagadáshoz.

8.3. Gyermekek és törvényes képviselők
Gyermek adatának kezelésekor a gyermek mindenek felett álló érdekét, életkorát, érettségét, kiszolgáltatottságát és jövőbeli hatásokat külön kell értékelni. A gyermek saját érintetti jogokkal rendelkezik; a tájékoztatást számára is érthetően kell megadni. A törvényes képviselő közreműködése nem korlátlan hozzáférési jog: a gyermek magánszféráját, véleményét, nagykorúságát és a Szkt. speciális szabályait figyelembe kell venni. Kiskorút reklámcélból profilozni, szükségtelen nyomkövetővel követni vagy nyilvános portré közzétételéhez hátrány kilátásba helyezésével hozzájárulásra ösztönözni tilos.

9. Az érintetti jogok teljesítésének eljárása

9.1. Kérelem fogadása és határidő
A Centrum bármely szervezeti egységéhez szóban, írásban vagy elektronikus úton érkező, tartalma szerint adatvédelmi kérelemnek minősülő megkeresést azonnal, de legkésőbb egy munkanapon belül továbbítani kell az adatvédelmi tisztviselő munkáját segítő koordinátornak és az adatvédelmi tisztviselőnek. A kérelem érvényessége nem függ a „GDPR” szó használatától vagy meghatározott űrlaptól. A Centrum indokolatlan késedelem nélkül, legkésőbb egy hónapon belül válaszol. Az összetettség vagy kérelmek száma miatt lehetséges további két hónapos hosszabbításról az első hónapon belül, indokolással kell tájékoztatni.

9.2. Eljárási lépések
1. A koordinátor a D. melléklet szerinti naplóban rögzíti a kérelmet, a határidőt, érintett rendszereket, felelőst és azonosítási módot.

2. A személyazonosságot kockázatarányosan kell ellenőrizni; rutinszerű okmánymásolat kérés tilos. Kétség esetén csak a szükséges kiegészítő adat kérhető.
3. A folyamatgazdák és rendszerfelelősök haladéktalanul, főszabály szerint öt munkanapon belül megőrzik és átadják a releváns adatot, naplót és forrásinformációt.
4. Hozzáférési másolat előtt el kell különíteni a kérelmező adatait, és védeni kell más személy jogait; a megtagadás nem lehet általános, szükség esetén kitakarás alkalmazandó.
5. Törlés, korlátozás vagy helyesbítés esetén az intézkedést minden releváns rendszerben, iratban, kereshető másolatban és címzettnél végre kell hajtani, vagy a jogszerű kivételt dokumentálni kell.
6. A válasz közérthető, teljes és bizonyítható módon kerül kiküldésre; az ügy lezárását, végrehajtását és esetleges jogorvoslati tájékoztatását a napló rögzíti.

A korlátozás alatt álló adat egyértelmű jelöléssel csak tárolható, kivéve az érintett hozzájárulását, jogi igényt, más személy jogainak védelmét vagy fontos közérdeket. Tiltakozás esetén a folyamatgazda és a DPO megvizsgálja, van-e elsőbbséget élvező kényszerítő ok. Közvetlen üzletszerzési célú tiltakozás esetén az adat e célra tovább nem kezelhető.

A kérelmi dokumentációt a lezárástól számított 5 évig kell megőrizni, jogvita vagy hatósági eljárás esetén annak végleges lezárásáig. A személyazonosításhoz ideiglenesen bekért többletadatot a sikeres azonosítás után törölni kell, ha további megőrzése nem szükséges.

10. Adatmegőrzés, törlés, anonimizálás és irattározás

10.1. Megőrzési rend

A megőrzési időt elsődlegesen jogszabály, irattári terv, szerződéses kötelezettség, jogviszonyi cél vagy dokumentált igényérvényesítési szükséglet határozza meg. Ugyanazon irat különböző adataihoz vagy céljaihoz eltérő határidő tartozhat. A leghosszabb határidő nem alkalmazható automatikusan minden másolatra és rendszerre. A nyilvántartásban a konkrét időt, kezdő eseményt, kivételt és törlés felelősét rögzíteni kell.

Folyamatcsalád	Irányadó belső megőrzés	Kontroll
Számviteli, adó- és kifizetői bizonylat	Legalább 8 év a vonatkozó törvényi kezdőponttól.	Csak bizonylati tartalom; munkapéldány és fölös másolat előbb törlendő.
Tanulói intézményi személyes adatok	A Szkt. szerinti adat főszabály szerint a jogviszony megszűnésétől számított 10. év utolsó napjáig.	Törzslap, bizonyítvány-nyilvántartás és maradandó irat külön, hosszabb lehet.
Felnőttképzési adat és dokumentum	Az Fktv. szerinti 8. év végéig, a törvényben meghatározott kezdőponttal.	Képzéstípus és dokumentum szerint ellenőrizendő.
Szkt. szerinti alkalmazotti adat	A jogviszony megszűnésétől számított 5 év, ha az adott adatkörre a Szkt. ezt írja elő.	Személyi és nyugdíjbizonyító irat csak irattári/jogi indokkal hosszabb.
Munkajogi és bérigény	Az Mt. szerinti igény idejéig; számviteli/bérbizonylatnál 8 év.	A teljes személyi anyagra nem alkalmazható automatikusan azonos idő.
Álláspályázat	Lezárás után legfeljebb 3 hónap; állományban külön hozzájárulással legfeljebb 12 hónap.	Visszavonáskor törlés; jogvita esetén csak releváns bizonyíték zárolható.
Szerződés és partnerkapcsolat	Megszűnés + általános igényérvényesítési idő; bizonylat 8 év.	Kapcsolattartói törzsadat kapcsolat megszűnésekor felülvizsgálandó.
Web- és biztonsági napló	Cél szerint jellemzően 30–90 nap; hozzáférési napló indokoltan 6–12 hónap.	Incidensrészlet elkülöníthető; anonim statisztika nem személyes adat.

