NYÍRZEM NYÍRSÉG-ZEMPLÉN COOP
KERESKEDELMI ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

4600 Kisvárda, Szent László út 38.

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Verzió: 2026/1

Felülvizsgálat dátuma: 2026. augusztus 27.

Hatálybalépés: a jóváhagyás napján

Jóváhagyta: SAJTOSNÉ PÉKÓ NORA

Beosztás: IGAZGATÓ

Jóváhagyás dátuma: 2026. 08. 27.

A szabályzat a társaság belső adatvédelmi és adatbiztonsági rendjét határozza meg. Az egyes érintetti körökre és adatkezelésekre vonatkozó részletes, GDPR 13–14. cikk szerinti tájékoztatókat külön dokumentumban kell kiadni.

Sajtosné Pékó Nóra

NYÍRZEM
Nyírség-Zemplén Coop
Kereskedelmi Zrt.
4600 Kisvárda, Szent L. u. 38.
Adószám:11827218-2-15
K&H: 10404436-44812633

Dokumentumkezelési adatok

Adatkezelő	NYÍRZEM Nyírség-Zemplén COOP Kereskedelmi Zrt. (Nyírzem Zrt.)
Székhely	4600 Kisvárda, Szent László út 38.
Cégjegyzékszám	15-10-040266
Adószám	11827218-2-15
Adatvédelmi kapcsolattartás	bejelentes@nyirzem.hu • +36 45 420 179
Felülvizsgálat	Legalább évente, továbbá lényeges jogszabály-, szervezeti, technológiai vagy adatkezelési változás esetén.

1. A szabályzat célja és jogi háttere

1.1. A szabályzat célja, hogy a Nyírzem Zrt. személyesadat-kezelési tevékenységei egységes, dokumentált és ellenőrizhető rendben, az elszámoltathatóság elvének megfelelően történjenek; meghatározza a felelősségi köröket, az érintetti jogok kezelésének, az adatvédelmi incidensek kezelésének, az adatfeldolgozók igénybevételének és az adatbiztonsági intézkedéseknek a minimumkövetelményeit.

1.2. A szabályzat elsődleges jogi alapja az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR), valamint – a mindenkor hatályos rendelkezései szerint – a 2011. évi CXII. törvény (Infotv.). A munkaviszonnyal összefüggő adatkezelések során irányadó különösen a 2012. évi I. törvény (Munka Törvénykönyve), a számviteli és bizonylatmegőrzési kötelezettségeknél a 2000. évi C. törvény, közvetlen üzletszerzésnél pedig a 2008. évi XLVIII. törvény.

1.3. A szabályzatot a mindenkor hatályos jogszabályokkal, az Európai Adatvédelmi Testület (EDPB) iránymutatásaival, valamint a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) közzétett állásfoglalásaival és gyakorlatával összhangban kell alkalmazni.

1.4. Jogszabályváltozás esetén a magasabb szintű és közvetlenül alkalmazandó jogszabály rendelkezése elsőbbséget élvez. A szabályzat jogszabállyal ellentétes része nem alkalmazható; az eltérést haladéktalanul felül kell vizsgálni.

2. Személyi és tárgyi hatály

2.1. A szabályzat kiterjed a társaság valamennyi szervezeti egységére, munkavállalójára, vezető tisztségviselőjére, megbízottjára, továbbá mindazon személyre, aki a társaság utasítása alapján személyes adathoz hozzáfér.

2.2. Tárgyi hatálya kiterjed minden, részben vagy egészben automatizált módon végzett személyesadat-kezelésre, valamint a nem automatizált módon kezelt, nyilvántartási rendszer részét képező vagy azzá tenni kívánt személyes adatokra.

2.3. A szabályzat irányadó különösen a munkavállalói, álláspályázói, vevői, beszállítói és üzleti kapcsolattartói, panaszügyi, kamerás, beléptetési, marketing-, informatikai és jogérvényesítési adatkezelésekre, amennyiben a társaság ilyen adatkezelést ténylegesen végez.

3. Alapfogalmak

Személyes adat: azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.

Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége.

Adatkezelő: aki a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.

Adatfeldolgozó: aki az adatkezelő nevében személyes adatokat kezel.

Címzett: akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e.

