ADATKEZELÉSI SZABÁLYZAT

Belső adatvédelmi és adatbiztonsági szabályzat

Adatkezelő: BÜKI Fejlesztési és Beruházási Kft.

Verzió: 3.0

Hatálybalépés: 2026. szeptember 2.

Státusz: Hatályos változat

Rendeltetés. A szabályzat a társaság adatkezelési irányításának belső kerete. Nem helyettesíti az egyes érintetti köröknek szóló adatkezelési tájékoztatókat, az adatkezelési nyilvántartást, az adatfeldolgozói szerződéseket vagy a kamerás szabályozást.

Jóváhagyás és dokumentumgazda

Szerep	Név / szervezeti egység
Jóváhagyó ügyvezető	Csabai Imre
Jóváhagyó ügyvezető	Neumann Péter
Adatvédelmi tisztviselő / dokumentumgazda	Kun Beáta
Következő rendes felülvizsgálat	2027. szeptember 2., illetve jogszabályi, szervezeti vagy technológiai változáskor haladéktalanul

1. Az adatkezelő és a szabályzat hatálya

Adatkezelő: BÜKI Fejlesztési és Beruházási Kft. (székhely: 1025 Budapest, Csévi u. 8.; cégjegyzékszám: 01-09-171611; adószám: 13311207-2-41). A szálláshely címe: Caramell Premium Resort, 9740 Bük, Európa út 18. E-mail: info@caramell.hu; telefon: +36 94 558 030.

Adatvédelmi tisztviselő: Kun Beáta. Kapcsolat: kun.beata@caramell.hu; +36 30 624 3688; postacím: 1025 Budapest, Csévi u. 8.

A szabályzat személyi hatálya kiterjed a társaság munkavállalóira, vezetőire, megbízottaira és minden olyan személyre, aki a társaság nevében személyes adatot kezel. Tárgyi hatálya az elektronikus és papíralapú adatkezelésekre, különösen a vendég-, foglalási, rendezvény-, marketing-, munkavállalói, pályázói, partneri, kamerás és informatikai adatkezelésekre terjed ki.

2. Irányadó szabályok és fogalmak

A szabályzat alapja különösen az (EU) 2016/679 rendelet (GDPR), a 2011. évi CXII. törvény (Infotv.), a turisztikai térségek fejlesztésének állami feladatairól szóló 2016. évi CLVI. törvény és végrehajtási szabályai, továbbá az alkalmazandó számviteli, adó-, fogyasztóvédelmi, munkaügyi és vagyonvédelmi rendelkezések.

A GDPR fogalmai irányadók. Különleges adat különösen az egészségi állapotra vonatkozó adat; adatvédelmi incidens a kezelt személyes adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását sértő esemény.

3. Alapelvek és felelősség

- jogszerűség, tisztességes eljárás és átláthatóság;
- célhoz kötöttség és adattakarékosság;
- pontosság és szükség szerinti helyesbítés;
- korlátozott tárolhatóság;
- integritás, bizalmas jelleg és megfelelő biztonság;
- elszámoltathatóság: a megfelelés dokumentálása és bizonyíthatósága.

Minden szervezeti egység vezetője felel azért, hogy új adatkezelés, új rendszer, szolgáltató vagy adatátadás bevezetése előtt az adatvédelmi tisztviselő bevonása megtörténjen. A hozzáférés kizárólag munkaköri szükséglet alapján adható.

4. Jogszerűség és célmeghatározás

Személyes adat csak előre meghatározott célból, megfelelő jogalapon és a szükséges mértékben kezelhető. A leggyakoribb jogalapok: szerződés teljesítése vagy előkészítése; jogi kötelezettség; jogos érdek megfelelő érdekmérlegeléssel; hozzájárulás; kivételesen létfontosságú érdek. Különleges adat csak a GDPR 9. cikkében meghatározott további feltétellel kezelhető.

Tilos. A hozzájárulást olyan adatkezeléshez használni, amely valójában kötelező vagy a szerződés teljesítéséhez szükséges. A hírlevél-hozzájárulás külön, önkéntes és bármikor visszavonható.

5. Tájékoztatás és az érintetti jogok

Ha az adat közvetlenül az érintettől érkezik, a GDPR 13. cikke szerinti tájékoztatást az adatfelvételkor kell megadni. Ha az adat például munkáltatótól, rendezvényszervezőtől, utazási irodától vagy online közvetítőtől érkezik, a GDPR 14. cikke szerinti tájékoztatás szükséges, főszabály szerint legkésőbb egy hónapon belül, illetve az első kapcsolatfelvételkor vagy az első adattovábbításkor.