Folyamatcsalád	Irányadó belső megőrzés	Kontroll
Adatvédelmi incidens és jogkérelem	Lezárástól 5 év.	Jogvita esetén a releváns rész a végleges lezárásig.
Kamerafelvétel	Kameránként indokolt rövid idő; főszabály szerint 72 óra, dokumentált szükségességgel legfeljebb 7 nap.	30 nap vagy hosszabb csak kivételes, kameránként bizonyított szükségességgel és DPIA-kontrollal.
Részletes GPS-adat	A célhoz szükséges rövid idő, legfeljebb 90 nap.	Menetlevél/számviteli bizonylat külön 8 év lehet; folyamatos magánidős követés tilos.

10.2. Törlés és selejtezés

A folyamatgazda legalább negyedévente futtatja vagy kezdeményezi a lejárt adatok törlését. Az elektronikus törlésnek ki kell terjednie az éles rendszerre, exportokra, munkapéldányokra, megosztásokra és – a technikai mentési ciklus szerint – biztonsági másolatokra. A mentésből történő visszaállításkor a közben lejárt vagy korábban törölt adatot ismét törölni kell. Papíriratot ellenőrzött, visszaállíthatatlan módon kell megsemmisíteni vagy irattári/levéltári rend szerint átadni.

Jogi igény, hatósági ügy vagy incidens miatti zárolás csak a szükséges adatra, dokumentált kezdő- és felülvizsgálati idővel alkalmazható. A „perveszély” általános hivatkozása nem indokolja teljes adatállomány határozatlan megőrzését. Törlésről vagy anonimizálásról az E. melléklet szerinti jegyzőkönyv készül.

11. Hozzáférés-kezelés és információbiztonság

11.1. Alapkövetelmények

- személyre szóló azonosító, legkisebb szükséges jogosultság, feladatkörök elkülönítése és jóváhagyási lánc;
- belépéskor, munkakörváltozáskor és kilépéskor dokumentált jogosultságkezelés; megszűnő hozzáférés főszabály szerint azonnal, legkésőbb a munkanap végéig visszavonandó;
- negyedéves kiemelt/adminisztrátori és legalább féléves általános jogosultság-felülvizsgálat;
- erős hitelesítés, adminisztrátori és távoli hozzáférésnél többtényezős azonosítás, ahol technikailag elérhető;
- titkosított adatátvitel, hordozható eszköz és különleges adatok kockázatarányos titkosítása; engedély nélküli pendrive tiltása;
- naprakész frissítés-, kártevő-, tűzfal-, e-mail- és végpontvédelem, sérülékenység-kezelés és biztonsági konfiguráció;
- elkülönített, tesztelt biztonsági mentés; helyreállítási célok és felelősök dokumentálása;
- papíriratok zárt tárolása, tiszta asztal, biztonságos nyomtatás, ellenőrzött szállítás és megsemmisítés;
- naplózás az adminisztrátori, hozzáférési, export-, törlési és biztonsági eseményekről; a naplóhoz való hozzáférés elkülönítése;
- személyes adat fejlesztési vagy tesztkörnyezetben csak dokumentált szükségesség, minimalizálás és maszkolás mellett használható.

11.2. Levelezés, fájlmegosztás és hordozható eszköz

Személyes adatot kizárólag jóváhagyott intézményi rendszerben lehet továbbítani és tárolni. Tömeges küldésnél a címzettek egymás előtti felfedését BCC, címlista-kezelő vagy személyre szabott küldés akadályozza meg. Különleges, nagy mennyiségű vagy magas kockázatú adat e-mailben csak szükségesség esetén, megfelelő titkosítással és a jelszó külön csatornán történő közlésével továbbítható. Magán e-mail, fogyasztói felhő, nyilvános fájlmegosztó, ismeretlen üzenetküldő és engedély nélküli külső adathordozó használata tilos.

11.3. Fizikai és működésfolytonossági védelem

A különleges, gyermekvédelmi, fegyelmi, bér-, vagyonnyilatkozati és vizsgálati iratokat elkülönítetten, szűkített hozzáféréssel kell kezelni. Az irattár, szerverhelyiség, kulcs és belépőkártya hozzáférését nyilvántartani kell. A rendszerfelelős évente helyreállítási próbát végez, és dokumentálja a helyreállíthatóságot, a hiányosságot és a javító intézkedést.

12. Adatvédelmi incidensek kezelése

12.1. Bejelentés és azonnali intézkedés

Minden munkatárs köteles az adatvédelmi incidens tényét vagy megalapozott gyanúját azonnal, legkésőbb 4 munkaórán belül a kijelölt incidenscsatornán bejelenteni. Az adatfeldolgozói szerződés ettől eltérően, indokolatlan késedelem nélküli – javasoltan 12 órás – értesítést ír elő. A bejelentő nem törölhet bizonyítékot, nem kommunikálhat önállóan az érintettekkel vagy a sajtóval, és nem várhat a teljes ok feltárására.