Hozzájárulás: az érintett önkéntes, konkrét, megfelelő tájékoztatáson alapuló és egyértelmű akaratnyilvánítása.

Különleges adat: a GDPR 9. cikk (1) bekezdésében meghatározott különleges személyesadat-kategória.

Adatvédelmi incidens: a biztonság olyan sérülése, amely személyes adatok véletlen vagy jogellenes megsemmisítéséhez, elvesztéséhez, megváltoztatásához, jogosulatlan közléséhez vagy az azokhoz való jogosulatlan hozzáféréshez vezet.

Álnevesítés: olyan adatkezelés, amelynek eredményeként további információ felhasználása nélkül az adat már nem kapcsolható meghatározott érintetthez, feltéve, hogy a további információt elkülönítve kezelik.

4. Az adatkezelés alapelvei

- Jogszerűség, tisztességes eljárás és átláthatóság: személyes adat csak megfelelő jogalappal, tisztességesen és az érintett számára érthető módon kezelhető.
- Célhoz kötöttség: adat csak előre meghatározott, egyértelmű és jogszerű célból gyűjthető; azzal össze nem egyeztethető további felhasználás nem megengedett.
- Adattakarékosság: csak a cél eléréséhez megfelelő, releváns és szükséges adat kezelhető.
- Pontosság: észszerű intézkedésekkel biztosítani kell a pontatlan adatok helyesbítését vagy törlését.
- Korlátozott tárolhatóság: személyes adat az azonosíthatóságot lehetővé tevő formában csak a szükséges ideig őrizhető meg.
- Integritás és bizalmas jelleg: megfelelő technikai és szervezési intézkedésekkel kell védeni az adatokat.
- Elszámoltathatóság: a társaságnak képesnek kell lennie a megfelelés igazolására, különösen nyilvántartásokkal, döntési dokumentumokkal és ellenőrizhető eljárásokkal.

5. Adatkezelési jogalapok és azok megválasztása

5.1. Minden adatkezelési célhoz külön meg kell határozni az alkalmazandó jogalapot. A hozzájárulás nem tekinthető általános vagy alapértelmezett jogalapnak.

Jogalap	Tipikus alkalmazás	Követelmény
GDPR 6. cikk (1) a) – hozzájárulás	pl. opcionális marketing, ha más jogalap nem megfelelő	önkéntes, konkrét, tájékozott, egyértelmű; bizonyítható; ugyanolyan könnyen visszavonható
GDPR 6. cikk (1) b) – szerződés	szerződés megkötéséhez vagy teljesítéséhez objektíven szükséges adatkezelés	nem terjeszthető ki kényelmi vagy más célokra
GDPR 6. cikk (1) c) – jogi kötelezettség	adó-, számviteli-, munkaügyi és más kötelező nyilvántartások	a konkrét jogszabályi kötelezettséget dokumentálni kell
GDPR 6. cikk (1) f) – jogos érdek	pl. vagyonvédelem, egyes üzleti kapcsolattartási vagy igényérvényesítési célok	előzetes érdekmérlegelés, szükségesség és arányosság dokumentálása; tiltakozási jog biztosítása
GDPR 6. cikk (1) d/e)	csak ha az adott adatkezelés	jogi és ténybeli feltételeket külön

	ténylegesen e körbe esik	ellenőrizni kell

5.2. Különleges személyes adat csak a GDPR 9. cikk (2) bekezdésében meghatározott valamely kivétel fennállása mellett kezelhető. A 9. cikk szerinti feltétel nem helyettesíti a 6. cikk szerinti jogalap vizsgálatát.

5.3. Bűnügyi személyes adatok kezelése kizárólag megfelelő uniós vagy tagállami jogi felhatalmazás és garanciák mellett végezhető. Munkaviszonyban a Munka Törvénykönyve külön feltételeit is alkalmazni kell.

6. Beépített és alapértelmezett adatvédelem

6.1. Új rendszer, folyamat, szolgáltatás vagy adatkezelési cél bevezetésekor már a tervezési szakaszban vizsgálni kell a GDPR-követelményeket.

- csak a szükséges adatmezők legyenek kötelezők;
- az alapértelmezett hozzáférés a feladatellátáshoz szükséges legszűkebb körre terjedjen ki;
- megőrzési idők és törlési folyamatok már a rendszer kialakításakor legyenek meghatározva;
- ahol ésszerűen lehetséges, álnevesítést, titkosítást és naplózást kell alkalmazni;
- új technológia vagy magas kockázat esetén adatvédelmi hatásvizsgálat szükségességét értékelni kell.