- hozzáférés és másolat kérése;
- helyesbítés;
- törlés, ha annak feltételei fennállnak;
- adatkezelés korlátozása;
- adathordozhatóság a jogszabályi feltételek mellett;
- tiltakozás jogos érdeken vagy közérdekű feladaton alapuló adatkezelés ellen;
- hozzájárulás visszavonása;
- panasz a NAIH-nál és bírósági jogorvoslat.

A kérelmet indokolatlan késedelem nélkül, főszabály szerint egy hónapon belül kell megválaszolni. Szükség esetén a határidő további két hónappal meghosszabbítható, amelyről az érintettet egy hónapon belül, indoklással tájékoztatni kell. Az érintett személyazonossága arányos módon ellenőrizhető.

6. Adatkezelési nyilvántartás és megőrzés

A társaság a GDPR 30. cikke szerinti nyilvántartást naprakészen vezeti. A nyilvántartás legalább a célt, érintetti és adatkategóriákat, jogalapot, címzetteket, harmadik országbeli adattovábbítást, törlési határidőt és biztonsági intézkedéseket tartalmazza.

A megőrzési időt adatkezelésenként kell meghatározni. A határidő lejártakor az adatot biztonságosan törölni vagy anonimizálni kell, kivéve, ha folyamatban lévő igény, hatósági eljárás vagy jogszabály

hosszabb megőrzést követel. A számviteli bizonylatokat a mindenkor hatályos számviteli megőrzési idő szerint kell őrizni.

7. Szállodai adatkezelések

Terület	Fő szabály
Ajánlatkérés és foglalás	A szerződés előkészítéséhez és teljesítéséhez szükséges adatok kezelhetők; csoportfoglalásnál az adatforrást és a GDPR 14. cikk szerinti tájékoztatást dokumentálni kell.
Bejelentkezés és vendégnyilvántartás	Csak a szolgáltatáshoz és jogszabályi kötelezettséghez szükséges adatok vehetők fel. A személyazonosító okmány adatainak rögzítése a VIZA-szabályok szerint történik.
VIZA	A vendégazonosítási és adattovábbítási kötelezettséget a hatályos turisztikai szabályok szerint kell teljesíteni; a vendéget külön tájékoztatni kell.
NTAK	Az NTAK felé statisztikai, személyazonosításra nem alkalmas szálláshelyi adatok továbbíthatók a jogszabály szerinti körben.
Wellness / egészségügyi információ	Egészségi adat csak akkor kérhető, ha a szolgáltatás biztonságos nyújtásához ténylegesen szükséges, és megfelelő GDPR 9. cikk szerinti feltétel fennáll.
Kamera	Külön kamerás adatkezelési szabályzat és tájékoztató szükséges, kameránként dokumentált céllal, látószöggel és megőrzési idővel.
Marketing	A szolgáltatási kommunikáció és a reklámcél elkülönítendő. Hírlevél csak megfelelő hozzájárulással küldhető; a leiratkozást azonnal érvényesíteni kell.

8. Adatfeldolgozók és közös adatkezelés

A szállodai működésben adatfeldolgozók igénybevétele releváns. Ide tartozhat többek között a szállodai PMS, foglalási motor és channel manager, webtárhely, levelezés, informatikai támogatás, online fizetés, bérszámfejtés, marketing- és ügyfélkommunikációs rendszer. Adatfeldolgozó csak dokumentált átvilágítás és a GDPR 28. cikkének megfelelő szerződés alapján vehető igénybe.

- a szolgáltató pontos jogi neve, székhelye és szerepe;
- az adatkezelés tárgya, időtartama, célja, adatkategóriái és érintettjei;
- titoktartás, biztonság, al-adatfeldolgozók, incidensjelzés és audit;
- adatok visszaadása vagy törlése a szolgáltatás végén;
- EGT-n kívüli hozzáférés vagy adattovábbítás jogalapja és garanciái.

Közös adatkezelés esetén a felek a GDPR 26. cikke szerinti megállapodásban átláthatóan rögzítik felelősségüket. Az önálló adatkezelők közötti adattovábbítást külön jogalap és tájékoztatás alapján kell értékelni.

9. Harmadik országba történő adattovábbítás

Az Európai Gazdasági Térségen kívüli továbbítás vagy távoli hozzáférés csak megfelelőségi határozat, megfelelő garancia - például általános szerződési feltételek - vagy a GDPR szerinti kivételes feltétel alapján történhet. A transzferhatás-vizsgálat és szükséges kiegészítő intézkedések dokumentálandók.