Az IT azonnal korlátozza a további kárt: téves e-mail visszahívása és címzett megkeresése, fiók tiltása, jelszócsere, eszköz távoli zárolása, hálózati elkülönítés, jogosultság visszavonása, naplók és bizonyítékok sértetlen megőrzése. Az intézkedés nem semmisítheti meg a kivizsgáláshoz szükséges adatot.

12.2. Kockázatértékelés és döntés

1. A koordinátor az F. melléklet szerinti incidensnaplót megnyitja, rögzíti a tudomásszerzés pontos időpontját és kijelöli a vizsgálati felelősöket.
2. Az incidenscsoport feltárja az érintettek számát és körét, az adatok jellegét és mennyiségét, a hozzáférhetőséget, a valószínű következményeket, a visszaélés lehetőségét és a megtett intézkedéseket.
3. Az adatvédelmi tisztviselő haladéktalanul véleményezi a természetes személyek jogaira és szabadságaira jelentett kockázatot, a NAIH-bejelentés és az érintetti tájékoztatás szükségességét.
4. A hatáskörrel rendelkező vezető dönt. A NAIH-bejelentést indokolatlan késedelem nélkül, lehetőség szerint a tudomásszerzéstől számított 72 órán belül meg kell tenni, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal.
5. Magas kockázat esetén az érintetteket indokolatlan késedelem nélkül, világosan tájékoztatni kell, kivéve, ha a GDPR 34. cikkének dokumentált kivétele alkalmazható.
6. A kivizsgálás gyökérok-elemzéssel, helyesbítő és megelőző intézkedéssel, felelőssel és határidővel zárul; a végrehajtást utóellenőrizni kell.

Minden incidens dokumentálandó:
A NAIH-nak be nem jelentett incidensnél is rögzíteni kell a tényeket, hatásokat, intézkedéseket és a be nem jelentés kockázati indokát. A 72 órás határidő a tudomásszerzéstől fut; a döntéshozó távolléte vagy a teljes vizsgálat befejezetlensége nem igazolja a késedelmet. Hiányos adatok esetén szakaszos bejelentés tehető.

Az incidensnyilvántartást és a kapcsolódó döntési dokumentumokat a lezárástól számított 5 évig, folyamatban lévő hatósági vagy bírósági ügyben annak végleges lezárásáig kell megőrizni.

13. Adatfeldolgozók, címzettek és adatkezelői szerepek

13.1. Beszállítói előzetes vizsgálat

Személyes adatot érintő szolgáltatás csak a G. melléklet szerinti átvilágítás után vehető igénybe. Vizsgálandó a szolgáltató szakértelme, biztonsági és adatvédelmi intézkedése, incidensmúltja, tanúsítása, adatkezelési helye, al-adatfeldolgozói lánca, törlési és hordozhatósági képessége, hatósági hozzáférési kockázata, üzletmenet-folytonossága és szerződéses felelőssége. Ingyenes vagy kipróbálási szolgáltatás sem kivétel.

13.2. Kötelező szerződéses tartalom

- az adatkezelés tárgya, időtartama, jellege, célja, adatok és érintettek kategóriái;
- kizárólag dokumentált utasítás, titoktartás, célkorlátozás és megfelelő biztonság;
- al-adatfeldolgozó előzetes egyedi vagy általános engedélye és változás elleni tiltakozás lehetősége;
- érintetti kérelmek, DPIA, audit, NAIH-vizsgálat és elszámoltathatóság támogatása;
- incidens indokolatlan késedelem nélküli, szerződésben meghatározott rövid határidejű jelzése és folyamatos információadás;
- a szolgáltatás végén az adatok választás szerinti visszaszolgáltatása és bizonyítható törlése, mentések kezelése;
- auditjog, bizonyítékok átadása, hiányosság javítása, lényeges jogsértésnél felfüggesztés és megszüntetés;
- harmadik országbeli továbbítás és hatósági megkeresés kezelése, kiegészítő garanciák.

A MÁK, NAV, Oktatási Hivatal, egészségügyi szolgáltató, duális képzőhely, bank, posta, bíróság vagy hatóság szerepét nem szabad automatikusan adatfeldolgozóként rögzíteni; saját törvényi cél és döntési jog esetén önálló adatkezelők. Közös cél- és eszközmeghatározás esetén a GDPR 26. cikke szerinti megállapodás és az érintettek számára hozzáférhető lényeg szükséges.

14. Nemzetközi adattovábbítás

Az EGT-n kívüli továbbítás, távoli hozzáférés, támogatás, mentés vagy globális felhőszolgáltatás csak előzetes dokumentált vizsgálat után engedélyezhető. Elsőként megfelelőségi határozat, ennek hiányában megfelelő garancia – jellemzően általános adatvédelmi kikötés – és szükség esetén adattovábbítási hatásvizsgálat alkalmazandó. Vizsgálni kell a célország jogát és gyakorlatát, a hozzáférési lehetőségeket, titkosítást és kulcskezelést, adatlokalizációt, álnevesítést, szerződéses értesítést és jogorvoslatot.

A GDPR 49. cikke szerinti kivétel nem használható rendszeres, tömeges vagy szervezetszerű továbbítás általános alapjaként. A szolgáltató puszta szerződéses kijelentése nem elegendő. A folyamatnyilvántartásban fel kell tüntetni a címzettet, országot, mechanizmust, dokumentum verzióját és a kiegészítő intézkedést.