7. Adatkezelési tevékenységek nyilvántartása

7.1. A társaság a GDPR 30. cikkével összhangban adatkezelési nyilvántartást vezet az alkalmazandó körben. A nyilvántartásnak naprakészen tartalmaznia kell legalább az adatkezelési célokat, az érintetti és adatkategóriákat, címzetteket, harmadik országbeli adattovábbításokat, törlési határidőket és a technikai-szervezési intézkedések általános leírását.

7.2. Új adatkezelés nem indítható a cél, jogalap, adatkör, érintetti kör, megőrzési idő, címzettek/adatfeldolgozók, érintetti tájékoztatás és biztonsági intézkedések dokumentálása nélkül.

8. Érintetti tájékoztatás

8.1. Ha a személyes adatot közvetlenül az érintettől gyűjtik, a GDPR 13. cikk szerinti, ha más forrásból származik, a GDPR 14. cikk szerinti tájékoztatást kell biztosítani a rendeletben meghatározott időpontban és tartalommal.

8.2. A tájékoztató legyen tömör, átlátható, közérthető és könnyen hozzáférhető. Nem elegendő pusztán e belső szabályzatra hivatkozni.

8.3. A tájékoztatókban az adatkezelési célokat és jogalapokat tételesen, célonként kell feltüntetni. Jogos érdek esetén meg kell nevezni a jogos érdeket; adattovábbításnál a címzetteket vagy címzetti kategóriákat; a megőrzési időt pedig konkrétan vagy objektív szempontokkal kell megadni.

9. Az érintetti jogok gyakorlása

9.1. Az érintett kérelmezheti a hozzáférést, helyesbítést, törlést, az adatkezelés korlátozását, illetve az alkalmazandó feltételek mellett az adathordozhatóságot; jogos érdeken vagy közérdekű feladaton alapuló adatkezelés ellen tiltakozhat; hozzájárulását bármikor visszavonhatja a visszavonást megelőző adatkezelés jogszerűségének sérelme nélkül.

9.2. Az érintetti kérelmet indokolatlan késedelem nélkül, de főszabály szerint legkésőbb a beérkezéstől számított egy hónapon belül meg kell válaszolni. A határidő a GDPR feltételei mellett további két hónappal meghosszabbítható; erről és az okokról az érintettet az első hónapon belül tájékoztatni kell.

9.3. A kérelmek teljesítése főszabály szerint díjmentes. Nyilvánvalóan megalapozatlan vagy – különösen ismétlődő jellegük miatt – túlzó kérelmek esetén a GDPR 12. cikk (5) bekezdésének feltételei alkalmazhatók.

9.4. Ha kétség merül fel a kérelmező személyazonosságával kapcsolatban, kizárólag az azonosításhoz szükséges további információ kérhető.

9.5. A kérelmet, az elvégzett azonosítást, a döntést, a teljesítés módját és időpontját dokumentálni kell.

10. Automatizált döntéshozatal és profilalkotás

10.1. Kizárólag automatizált adatkezelésen alapuló, az érintettre nézve joghatással járó vagy őt hasonlóképpen jelentős mértékben érintő döntés csak a GDPR 22. cikkében meghatározott feltételek mellett alkalmazható.

10.2. Ha a társaság ilyen rendszert kíván bevezetni, annak megkezdése előtt külön jogi, adatvédelmi és technikai felülvizsgálat szükséges, és indokolt esetben adatvédelmi hatásvizsgálatot kell végezni.

11. Adatfeldolgozók és közös adatkezelés

11.1. Adatfeldolgozó csak megfelelő garanciákat nyújtó szolgáltató lehet. Az igénybevétel előtt értékelni kell legalább a szolgáltató biztonsági, titoktartási, al-adatfeldolgozói és incidenskezelési képességeit.

11.2. Az adatfeldolgozóval írásbeli, a GDPR 28. cikk (3) bekezdésének megfelelő szerződést kell kötni. A szerződésnek ki kell térnie többek között az utasítás szerinti adatkezelésre, titoktartásra, biztonságra, al-adatfeldolgozókra, érintetti jogok támogatására, incidensekre, törlésre/visszaadásra és ellenőrizhetőségre.

