

Békéscsaba Smart Management Kft.

ADATVÉDELMI POLITIKÁJA

ÉS

ADATVÉDELMI SZABÁLYZATA

Békéscsaba, 2024. május 21.

Kovács Gyula
ügyvezető

Szél Adrián
cégvezető

Békéscsaba Smart Management Kft.

ADATVÉDELMI POLITIKÁJA

Békéscsaba Smart Management Kft. - az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679. számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95146. EK irányelv hatályon kívül helyezéséről szóló rendelettel (a továbbiakban: GDPR) - összhangban, figyelemmel arra, hogy a Vállalkozás jelentős mennyiségű személyes adatot kezel, kiemelten fontosnak tartja a személyes adatok védelmét.

A Vállalkozás törekszik arra, hogy - a GDPR-ban megfogalmazott célhoz kötöttség és adattakarékosság elvének maradéktalan érvényesülése érdekében - a személyes adatokhoz kizárólag azok a személyek és ők is csak olyan mértékben férhessenek hozzá, akiknek és amilyen mértékben az az adott feladat ellátásához feltétlenül szükséges.

A Vállalkozás elkötelezett olyan megoldások és eljárásrendek kialakítása, illetőleg működtetése iránt, amely biztosítja a GDPR és a hazai adatvédelmi normák előírásainak történő megfelelést, és mindent elkövet annak érdekében, hogy az általa kezelt személyes adatokat a megfelelő biztonsági technológiák felhasználásával és eljárásrendek útján védje az illetéktelen hozzáféréstől.

A Vállalkozás kiemelt figyelmet fordít arra, hogy olyan partnerekkel működjön együtt, akik biztosítják a mindenkor hatályos adatvédelmi szabályoknak történő megfelelést, valamint az érintettek jogainak védelmét.

A Vállalkozás mindent elkövet annak érdekében, hogy ügyfelei, munkatársai, partnerei és minden más érintett megfelelő ismeretekkel rendelkezzen a személyes adataik Vállalkozás általi kezeléséről és az adatkezelésre irányadó szabályokról, továbbá minden érintett megfelelően gyakorolhassa a személyes adataihoz fűződő jogokat.

A Vállalkozás a szabályozásnak való folyamatos megfelelés érdekében törekszik olyan módszerek alkalmazására, melyek megnyugtató módon biztosítják az adatkezelésekhez kapcsolódó megoldások, eljárásrendek és technikai háttér rendszeres felülvizsgálatát és fejlesztését.

Bízunk benne, hogy a személyes adatok fenti szempontok szerint történő kezelése is hozzájárul ahhoz, hogy a Vállalkozás a jogszabályoknak megfelelően, Ügyfelei, Partnerei, tulajdonosai megalégedésére lássa el feladatát.

A Vállalkozás weboldalján (www.bcsenergia.hu) az Adatvédelem menüpont alatt elérhetőek a Vállalkozás adatkezelési tevékenységére vonatkozó legfontosabb információk, hatályos jogszabályok és szabályzatok, továbbá az adatvédelmi tisztviselő elérhetőségei.

Békéscsaba Smart Management Kft.

ADATVÉDELMI SZABÁLYZATA

Békéscsaba Smart Management Kft. (a továbbiakban: Vállalkozás) működése során a személyes adatok kezelésének szabályozására - az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679 rendeletében (a továbbiakban: GDPR), továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (a továbbiakban: Infotv.) foglaltakra figyelemmel - a természetes személyek adatainak védelme érdekében jelen szabályzatot adjuk ki:

I. rész

BEVEZETŐ RENDELKEZÉSEK

I/1. A szabályzat célja

Jelen szabályzat célja azon belső szabályok és eljárásrendek kialakítása és egyedi intézkedések megalapozása, amelyek biztosítják, hogy az Vállalkozás tevékenysége megfeleljen a GDPR és az Infotv. hatályos előírásainak, és elősegítse az érintettek jogainak érvényesítését, és ezzel megvalósuljon a Vállalkozás tevékenységét teljes egészét átfogó adatvédelmi mechanizmus.

I/2. Az adatkezelő

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 3. § 8. pontja alapján adatkezelőnek minősül az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.

Jelen adatkezelési tájékoztatóban hivatkozott adatkezelési tevékenységek tekintetében adatkezelőnek minősül:

Az adatkezelő

Békéscsaba Smart Management Kft.

Székhely: 5600 Békéscsaba, Szent István tér 7.