15. Munkavállalói és pályázói adatkezelések

15.1. Foglalkoztatás

A munkaviszonyhoz kapcsolódó személyes adat csak a munkaviszony létesítéséhez, teljesítéséhez, megszüntetéséhez, jogszabályi nyilvántartáshoz, bérhez, adóhoz, társadalombiztosításhoz, távolléthez, alkalmassághoz, munkavédelemhez, eszköz- és jogosultságkezeléshez, jogi igényhez vagy külön dokumentált célhoz szükséges körben kezelhető. Egészségügyi dokumentáció helyett a Centrum főszabály szerint csak az alkalmasság tényét, időbeli hatályát és szükséges korlátozást kapja meg; a foglalkozás-egészségügyi szolgáltató az orvosi dokumentáció tekintetében rendszerint önálló adatkezelő. Munkáltatói hozzájárulás csak valóban szabadon választható célra használható. Bér, jelenlét, szabadság, táppénz, CSED/GYED, járulék, munkabaleset, eszközkiadás, vagyonnyilatkozat és kötelező nyilvántartás nem hozzájáruláson alapul. A személyi anyaghoz csak a HR, a döntésre jogosult vezető és törvényes címzett férhet hozzá feladati körben.

15.2. Álláspályázók

A pályázati anyag a kiválasztáshoz szükséges adatokra korlátozandó. Interjún családi állapotra, gyermekvállalásra, vallásra, egészségre, fogyatékosságra, politikai nézetre vagy más magánéleti körülményre csak akkor kérdezhető rá, ha az adott munkakör szempontjából közvetlenül szükséges és jogszerű; ennek indokát előzetesen dokumentálni kell. Nyilvános közösségimédia-profil általános átvilágítása tilos; célzott ellenőrzés csak munkaköri szükségesség, előzetes tájékoztatás és dokumentált jogalap mellett végezhető.

Sikertelen pályázat anyaga a kiválasztás lezárását követően legfeljebb 3 hónapig őrizhető; későbbi álláslehetőséghez külön, önkéntes hozzájárulással legfeljebb 12 hónapig. Referencia csak a pályázó előzetes tájékoztatása és megfelelő jogalap alapján kérhető. Automatikus kizárás vagy kizárólag algoritmikus rangsorolás nem alkalmazható emberi kontroll nélkül.

16. Tanulói, felnőttképzési és gyermekeket érintő adatkezelések

A tanulói, jelentkezési, beiratkozási, oktatási, értékelési, hiányzási, vizsga-, bizonyítvány-, ösztöndíj-, duális képzési, felnőttképzési és tanügyi adatok kezelését az Szkt., Szkr., Fktv., Onytv. és kapcsolódó szabályok szerinti célra és adatkörben kell végezni. A KRÉTA és más rendszer jogosultságát szerepkörre, intézményre, osztályra és feladatra kell korlátozni. A törvényes képviselői hozzáférést a gyermek életkora, jogállása és speciális ágazati szabály szerint kell biztosítani vagy korlátozni.

SNI-, BTMN-, fogyatékossági, egészségi, szociális és gyermekvédelmi adat csak a támogatás, kedvezmény, biztonság vagy jogszabályi feladat szükséges körében, elkülönített hozzáféréssel kezelhető. Teljes szakértői vagy egészségügyi irat helyett lehetőség szerint a releváns megállapítást, kedvezményt és érvényességet kell rögzíteni. Gyermekvédelmi jelzéshez vagy törvényes adattovábbításhoz hozzájárulás nem szükséges, de az adatminimalizálás igen.

Digitális oktatási platform csak jóváhagyás, szerződéses és biztonsági vizsgálat után használható. Magánfiók kötelezővé tétele, óra vagy vizsga indokolatlan rögzítése, arcfelismerés, rejtett figyelemkövetés, érzelemfelismerés és gyermekek reklámprofilozása tilos. Szakirányú oktatásnál a duális képzőhely adatkezelői szerepét és a továbbított adatkört írásban rendezni kell.

17. Partneri, pénzügyi, projekt- és rendezvényi adatkezelések

Természetes személy partnernél a szerződés teljesítéséhez, jogi személy kapcsolattartójánál a közfeladati vagy dokumentált kapcsolattartási célhoz szükséges adat kezelhető. Személyazonosító okmány száma vagy más hatósági azonosító csak jogszabályi, pénzügyi vagy tényleges azonosítási szükséglet esetén rögzíthető; okmánymásolat főszabály szerint nem készül. A partner kapcsolattartóját akkor is tájékoztatni kell, ha adatait a munkáltatója adta át.

Számlázási, adózási, kifizetői, ösztöndíj-, támogatási és pályázati adatokat az alkalmazandó bizonylati és auditkötelezettség szerint kell kezelni. A támogató vagy ellenőrző szerv igénye nem írhatja felül a célhoz kötöttséget; a pályázati felhívás és szerződés adatigényét a benyújtás előtt ellenőrizni kell. A számviteli 8 éves idő nem hosszabbítja meg automatikusan a teljes kapcsolattartási vagy rendezvényadatbázist.

Workshop, fizetős rendezvény, ajándéksorsolás vagy nyereményjáték előtt külön részvételi szabály, tájékoztató, adatmezőlista, sorsolási vagy kiválasztási integritás, nyertes-közzétételi jogalap és törlési terv szükséges. A rendezvényen készült egyedi portré vagy promóciós videó főszabály szerint külön hozzájárulással tehető közzé; tömegfelvételnél előzetes jelzés, szükségesség, arányosság és a Ptk. szabályai alkalmazandók. Marketingcélú későbbi megkereséshez az érintett önkéntes hozzájárulása szükséges; a rendezvényre jelentkezés nem marketing-hozzájárulás.