11.3. Ha két vagy több fél közösen határozza meg az adatkezelés céljait és eszközeit, a GDPR 26. cikk szerinti közös adatkezelői megállapodást kell kötni.

11.4. Az adatfeldolgozók aktuális jegyzékét külön nyilvántartásban kell vezetni. A korábbi szabályzatban szereplő, saját társaság adatfeldolgozóként való feltüntetése nem alkalmazható.

12. Harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás

12.1. Az Európai Gazdasági Térségen kívülre történő adattovábbítás előtt meg kell vizsgálni a GDPR V. fejezetének feltételeit, ideértve a megfelelőségi határozatot, megfelelő garanciákat vagy kivételes jogalapot.

12.2. Standard szerződéses kikötések alkalmazása esetén szükség szerint adattovábbítási hatásvizsgálatot és kiegészítő intézkedéseket kell dokumentálni. Felhő- és SaaS-szolgáltatás igénybevétele előtt az adattárolás és támogatási hozzáférések földrajzi helyét is tisztázni kell.

13. Adatbiztonsági követelmények

13.1. A társaság a kockázattal arányos technikai és szervezési intézkedéseket alkalmaz. A biztonsági szint meghatározásakor figyelembe kell venni a technika állását, a megvalósítás költségeit, az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a természetes személyek jogaira jelentett kockázatokat.

- szerepköralapú, legkisebb jogosultság elvén működő hozzáférés-kezelés;
- egyedi felhasználói azonosítók; megosztott fiókok kerülése;
- erős hitelesítés és ahol indokolt, többtényezős hitelesítés;
- naprakész végpontvédelem, biztonsági frissítések és sebezhetőség-kezelés;

- titkosított adatátvitel; hordozható eszközök és érzékeny adatállományok megfelelő védelme;
- rendszeres, ellenőrzött biztonsági mentés és visszaállítási próba;
- hozzáférések rendszeres felülvizsgálata és a megszűnt jogviszonyhoz kapcsolódó jogosultságok haladéktalan visszavonása;
- naplózás az indokolt rendszereknél; a naplókhoz való hozzáférés korlátozása;
- papíralapú iratok zárható tárolása, biztonságos selejtezése;
- személyes adatot tartalmazó e-mail és fájl megosztásakor a címzettek, mellékletek és jogosultságok ellenőrzése;
- rendszeres adatvédelmi és információbiztonsági oktatás.

14. Adatvédelmi incidensek kezelése

14.1. Minden munkatárs köteles a feltételezett adatvédelmi incidenst haladéktalanul, lehetőleg észlelést követően azonnal jelenteni a kijelölt belső kapcsolattartónak. A bejelentés késedelme nem megengedett azért, mert még nem ismert minden részlet.

14.2. A társaság minden incidenst nyilvántart és értékel. A nyilvántartás tartalmazza az incidens tényét, körülményeit, érintett adatok és személyek körét, következményeit, kockázatértékelését, megtett intézkedéseket és a bejelentési döntés indokait.

14.3. Ha az incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira, a felügyeleti hatóságnak indokolatlan késedelem nélkül és – ha lehetséges – legkésőbb a tudomásszerzéstől számított 72 órán belül be kell jelenteni. Ha a kockázat várhatóan magas, az érintetteket is indokolatlan késedelem nélkül tájékoztatni kell, kivéve a GDPR 34. cikkében meghatározott eseteket.

14.4. Adatfeldolgozóval kötött szerződésben elő kell írni, hogy az adatfeldolgozó a tudomására jutott incidenst indokolatlan késedelem nélkül jelenti a társaságnak.

14.5. A NAIH aktuális incidensbejelentő rendszerének és elérhetőségeinek használatáról az incidens kezelésekor a Hatóság honlapján közzétett mindenkori tájékoztatás alapján kell eljárni.

15. Adatvédelmi hatásvizsgálat (DPIA) és előzetes konzultáció

15.1. Ha valamely adatkezelés – különösen új technológia alkalmazásával, jellegére, hatókörére, körülményeire és céljaira tekintettel – valószínűsíthetően magas kockázattal jár, a megkezdése előtt adatvédelmi hatásvizsgálatot kell végezni.