Cégjegyzékszám: 04 09 016850

Adószám: 32249084-2-04

Képviselő: Kovács Gyula ügyvezető

Elérhetőség:

- **Postai cím:** : 5600 Békéscsaba, Szent István tér 7.
- **E-mail cím:** info.smartbcs@gmail.com
- **Telefonszám:** +36 20 257 6506

Adatvédelmi tisztviselő:

Szécsi Jenő

Elérhetőség:

- **Postai cím:** 5600 Békéscsaba, Szent István tér 7.
- **E-mail cím:** szecsi.jeno@bcsenergia.hu
- **Telefonszám:** +36 20 808 4990

Az adatkezelő kijelenti, hogy az adatkezelés minden szakaszában az Infotv. és az Európai Unió Általános Adatvédelmi Rendelete (GDPR) előírásainak megfelelően jár el.

I/3. A szabályzat hatálya

Jelen szabályzat hatálya a Vállalkozás által annak hatásköre és feladatellátása során kezelt, illetve nyilvántartott személyes adatok [GDPR 4. cikk 1.] kezelésére [GDPR 4. cikk 2.] terjed ki.

Ennek megfelelően jelen szabályzat hatálya kiterjed a Vállalkozásnál folyó, a személyes adatokkal kapcsolatos valamennyi ügyintézési és ügykezelési eljárásra, az adatkezelés során felhasznált valamennyi tárgyi és informatikai eszközre, függetlenül azok üzemeltetési helyétől és a tulajdoni helyzetétől.

Jelen szabályzat rendelkezéseit Vállalkozással munkavégzésre irányuló jogviszonyban álló minden olyan személy köteles alkalmazni, aki munkakörének, illetőleg munkavégzésre irányuló jogviszonyát szabályozó szerződésének teljesítése során személyes adatokat kezel, függetlenül attól, hogy munkáját közszolgálati jogviszony, munkaviszony vagy munkavégzésre irányuló más jogviszony keretében végzi (a továbbiakban: munkatársak).

1/4. Fogalmak

Jelen szabályzat alkalmazásában

1) **személyes adat:** azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható [GDPR 4. cikk 1. pont];

2) **adatkezelés:** a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés [GDPR 4. cikk 2. pont];

3) **az adatkezelés korlátozása:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából [GDPR 4. cikk 3. pont];

4) **profilalkotás:** személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészség1 állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják [GDPR 4. cikk 4. pont];

5) **álnevesítés:** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni [GDPR 4. cikk 5. pont];

6) **nyilvántartási rendszer:** a személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető [GDPR 4. cikk 6. pont];

7) **adatkezelő:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja [GDPR 4. cikk 7. pont];

8) **adatifeldolgozó:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel [GDPR 4. cikk 8. pont];

9) **címzett:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak [GDPR 4. cikk 9. pont];

10) **harmadik fél:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak [GDPR 4. cikk 10. pont];

11) **az érintett hozzájárulása:** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez [GDPR 4. cikk 11. pont];

12) **adatvédelmi incidens:** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi [GDPR 4. cikk 12. pont].

1/5. Alapelvek

1. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni (**jogszerűség, tisztességes eljárás és átláthatóság elve**) [GDPR 5. cikk (1) bek. a) pont].

2. Személyes adat kezelése kizárólag meghatározott, egyértelmű és törvényes célból történhet, az adatok kezelése nem végezhető célokkal össze nem egyeztethető módon (**célhoz kötöttség elve**) [GDPR 5. cikk (1) bek. b) pont].

3. A személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk (**adattakarékosság elve**) [GDPR 5. cikk (1) bek. c) pont].

4. A személyes adatoknak pontosnak és ahol szükséges, naprakésznek kell lenniük (**pontos és naprakész adtakezelés elve**) [GDPR 5. cikk (1) bek. d) pont].

5. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (**korlátozott tárolhatóság elve**) [GDPR 5. cikk (1) bek. e) pont].

6. A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezeti intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (**integritás és bizalmasság elve**) [GDPR 5. cikk (1) bek. f) pont].

7. Az adatkezelő felelős a jelen szabályzatban meghatározott alapelveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására. Ennek megfelelően a munkatársak is úgy kötelesek eljárni, hogy szükség esetén az alapelveknek való megfelelés igazolására felettesük felhívására képesek legyenek (**elszámoltathatóság elve**) [GDPR 5. cikk (2) bek.].