18. Megfigyelés, beléptetés, GPS és munkáltatói ellenőrzés

18.1. Közös garanciák

Kamera, GPS, beléptetési napló, e-mail-, internet- vagy eszközellenőrzés csak előre meghatározott, valós és dokumentált célból, megfelelő jogalappal, szükségességi és arányossági vizsgálattal, előzetes részletes tájékoztatással, a legkevésbé beavatkozó megoldással és szűk hozzáféréssel alkalmazható. Hozzájárulás munkáltatói vagy vagyonvédelmi megfigyeléshez nem megfelelő jogalap. Titkos vagy folyamatos teljesítménymegfigyelés, öltöző, mosdó, pihenő- és érdekképviseleti helyiség megfigyelése tilos.

18.2. Kamerarendszer

Minden kameráról kameraazonosítót, helyet, látómezőt, célt, jogalapot, érdekmérlegelést, megőrzést, hozzáférőt, maszkot, rögzítési módot és tájékoztató táblát tartalmazó jegyzék készül. A látómező nem terjedhet szükségtelenül közterületre, munkavégzés folyamatos megfigyelésére vagy különleges adatot feltáró területre. Hangrögzítés főszabály szerint tilos. Felvétel megtekintése, mentése, zárolása és kiadása két személyes kontrollal és jegyzőkönyvvel történik.

Felhasználás hiányában a felvétel főszabály szerint 72 órán belül törlendő. Kameránként dokumentált szükségesség esetén legfeljebb 7 nap állapítható meg; ennél hosszabb idő csak kivételes, konkrét kockázattal, DPIA-kontrollal és vezetői jóváhagyással. Az érintett a felülírás előtt kérheti a rá vonatkozó rész megőrzését, pontos hely és idő megadásával. A korábbi tájékoztatókban szereplő egységes 7 nap csak a kameraenkénti felülvizsgálat és szükségesség igazolása után tartható fenn.

18.3. GPS, e-mail, internet és eszköz

GPS csak jármű- és vagyonvédelemhez, munkaszervezéshez vagy dokumentált elszámolási célhoz használható. Magánhasználat engedélyezésekor biztosítani kell a magánút kikapcsolását vagy más hatékony elkülönítését. Részletes mozgásadat legfeljebb 90 napig, lehetőség szerint rövidebb ideig őrizhető. A munkavállaló tartózkodási helyének munkaidőn kívüli folyamatos követése tilos.

E-mail-, internet- és eszközellenőrzésnél előzetesen rögzíteni kell az ellenőrzés célját, körét, módszerét, kiváltó okát, jogosultját és garanciáit. Első lépésként metaadat, forgalmi vagy biztonsági esemény vizsgálandó; tartalom csak akkor, ha a cél másként nem érhető el. A munkavállaló jelenlétét vagy előzetes értesítését biztosítani kell, kivéve, ha ez a vizsgálatot meghiúsítaná; az eltérést indokolni kell. Magánjellegű tartalmat lehetőség szerint olvasás nélkül el kell különíteni. Az ellenőrzésről jegyzőkönyv készül, és jogorvoslati lehetőséget kell biztosítani.

19. Honlap, sütik, közösségi média és nyilvános közzététel

19.1. Honlap és sütik

A www.szfszc.hu tájékoztató weboldal; jelenlegi működésében nincs saját kapcsolatfelvételi, üzenetküldő, regisztrációs, hírlevél-, dokumentumfeltöltő vagy közvetlen jelentkezési felület. A honlap saját keresője nem ügyintézési csatorna. A szerver- és biztonsági napló főszabály szerint legfeljebb 90 napig tartható; személy szerinti látogatói profil nem készíthető.

Nem szükséges analitikai, kényelmi, közösségi vagy marketingcélú süti, helyi tároló, pixel vagy külső követőkérés csak előzetes, célonkénti hozzájárulás után indulhat. Az elutasítás az elfogadással azonosan könnyű, a közérdekű tartalom elérhető marad, a visszavonás állandóan hozzáférhető. A sütijegyzékben tényleges név, szolgáltató, cél, adat, jogalap és élettartam szerepel.

19.2. Közösségi média és külső platform

A Centrum közösségi oldalán végzett moderálás, üzenetkezelés és oldalstatisztika szerepeit platformonként fel kell mérni; a Meta vagy más platform nem minősíthető automatikusan adatfeldolgozónak. Külön kezelendő a Centrum saját tartalma, az érintett nyilvános hozzászólása, a privát megkeresés és a platform által önállóan végzett profilalkotás. Ügyintézési, egészségi, tanügyi vagy más bizalmas adatot közösségi üzenetben nem szabad érdemben kezelni; biztonságos csatornára kell terelni.

Microsoft Forms vagy más külső űrlap csak előzetes folyamat- és beszállítói vizsgálattal, a mezők minimalizálásával, megfelelő tájékoztatóval, hozzáféréssel, export- és törlési renddel használható. A www.szfszc.hu oldalról elérhető külső link nem teszi az űrlapot a honlap részévé, de a Centrum által kezdeményezett űrlapos adatgyűjtésért a Centrum adatkezelői felelőssége fennállhat.