10. Adatbiztonság

- szerepköralapú hozzáférés, egyedi azonosító, erős jelszó és ahol lehetséges többtényezős hitelesítés;
- jogosultságok rendszeres felülvizsgálata és azonnali megszüntetése kilépéskor;
- eszközök, hálózatok, biztonsági mentések és hordozható adathordozók megfelelő védelme;
- naplózás, sérülékenység- és frissítéskezelés, kártékony kód elleni védelem;
- papíralapú iratok zárt tárolása, tiszta asztal és biztonságos megsemmisítés;
- személyes adat küldésekor címzettellenőrzés, szükség szerint titkosítás vagy védett átadási csatorna;
- rendszeres mentési és helyreállítási teszt.

11. Adatvédelmi incidens

Minden munkatárs köteles az elveszett iratot vagy eszközt, téves címzettnek küldött üzenetet, jogosulatlan hozzáférést, zsarolóvírust, rendszerhibát vagy más gyanús eseményt haladéktalanul jelenteni a vezetőjének és az adatvédelmi tisztviselőnek. A jelentés nem késleltethető a teljes kivizsgálásig.

1. Az esemény azonnali behatárolása és a bizonyítékok megőrzése.
2. Az érintett adatok, személyek, következmények és intézkedések dokumentálása az incidens-nyilvántartásban.
3. Kockázatértékelés az érintettek jogaira és szabadságaira nézve.
4. Ha valószínűsíthető kockázat áll fenn, bejelentés a NAIH-nak lehetőség szerint 72 órán belül.
5. Magas kockázat esetén az érintettek közérthető tájékoztatása, kivéve a GDPR szerinti mentességet.
6. Helyesbítő intézkedés, utóelemzés és szabályzat- vagy rendszerfrissítés.

12. Adatvédelmi hatásvizsgálat

Új, várhatóan magas kockázatú adatkezelés előtt adatvédelmi hatásvizsgálatot kell végezni. Különösen értékelendő az új technológia, nagy léptékű megfigyelés, profilalkotás, különleges adatok nagy körű kezelése, valamint több adatforrás összekapcsolása. A tisztviselő véleményét ki kell kérni.

13. Az adatvédelmi tisztviselő

Az adatvédelmi tisztviselő szakmailag függetlenül jár el, közvetlenül a legfelső vezetésnek jelent, feladatai miatt nem utasítható és nem érheti hátrány. Részt vesz az adatvédelmi kérdésekben, tanácsot ad, ellenőrzi a megfelelést, közreműködik a hatásvizsgálatokban, kapcsolatot tart a felügyeleti hatósággal és támogatja az érintetti kérelmek kezelését.

14. Oktatás, ellenőrzés és fegyelmi felelősség

Belépéskor és ezt követően rendszeresen adatvédelmi oktatást kell tartani; a részvételt dokumentálni kell. A kiemelt jogosultságú és vendégadatokkal dolgozó munkatársak célzott képzést kapnak. A szabályzat megsértése munkajogi, polgári jogi, hatósági vagy büntetőjogi következménnyel járhat.

15. Felülvizsgálat és hatály

A szabályzat 2026. szeptember 2-án lép hatályba, és a korábbi belső adatkezelési szabályzat helyébe lép. Felülvizsgálata legalább évente, továbbá jogszabály-, szervezet-, rendszer-, szolgáltató- vagy adatkezelési változáskor kötelező. A változásokat verziószámmal és jóváhagyással kell dokumentálni.

1. melléklet - Kötelező adatkezelési leltár

Mező	Kitöltési követelmény
Adatkezelés megnevezése	Folyamat és felelős szervezeti egység.
Cél és jogalap	Konkrét cél; GDPR 6. cikk, szükség esetén 9. cikk; jogos érdek esetén érdekmérlegelés.
Érintettek és adatok	Érintetti kör, adatkategóriák, különleges adat jelölése.
Forrás és tájékoztató	Közvetlen vagy harmadik fél; alkalmazott 13/14. cikk szerinti tájékoztató.
Címzettek / adatfeldolgozók	Pontos jogi név, szerep, ország, szerződés és al-adatfeldolgozók.

Megőrzés	Konkrét idő vagy objektív törlési feltétel, jogszabályi hivatkozással.
Biztonság	Hozzáférés, naplózás, titkosítás, mentés, fizikai védelem.
Adattovábbítás	Hatóság, önálló adatkezelő, közös adatkezelő; EGT-n kívüli garancia.
DPIA / incidens	Hatásvizsgálati döntés és kapcsolódó incidensek.

2. melléklet - Források

- GDPR: https://eur-lex.europa.eu/eli/reg/2016/679/oj/hun
- Nemzeti Jogszabálytár: https://njt.hu
- NAIH: https://naih.hu
- VIZA tájékoztató: https://vizainfo.hu
- NTAK információ: https://info.ntak.hu