15.2. DPIA szükségességét különösen nagymértékű megfigyelés, különleges adatok kiterjedt kezelése, módszeres értékelés/profilalkotás, új technológiák vagy sérülékeny érintetti csoportok esetén kell vizsgálni, figyelembe véve a NAIH és az EDPB aktuális listáit és iránymutatásait.

15.3. Ha a hatásvizsgálat szerint a magas kockázat megfelelő intézkedésekkel sem mérsékelhető, az adatkezelés megkezdése előtt a GDPR 36. cikke szerinti előzetes konzultációt kell kezdeményezni.

16. Adatvédelmi tisztviselő

16.1. A társaság rendszeresen felülvizsgálja, fennáll-e a GDPR 37. cikke szerinti kötelező adatvédelmi tisztviselő-kijelölési eset. Amennyiben igen, a tisztviselőt megfelelő szakértelemmel, független feladatellátással és közvetlen felső vezetői beszámolási lehetőséggel kell kijelölni.

16.2. Ha adatvédelmi tisztviselő kijelölésére kerül sor, elérhetőségét közzé kell tenni és a NAIH részére be kell jelenteni a mindenkori előírások szerint. Az adatvédelmi tisztviselő nem kaphat olyan feladatot, amely összeférhetetlenséget eredményez.

16.3. Ha a kijelölés nem kötelező és a társaság nem jelöl ki GDPR szerinti adatvédelmi tisztviselőt, belső adatvédelmi kapcsolattartó kijelölhető; e személyt azonban nem szabad megtévesztően „adatvédelmi tisztviselőként" feltüntetni.

17. Munkavállalói és HR-adatkezelések

17.1. A munkáltató csak a munkaviszony létesítése, teljesítése, megszűnése, megszüntetése vagy munkaviszonyból eredő igény érvényesítése szempontjából lényeges személyes adatot kérhet, illetve kezelhet, továbbá teljesítheti a rá irányadó jogi kötelezettségeket.

17.2. A munkavállalókat a munkáltatói adatkezelésekről előzetesen, írásban és a GDPR 13–14. cikke szerinti tartalommal tájékoztatni kell. Munkaviszonyban a hozzájárulás önkéntességét a függőségi helyzet miatt különösen körültekintően kell értékelni.

17.3. Alkalmassági vizsgálat, biometrikus adat, bűnügyi személyes adat vagy technikai ellenőrzés kizárólag a Munka Törvénykönyvében és más alkalmazandó jogszabályokban meghatározott feltételekkel alkalmazható.

17.4. A munkavállaló munkaviszonnyal összefüggő magatartása ellenőrizhető, és technikai eszköz is alkalmazható, de az ellenőrzésnek szükségesnek, arányosnak, célhoz kötöttnek kell lennie; az alkalmazott eszközről és az ellenőrzés lényeges körülményeiről előzetesen írásban tájékoztatni kell.

17.5. A munkavégzéshez biztosított számítástechnikai eszközök használatára külön informatikai/eszközhasználati szabályzat adható ki. Az ellenőrzés során a magánjellegű tartalom megismerését a jogszabályi keretek között kerülni kell.

18. Elektronikus megfigyelés és kamerarendszer

18.1. Kamerás megfigyelés csak konkrét, dokumentált és jogszerű célból működtethető. Jogos érdeken alapuló kamerázás előtt érdekmérlegelési tesztet kell készíteni, és meg kell vizsgálni, hogy a cél kevésbé beavatkozó eszközzel elérhető-e.

18.2. A kamerák látószögét úgy kell beállítani, hogy szükségtelen területet – különösen olyan helyet, ahol az érintett magánszférája kiemelten védendő – ne figyeljenek. Munkavállaló folyamatos munkavégzésének megfigyelése főszabályként nem lehet önálló cél.

18.3. A megőrzési időt kameránként vagy célonként szükségességi alapon kell meghatározni és dokumentálni. Nem alkalmazható automatikusan egy korábbi jogszabályból vagy mintából átvett általános megőrzési idő.

18.4. A megfigyelt területre belépés előtt jól látható első szintű tájékoztatást kell elhelyezni, és könnyen hozzáférhetővé kell tenni a részletes kamerás adatkezelési tájékoztatót.