19.3. Képmás, videó, évkönyv és nyilvános adat

Név, portré, videó, eredmény, elérhetőség vagy más személyes adat nyilvánosságra hozatala külön adatkezelési cél, amelyhez önálló jogalap, tájékoztatás és közzétételi idő szükséges. Kötelező közzétételnél csak a jogszabály szerinti adatkör és idő alkalmazható. Egyedi promóciós tartalomnál főszabály szerint hozzájárulás szükséges; annak visszavonása a jövőbeli online felhasználást megszünteti, de a már jogszerűen kiadott nyomtatott példány visszahívása nem mindig lehetséges. Közzétételi felülvizsgálat legalább évente történik; elavult hírt, névsort, portrét és dokumentumot törölni vagy anonimizálni kell, ha további jogalap nincs.

20. Mesterséges intelligencia és automatizált döntéshozatal

Nyilvános vagy jóvá nem hagyott generatív MI-szolgáltatásba személyes, bizalmas, tanulói, munkavállalói, egészségi, vizsga-, szerződéses vagy biztonsági adat nem tölthető fel. MI-rendszer beszerzése vagy használata előtt adat- és modellfolyam, szolgáltatói szerep, tanítási felhasználás, megőrzés, harmadik ország, pontosság, diszkrimináció, emberi felülvizsgálat, információbiztonság, átláthatóság és DPIA-kötelezettség vizsgálandó. Különösen gyermekek, munkavállalók és jelentkezők esetén fokozott kontroll szükséges.

A Centrum felvételről, értékelésről, fegyelmi ügyről, foglalkoztatásról, ösztöndíjról vagy más jelentős kérdésről nem hozhat kizárólag automatizált, joghatással vagy hasonlóan jelentős hatással járó döntést,

kivéve a GDPR 22. cikkében megengedett, előzetesen jogilag és műszakilag jóváhagyott esetet. Ilyenkor is biztosítani kell az érdemi emberi beavatkozást, az álláspont kifejtését és a döntés vitatását. Érzelemfelismerés, rejtett viselkedési pontozás vagy gyermekek reklámprofilozása nem engedélyezett.

21. Oktatás, ellenőrzés, audit és vezetői felülvizsgálat

21.1. Oktatás

Személyes adathoz hozzáférés csak adatvédelmi és információbiztonsági oktatás után adható. Belépéskor, majd évente ismétlődő oktatás szükséges. Az oktatás tartalmát, időpontját, résztvevőjét, teljesítését és tudásellenőrzését dokumentálni kell. Az aláírás önmagában nem bizonyít megfelelő tudást; kockázatos hiányosságnál ismételt képzés szükséges.

21.2. Ellenőrzési program

- negyedévente: kiemelt jogosultságok, incidensintézkedések, lejárt hozzájárulások és közzétételi panaszok;
- félévente: adatfeldolgozói változások, webes sütik és külső kérések, kamerajegyzék, űrlapok, megosztások és nyilvános dokumentumok;
- évente: mind az 56 nyilvántartott folyamat folyamatgazdai igazolása, megőrzési és törlési próba, tájékoztatók, LIA/DPIA, harmadik ország, oktatás és szerződéses megfelelés;
- kockázat vagy esemény alapján: célzott audit incidens, panasz, új rendszer, szervezeti változás, hatósági döntés vagy ismétlődő hiba után.

Az adatvédelmi tisztviselő kockázatalapú éves ellenőrzési tervet és éves beszámolót készít. Az ellenőrzési megállapításhoz súlyosság, felelős, határidő és utóellenőrzés tartozik. Kritikus hiányosságnál az adatkezelés vagy rendszer használata ideiglenesen felfüggeszthető a kockázat csökkentéséig. A vezetés évente áttekinti legalább az incidenseket, kérelmeket, panaszokat, DPIA-kat, nyitott intézkedéseket, szolgáltatói kockázatokat, oktatási teljesítést és erőforrásigényt.

22. Iratkezelés, titoktartás és a szabályzat megsértésének következményei

Az adatvédelmi dokumentumokat verziószámmal, tulajdonossal, jóváhagyóval, hatálybalépéssel és felülvizsgálati dátummal kell kezelni. A korábbi verziót változatlanul meg kell őrizni az elszámoltathatóság és a korábbi adatkezelés bizonyíthatósága érdekében. A nyilvános tájékoztató és a belső szabályzat nem helyettesíti egymást; az előbbi az érintettnek szól, az utóbbi a végrehajtást rendeli el.

A személyes adatot kezelő személy titoktartási kötelezettsége a jogviszony megszűnése után is fennmarad. A szabályzat vétkes megszegése munkajogi, megbízási, kártérítési, fegyelmi, szabálysértési vagy büntetőjogi következményt vonhat maga után. A következmény arányos, dokumentált és tisztességes eljárásban állapítható meg. Jóhiszemű incidens- vagy hiányosságbejelentés miatt hátrány nem alkalmazható.

23. Átmeneti és záró rendelkezések

A szabályzat hatálybalépésétől számított 60 napon belül valamennyi folyamatgazda köteles a rá vonatkozó adatkezelési bejegyzést, tájékoztatót, szerződést, hozzáférést és megőrzési beállítást felülvizsgálni. A kritikus eltérést azonnal, a magas kockázatút 30 napon belül, az egyéb eltérést legfeljebb 90 napon belül rendezni kell. Az adatvédelmi tisztviselő a végrehajtásról összefoglaló jelentést készít a vezetés részére.

Kiemelt induló intézkedés: a kamerák tényleges megőrzését és látómezejét kameraenként össze kell vetni a tájékoztatókkal; a www.szfszc.hu mérési azonosító nélküli Google-hivatkozását el kell távolítani; az adatfeldolgozók és önálló adatkezelők szerepét szerződésenként ellenőrizni kell; a nyilvántartás kérdőjeles, feltételes vagy nem pontosított bejegyzéseit konkrét adattal kell lezárni; továbbá a korábbi tájékoztatók és a jelen szabályzat megőrzési határidejeit egységesíteni kell.