1/6. Az adatkezeléssel kapcsolatos feladatok

1. Az ügyvezető

- a) Gondoskodik arról, hogy a vállalkozás működése során a személyes adatok kezelése a hatályos nemzeti és európai uniós adatvédelmi jogszabályokkal, különösen a GDPR-ral és az Infotv.-vel összhangban történjen.
- b) Meghatározza az adatkezelés célját és kereteit, valamint gondoskodik a szükséges technikai és szervezési intézkedések megtételéről az adatok biztonsága érdekében.
- c) Kijelöli az adatvédelmi tisztviselőt (ha van), vagy ellátja az adatvédelmi tisztviselői feladatokat.

2. A cégvezető

- a) Folyamatosan tájékoztatja a munkatársakat a hatályos adatvédelmi jogszabályokról és a vállalkozás belső adatvédelmi szabályzatáról.
- b) Gondoskodik arról, hogy a munkatársak megfelelő képzésben részesüljenek az adatvédelemmel kapcsolatban.
- c) Ellenőrzi az adatkezelési tevékenységeket, és intézkednek az esetleges hiányosságok megszüntetése érdekében.

3. A munkatársak

- a) Munkavégzésük során maradéktalanul kötelesek betartani a hatályos nemzeti és uniós adatvédelmi jogszabályokat, különösen a GDPR és az Infotv. rendelkezéseit.
- b) Kötelesek megőrizni a munkavégzéssel kapcsolatban tudomásukra jutott személyes adatokat, és azokat kizárólag a munkavégzés céljára felhasználni.
- c) Adatkezeléssel kapcsolatban felmerülő kérdéseikkel fordulhatnak az adatvédelmi tisztviselőhöz (ha van), vagy az ügyvezetőhöz.
- d) Adatvédelmi incidens bekövetkezése esetén haladéktalanul kötelesek jelenteni azt az adatvédelmi tisztviselőnek (ha van), vagy az ügyvezetőnek.
- e) Az adatkezeléssel kapcsolatban feltárt visszasságokat kötelesek haladéktalanul jelezni az adatvédelmi tisztviselőnek (ha van), vagy az ügyvezetőnek. f) Részt vesznek a vállalkozás által szervezett adatvédelmi oktatáson.

4. Az informatikai rendszer üzemeltetője

- a) Gondoskodik az informatikai rendszer biztonságos működtetéséről, és megteszi a szükséges technikai és szervezési intézkedéseket az adatok védelme érdekében.
- b) Rendszeresen ellenőrzi az informatikai rendszer biztonságát, és intézkedik az esetleges sérülékenységek megszüntetése érdekében.

c) Segítséget nyújt a munkatársaknak az adatkezeléssel kapcsolatos technikai problémák megoldásában.

II. rész

AZ ADATKEZELÉS JOGALAPJA

Személyes adatok kizárólag akkor kezelhetők, ha a GDPR-ban és az alábbiakban meghatározására kerülő jogalpok valamelyike bizonyíthatóan fennáll.

II/1. Az érintett hozzájárulása

(GDPR 6. cikk (1) bekezdés a) pont)

A hozzájárulás az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez. A hozzájárulást az adatkezelés megkezdését megelőzően kell beszerezni.

Ennek megfelelően:

- a) a munkatársaknak megfelelő tájékoztatást kell adniuk az érintett részére az adatkezelésről;
- b) a hozzájárulást mindig aktív cselekedettel vagy nyilatkozattal kell megadni írásban, szóban vagy elektronikus úton;
- c) a munkatársaknak képesnek kell lenniük az adatkezelés során bármikor annak igazolására, hogy az érintett hozzájárult az adatkezeléshez;
- d) biztosítani kell, hogy az érintett a hozzájárulását bármikor visszavonhassa, és a hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Alkalmazott adatkezelések:

- **Hírlevél feliratkozás:** Az érintett feliratkozik a Vállalkozás hírlevelére, és ehhez megadja az e-mail címét.
- **Direkt marketing:** Az érintett hozzájárul ahhoz, hogy a Vállalkozás marketing célú ajánlatokkal, tájékoztatókkal keresse meg.
- **Fénykép- és videófelvetelek készítése rendezvényeken:** Az érintett hozzájárul ahhoz, hogy róla kép- és videófelvétel készüljön a Vállalkozás rendezvényein, és ezek a felvételek felhasználásra kerüljenek (pl. a Vállalkozás honlapján vagy közösségi média felületein).