18.5. A felvételek megtekintésére, kimentésére és továbbítására jogosult személyek körét szűken, írásban kell meghatározni; hozzáféréseket és kimentéseket indokolt esetben naplózni kell.

19. Közvetlen üzletszerzés és elektronikus marketing

19.1. Természetes személy részére közvetlen üzletszerzési célú elektronikus üzenet főszabály szerint csak előzetes, egyértelmű és kifejezett hozzájárulással küldhető, kivéve, ha alkalmazandó jogszabály kifejezett kivételt állapít meg.

19.2. A hozzájárulás megszerzését, tartalmát és időpontját bizonyíthatóan dokumentálni kell. A leiratkozásnak egyszerűnek és díjmentesnek kell lennie; visszavonás után marketingcélú küldés nem folytatható.

19.3. A marketingcélú adatbázis nem használható más, össze nem egyeztethető célra megfelelő jogalap és tájékoztatás nélkül.

20. Megőrzési idők és törlés

20.1. Minden adatkezeléshez dokumentált megőrzési időt vagy objektív törlési feltételt kell rendelni. A „törlési kérelemig" megfogalmazás önmagában nem megfelelő olyan adatkezelésnél, amelyhez jogszabályi megőrzés vagy más, előre meghatározható időtartam kapcsolódik.

20.2. Jogszabályban előírt megőrzési időt a jogszabály szerint kell alkalmazni. Például a számviteli bizonylatok és azok alátámasztására szolgáló iratok megőrzésénél a számviteli törvény mindenkori rendelkezései irányadók.

20.3. A törlés történhet fizikai megsemmisítéssel, biztonságos elektronikus törléssel vagy visszafordíthatatlan anonimizálással. A puszta hozzáférés-megvonás nem minden esetben azonos a törléssel.

20.4. Ha törlés helyett jogi igény, jogi kötelezettség vagy más jogszerű ok miatt korlátozás szükséges, az adatot elkülönítetten és a célhoz szükséges körben kell megőrizni.

21. Papíralapú iratok és fizikai biztonság

- Személyes adatot tartalmazó iratot nyitott, felügyelet nélküli helyen hagyni nem szabad.
- Az irattárak, személyzeti és pénzügyi iratok hozzáférését szerepkör szerint korlátozni kell.
- A selejtezésnek oly módon kell történnie, hogy a személyes adat ne legyen helyreállítható.
- Iratok külső helyre vitele csak üzleti szükséglet esetén, megfelelő védelmi intézkedéssel megengedett.
- Nyomtatók és közös másolóeszközök tálcáján személyes adatot tartalmazó dokumentum nem maradhat.

22. Adattovábbítás hatóságoknak és harmadik személyeknek

22.1. Hatósági vagy más külső adatkérés esetén a megkeresés jogalapját, címzettjét, terjedelmét és hitelességét ellenőrizni kell. Csak a jogszerűen és szükséges körben kért adat továbbítható.

22.2. Az adattovábbítást – ha jogszabály nem tiltja – oly módon kell dokumentálni, hogy utólag megállapítható legyen a továbbítás címzettje, jogalapja, célja, időpontja és adatköre.

23. Titoktartás, oktatás és munkatársi felelősség

23.1. Személyes adathoz csak az férhet hozzá, akinek arra feladata ellátásához szüksége van. A hozzáférő személyeket titoktartási kötelezettség terheli.

23.2. A munkatársak belépéskor, majd rendszeresen adatvédelmi és információbiztonsági oktatásban részesülnek. A magasabb kockázatú munkakörök számára célzott képzés biztosítandó.

23.3. A szabályzat megsértése munkajogi, polgári jogi, szabálysértési vagy büntetőjogi következménnyel járhat az alkalmazandó jog szerint.

24. Ellenőrzés, felülvizsgálat és változáskezelés

24.1. A társaság legalább évente felülvizsgálja az adatkezelési nyilvántartást, az adatfeldolgozói jegyzéket, a magas kockázatú adatkezeléseket, az incidensnyilvántartást és a kapcsolódó tájékoztatókat.

24.2. Soron kívüli felülvizsgálat szükséges különösen új üzleti folyamat, IT-rendszer, kamera, biometrikus megoldás, nagyobb szervezeti átalakítás, jelentős incidens, új adatfeldolgozó, harmadik országbeli adattovábbítás vagy releváns jogszabályváltozás esetén.