A szabályzat mellékletei a szabályzat részét képezik. A nyilvántartás, a szolgáltatói jegyzék, a rendszerleltár, a kamerajegyzék és a tájékoztatók ellenőrzött kapcsolódó dokumentumok; ezek operatív

módosítása a dokumentumkezelési rendben kijelölt jóváhagyással történik, és nem eredményezheti a szabályzat alapvető garanciáinak csökkentését.

A. MELLÉKLET
ÚJ VAGY MEGVÁLTOZÓ ADATKEZELÉS KONTROLLLAPJA

Kérelem azonosítója:

Folyamatgazda / szervezeti egység:

Tervezett indulás és változás oka:

Adatkezelési cél:

Érintettek és adatkategóriák:

Adatforrás és kötelező/önkéntes jelleg:

Jogalap; különleges/bűnügyi adat feltétele:

Rendszer, tárolási hely, hozzáférők:

Címzettek, adatfeldolgozók, al-adatfeldolgozók:

Megőrzés, törlési esemény és felelős:

EGT-n kívüli adattovábbítás és garancia:

Tájékoztató / hozzájárulás / LIA / DPIA hivatkozása:

Kontroll	Eredmény	Név, dátum, aláírás
Folyamatgazdai szükségesség és adatminimalizálás	☐ megfelelő ☐ javítandó ☐ elutasítva	
IT-biztonsági és törlési ellenőrzés	☐ megfelelő ☐ javítandó ☐ elutasítva	
Beszerzési / szerződéses ellenőrzés	☐ megfelelő ☐ javítandó ☐ nem alkalmazandó	
DPO-vélemény; LIA/DPIA szükségesség	☐ megfelelő ☐ feltételes ☐ DPIA ☐ elutasítva	
Vezetői döntés	☐ jóváhagyva ☐ feltétellel ☐ elutasítva	

B. MELLÉKLET
ÉRDEKMÉRLEGELÉSI TESZT – KÖTELEZŐ TARTALOM

1. Az adatkezelés pontos célja és az érvényesíteni kívánt jogszerű, valós és konkrét érdek.
2. Annak igazolása, hogy a Centrum az adott műveletnél nem közfeladatának végrehajtása során jár el, ezért a GDPR 6. cikk (1) f) alkalmazható.
3. A szükségesség: miért alkalmas az adatkezelés a célra, és miért nincs ugyanolyan hatékony, kevésbé beavatkozó alternatíva.
4. Az érintetti hatás: adatok jellege, mennyisége, forrása, megőrzése, címzettje, nyilvánosság, kiszolgáltatottság, gyermekek, észszerű elvárás és lehetséges kár.
5. Az érdekek és jogok mérlege; külön a magánszféra, autonómia, egyenlő bánásmód, véleménynyilvánítás és jogorvoslat.
6. Garanciák: adatminimalizálás, rövid megőrzés, hozzáférés, átláthatóság, tiltakozás, alternatíva, álnevesítés, audit.
7. Következtetés, fennmaradó kockázat, vezetői jóváhagyás, DPO-vélemény és következő felülvizsgálat.

Adatkezelési folyamat és azonosító:

Következtetés és feltételek:

Folyamatgazda / dátum / aláírás:

DPO-vélemény / dátum:

Vezetői döntés / dátum / aláírás:

C. MELLÉKLET
DPIA-ELŐSZŰRŐ ÉS HATÁSVIZSGÁLATI DÖNTÉS

Jelölje, fennáll-e az alábbi kockázati tényező. Két vagy több tényező rendszerint DPIA szükségességét jelzi; a NAIH kötelező jegyzékében szereplő műveletnél a DPIA a tényezők számától függetlenül kötelező.

Kockázati tényező	Igen / Nem	Indok és garancia
Rendszeres és módszeres értékelés vagy profilalkotás	☐ Igen ☐ Nem	
Automatizált jelentős döntés	☐ Igen ☐ Nem	
Módszeres megfigyelés, kamera, helyadat vagy online követés	☐ Igen ☐ Nem	
Különleges vagy bűnügyi adat nagy számban	☐ Igen ☐ Nem	
Nagy számú érintett vagy nagy adatmennyiség	☐ Igen ☐ Nem	
Adatállományok összekapcsolása vagy összevetése	☐ Igen ☐ Nem	
Gyermek, munkavállaló vagy más kiszolgáltatott érintett	☐ Igen ☐ Nem	
Új vagy innovatív technológia, biometria vagy MI	☐ Igen ☐ Nem	
Az érintett joggyakorlását vagy szolgáltatáshoz jutását akadályozó hatás	☐ Igen ☐ Nem	
NAIH kötelező hatásvizsgálati jegyzéke szerinti művelet	☐ Igen ☐ Nem	

Döntés: DPIA szükséges / nem szükséges és indok:

DPO-vélemény:

Döntéshozó / dátum / aláírás:

D. MELLÉKLET
ÉRINTETTI KÉRELMEK NYILVÁNTARTÁSA ÉS ELLENŐRZŐ LISTÁJA

Rögzítendő adat	Tartalom
Ügyazonosító; beérkezés és csatorna	
Kérelmező; érintetti minőség; arányos azonosítás	
Kérelem típusa és pontos tartalma	☐ hozzáférés ☐ helyesbítés ☐ törlés ☐ korlátozás ☐ tiltakozás ☐ hordozhatóság ☐ egyéb
Érintett folyamatok, rendszerek, címzettek	
Folyamatgazdák és részválasz-határidő	
Egy hónapos végső határidő; hosszabbítás indoka és közlése	
Harmadik személy jogainak védelme / kitakarás	
Döntés, végrehajtás, címzettek értesítése	
Válasz dátuma, módja, kézbesítés igazolása	
Lezárás, jogorvoslat, 5 éves törlési dátum	

E. MELLÉKLET
TÖRLÉSI, ANONIMIZÁLÁSI ÉS SELEJTEZÉSI JEGYZŐKÖNYV

Jegyzőkönyv azonosítója és dátuma:

Folyamat / rendszer / irattári tétel:

Érintetti és adatkategória:

Törlési idő bekövetkezésének oka és jogalapja:

Érintett időszak, rekord- vagy iratmennyiség:

Művelet: törlés / anonimizálás / iratmegsemmisítés / levéltári átadás:

Végrehajtás módja és eredménye:

Mentések és visszaállításkori újratörlés kezelése:

Kivételek / zárolt tételek és felülvizsgálatuk:

Végrehajtó és ellenőrző neve, aláírása:

F. MELLÉKLET
ADATVÉDELMI INCIDENS BEJELENTŐ- ÉS DÖNTÉSI LAP

Incidensazonosító:

Bejelentő, észlelés és tudomásszerzés pontos időpontja:

Mi történt, hol és mely rendszerben:

Érintettek köre és becsült száma:

Adatok kategóriája, érzékenysége és becsült mennyisége:

Bizalmasság / sértetlenség / rendelkezésre állás sérülése:

Azonnali kárenyhítő és bizonyítékmegőrző intézkedések:

Valószínű következmények és kockázati minősítés:

Döntési kérdés	**Igen / Nem / időpont**	**Indok / jóváhagyás**
NAIH-bejelentés szükséges?		
72 órás határidő tartható?		
Érintetti tájékoztatás szükséges?		
Más hatóság / szerződéses partner értesítendő?		
Szakaszos bejelentés szükséges?		

Gyökérok, helyesbítő és megelőző intézkedések:

DPO-vélemény; vezetői döntés; lezárás dátuma:

G. MELLÉKLET
ADATFELDOLGOZÓI / SZOLGÁLTATÓI ÁTVILÁGÍTÁSI LAP

Vizsgálati pont	Megfelel / eltérés	Bizonyíték / intézkedés
Szerep: adatfeldolgozó, önálló vagy közös adatkezelő		
Adat, érintett, cél, időtartam és utasítás pontos leírása		
Biztonsági intézkedések, titkosítás, hitelesítés, naplózás		
Incidensértesítés ideje és tartalma		
Érintetti kérelem, audit és DPIA támogatása		
Al-adatfeldolgozók és változáskezelés		
Adatkezelési helyek és EGT-n kívüli hozzáférés		
SCC / megfelelőségi határozat / TIA / kiegészítő garancia		
Megőrzés, mentés, visszaszolgáltatás és igazolt törlés		
Üzletmenet-folytonosság, kilépési és adathordozhatósági terv		
Adatfeldolgozói szerződés GDPR 28. cikk szerinti teljessége		
Kockázat, feltételek, jóváhagyás és következő felülvizsgálat		

H. MELLÉKLET
A NYILVÁNTARTOTT ADATKEZELÉSEK KONTROLLTÉRKÉPE

A Centrum 56 tételes adatkezelési folyamatnyilvántartását az alábbi kontrollcsaládok szerint kell évente felülvizsgálni. A felsorolás nem helyettesíti a tételes GDPR 30. cikk szerinti nyilvántartást.

Kontrollcsalád	Nyilvántartási tételek	Kiemelt ellenőrzés
Pénzügy, adó, kifizetés	1, 16–18, 28, 30–31, 41, 55–56	8 éves bizonylat; többletmásolat; MÁK/NAV/SAP szerep.
Partner és szerződés	2–3, 23, 31, 37–38, 41, 53	Kapcsolattartói jogalap; EV-adatkör; irattári és igényidő.
Munkavállaló és HR	4–10, 13, 16–21, 24, 29–35, 39, 42, 52, 54	Különleges adat; 5/8 éves és irattári idők; ellenőrzési LIA.
Álláspályázó	11–12	3 hónap; 12 hónapos; önkéntes hozzájárulás megléte; tiltott interjúadat.
Tanuló és felnőttképzés	14–15, 27–28, 40, 43–45	10/8 év; maradandó irat; SNI/BTMN; külső képzőhely szerepe.
Honlap, süti és közösségi média	22, 47	Tételes sütilista; külső kód; platformszerep; üzenetátterelés.
Képmás, rendezvény, marketing	25, 36–37, 48	Egyedi portré hozzájárulása; tömegfelvétel; az érintett önkéntes hozzájárulása
Megfigyelés és fizikai biztonság	26, 29, 46	Kameraenkénti idő és látómező; GPS magánidő; vendégnapló max. 6 hó.
Munkavédelem és egészség	19, 24, 39, 42–44	Szolgáltató önálló szerepe; alkalmasság ténye; irattári tétel.
Pályázat, jogvita, levéltár	6, 38, 49, 53	Támogatási idő; releváns bizonyíték; maradandó irat.
Adatvédelmi irányítás	50–51, 54	5 éves incidens/kérelem; 72 óra; hozzáférési napló 6–12 hó.