24.3. A szabályzat módosítása jóváhagyást követően lép hatályba. A munkatársakat a feladataikat érintő változásokról dokumentálható módon tájékoztatni kell.

25. Jogérvényesítés és felügyeleti hatóság

25.1. Az érintett a társasághoz az adatvédelmi kapcsolattartási elérhetőségen fordulhat. Panaszt tehet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál, továbbá bírósági jogorvoslatot vehet igénybe a GDPR és a magyar jog szerint.

25.2. NAIH aktuális adatok a szabályzat felülvizsgálatakor: 1055 Budapest, Falk Miksa utca 9–11.; levelezési cím: 1363 Budapest, Pf. 9.; honlap: www.naih.hu. Az elérhetőségeket közzététel előtt minden esetben ellenőrizni kell a Hatóság honlapján.

26. Záró rendelkezések

26.1. Jelen szabályzat a jóváhagyás napján lép hatályba, és ezzel egyidejűleg a társaság azonos tárgyú korábbi belső szabályzatának ellentétes rendelkezései hatályukat vesztik.

26.2. A szabályzat önmagában nem pótolja az egyes adatkezelésekhez szükséges érintetti tájékoztatókat, hozzájáruló nyilatkozatokat, érdekmérlegelési teszteket, adatfeldolgozói szerződéseket, kamerás dokumentációt, adatvédelmi hatásvizsgálatot vagy adatkezelési nyilvántartást.

26.3. A mellékletek minták. Azokat a társaság tényleges folyamataihoz kell kitölteni; nem alkalmazhatók automatikusan olyan adatkezelésre, amelynek tényei eltérnek a mintától.

1. melléklet – Adatkezelési nyilvántartás mintája

Adatkezelés/cél	Érintettek	Adatok	Jogalap	Címzettek / adatfeldolgozók	Megőrzés	Biztonsági intézkedés
Munkaviszony adminisztráció	munkavállalók	azonosító, kapcsolati, munkaviszonyi adatok	GDPR 6(1)c / 6(1)b; Mt. és egyéb jogszabály	bérszámfejtő, hatóságok – ténylegesen alkalmazott kör szerint	jogszabályi / igényérvényesítési idők szerint	jogosultságkezelés, zárt HR-tárhely
Szerződéses partner kapcsolattartó	partner természetes személy kapcsolattartói	név, beosztás, munkahelyi elérhetőség	jogos érdek vagy szerződés – tényállástól függően	belső kapcsolattartók, szükséges szolgáltatók	kapcsolat fennállása + indokolt jogérvényesítési idő	hozzáférés-korlátozás
Panaszkezelés	panaszosok	azonosító, elérhetőség, panasz tartalma	jogi kötelezettség / jogos érdek – konkrét jogszabály szerint	illetékes munkatársak, hatóság szükség esetén	konkrét jogszabály szerint	elkülönített ügykezelés
Kamerás megfigyelés (ha van)	belépők, munkavállalók, vásárlók	képmás, mozgás, időpont	GDPR 6(1)f – dokumentált jogos érdek	szűk jogosulti kör, hatóság jogszerű megkeresésre	célhoz szükséges, külön meghatározandó	jogosultság, naplózás, védett rendszer
Marketing (ha van)	feliratkozók	név, e-mail, hozzájárulási metaadat	GDPR 6(1)a; Grt. követelményei	hírlevél-szolgáltató – ha van	visszavonásig + bizonyíthatósághoz szükséges korlátozott adatok	leiratkozás, hozzáférés-korlátozás

2. melléklet – Érintetti kérelem kezelési lap

Kérelem beérkezése	
Kérelmező / azonosítás módja	
Kérelem típusa	hozzáférés / helyesbítés / törlés / korlátozás / hordozhatóság / tiltakozás / egyéb
Érintett rendszerek és szervezeti egységek	
Határidő	főszabály szerint 1 hónap
Hosszabbítás szükséges?	igen / nem; indok:
Döntés és jogalap	
Teljesítés / elutasítás dátuma	
Érintett tájékoztatásának módja	

3. melléklet – Adatvédelmi incidens belső adatlap

Észlelés időpontja	
Belső bejelentés időpontja és bejelentő	
Tudomásszerzés GDPR szerinti időpontja	
Incidens leírása	
Érintettek kategóriái / becsült száma	
Érintett adatok kategóriái / becsült mennyisége	
Lehetséges következmények	
Azonnali intézkedések	
Kockázatértékelés	nem valószínű kockázat / kockázat / magas kockázat
NAIH-bejelentés szükséges?	igen / nem; döntés indoka

NAIH-bejelentés időpontja	
Érintetti tájékoztatás szükséges?	igen / nem; döntés indoka
Lezárás és megelőző intézkedések	

4. melléklet – Új adatkezelés indítási ellenőrzőlista

☐ Az adatkezelés célja konkrétan és dokumentáltan meghatározott.

☐ A szükséges személyes adatok köre minimalizált.

☐ A GDPR 6. cikk szerinti jogalap meghatározott; különleges adatnál a 9. cikk szerinti feltétel is.

☐ A megőrzési idő vagy törlési feltétel meghatározott.

☐ Az érintetti tájékoztató elkészült / frissült.

☐ Jogos érdek esetén az érdekmérlegelési teszt elkészült.

☐ Adatfeldolgozó esetén a GDPR 28. cikk szerinti szerződés rendelkezésre áll.

☐ Harmadik országbeli adattovábbítás vizsgálata megtörtént.

☐ A hozzáférési jogosultságok és biztonsági intézkedések meghatározottak.

☐ A DPIA szükségességét megvizsgálták.

☐ Az adatkezelési nyilvántartás frissült.

☐ A törlési/archiválási folyamat technikailag megvalósított.

5. melléklet – Érdekmérlegelési teszt minimumtartalma

- A tervezett adatkezelés és a jogos érdek pontos leírása.
- Annak vizsgálata, hogy a cél elérése szükségessé teszi-e a személyes adatok kezelését, és van-e kevésbé beavatkozó alternatíva.
- Az érintettek ésszerű elvárásainak, helyzetének és az adatok jellegének értékelése.
- A lehetséges hátrányok és kockázatok, valamint a mérséklő garanciák bemutatása.
- Az érdekek összevetésének indokolt eredménye.
- Az érintetti tájékoztatás és tiltakozási jog gyakorlásának módja.
- A teszt készítésének és felülvizsgálatának dátuma, felelős személy.

6. melléklet – Adatfeldolgozói szerződés ellenőrzőlista

- Az adatkezelés tárgya, időtartama, jellege és célja.
- A személyes adatok típusa és az érintettek kategóriái.
- Adatkezelő dokumentált utasításai.
- Titoktartási kötelezettség.
- GDPR 32. cikk szerinti biztonsági intézkedések.
- Al-adatfeldolgozó igénybevételének feltételei.
- Érintetti jogok teljesítésének támogatása.
- Incidens-, DPIA- és hatósági együttműködés.
- Adatok visszaadása vagy törlése a szolgáltatás végén.
- A megfelelés igazolásához szükséges információk és auditjog.
- Nemzetközi adattovábbítások és adattárolási helyek rendezése.

7. melléklet – Források és felülvizsgálati hivatkozások

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR), EUR-Lex: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=HU

2011. évi CXII. törvény (Infotv.), Nemzeti Jogszabálytár: https://njt.hu/jogszabaly/2011-112-00-00

2012. évi I. törvény a munka törvénykönyvéről, Nemzeti Jogszabálytár: https://njt.hu/jogszabaly/2012-1-00-00

2000. évi C. törvény a számvitelről, Nemzeti Jogszabálytár: https://njt.hu/jogszabaly/2000-100-00-00

2008. évi XLVIII. törvény a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól, Nemzeti Jogszabálytár: https://njt.hu/jogszabaly/2008-48-00-00

NAIH – Érintetti jogok, adatvédelmi incidensek, kamerás adatkezelések és aktuális elérhetőségek: https://www.naih.hu/

Felülvizsgálati megjegyzés: a dokumentum 2026. augusztus 27-i állapot szerint készült. A konkrét adatkezelési tájékoztatók és mellékletek véglegesítéséhez a társaság tényleges adatkezeléseinek, informatikai rendszereinek, adatfeldolgozóinak, kamerarendszerének, HR- és marketingfolyamatainak tételes leltára szükséges.