II/2. Szerződéses viszonyon alapuló adatkezelés

(GDPR 6. cikk (1) bekezdés b) pont)

Szerződésen alapuló adatkezelés esetén az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az e szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

Szerződésen alapuló adatkezelés esetén is fokozottan figyelemmel kell lenni az adattakarékosság elvére. Ennek megfelelően szerződésben szerepeltetni és szerződéssel kapcsolatban személyes adatot kezelni csak a szerződés teljesítéséhez szükséges mértékben lehet.

Alkalmazott adatkezelések:

- **Ügyfelek adatainak kezelése:** Az ügyfelek személyes adatait (név, elérhetőség, számlázási adatok stb.) a szerződéskötés, a szolgáltatásnyújtás, a számlázás és a szerződésből eredő jogok és kötelezettségek érvényesítése céljából kezeljük.
- **Partnerek adatainak kezelése:** A partnereinkkel kötött szerződések teljesítése érdekében kezeljük a partnerek kapcsolattartóinak személyes adatait (név, beosztás, elérhetőség).
- **Munkavállalók adatainak kezelése:** A munkavállalókkal kötött munkaszerződések teljesítése érdekében kezeljük a munkavállalók személyes adatait (név, lakcím, adóazonosító jel, bankszámlaszám stb.).
- **Ajánlatkérés:** Amennyiben Ön ajánlatot kér tőlünk, az ajánlat elkészítéséhez és megküldéséhez szükséges személyes adatait (név, elérhetőség) kezeljük.

Adattakarékosság elve:

A szerződéses viszonyból eredő adatkezelés során is kiemelten fontos az adattakarékosság elve. Csak olyan személyes adatokat kezelünk, amelyek a szerződés teljesítéséhez feltétlenül szükségesek, és azokat csak a szerződés teljesítéséhez szükséges ideig őrizzük meg.

II/3. Jogi kötelezettség teljesítésével összefüggő adatkezelés

(GDPR 6. cikk (1) bekezdés c) pont)

Személyes adat kezelése lehetséges, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. A jogi kötelezettségen alapuló adatkezelés esetén a kezelhető adatok körére, az adatkezelés céljára, az adatok tárolásának időtartamára, a címzettek az alapul szolgáló jogszabály rendelkezései irányadók.

Ezen jogalapon folytatott adatkezelés esetén a munkatársaknak mindig képeseknek kell lenniük annak igazolására, hogy a jogi kötelezettséget hatályos jogszabály írja elő. A vonatkozó jogszabály változása esetén vizsgálni kell, hogy a személyes adat kezelésének jogalapja fennáll-e.

Alkalmazott adatkezelések:

- **Könyvviteli és adózási kötelezettségek:** A számviteli és adózási törvények által előírt bizonylatok kiállítása és megőrzése érdekében kezeljük a személyes adatokat (pl. név, cím, adószám).
- **Munkajogi kötelezettségek:** A munkajogi törvények betartása érdekében kezeljük a munkavállalók személyes adatait (pl. név, lakcím, TAJ szám, bankszámlaszám).
- **Hatósági adatszolgáltatás:** Amennyiben jogszabály kötelez minket erre, személyes adatokat továbbítunk az illetékes hatóságoknak (pl. bíróság, rendőrség).

II/4. Jogos érdeken alapuló adatkezelés

(GDPR 6. cikk (1) bekezdés f) pont)

Személyes adat kezelése lehetséges, ha az az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes 7 adatok védelmét teszik szükségessé, különösen ha az érintett gyermek [GDPR 6. cikk (1) bek. f) pont].

Alkalmazott adatkezelések:

- **Videófelvételek készítése rendezvényeken:** A Vállalkozás rendezvényein kép- és videófelvételek készülhetnek, amelyeken az érintettek is szerepelhetnek. Ezen felvételek készítésének és felhasználásának célja a Vállalkozás tevékenységének, szolgáltatásainak népszerűsítése, valamint a rendezvények dokumentálása.
- **Ügyfél-elégedettségi felmérés:** A Vállalkozás jogos érdeke fűződik ahhoz, hogy ügyfelei elégedettségét felmérje, hogy szolgáltatásait fejleszthesse.
- **Csalás megelőzése és biztonság:** Jogos érdekünk a csalás megelőzése és a Vállalkozás biztonságának garantálása, ezért zárláncú kamerarendszert üzemeltetünk telephelyünkön.
- **Informatikai rendszer védelme:** Jogos érdekünk az informatikai rendszerünk védelme, ezért naplózzuk a rendszerhasználatot és az esetleges jogsértéseket.

II/5. Létfontosságú érdeken alapuló („vis maior”) adatkezelés

(GDPR 6. cikk (1) bekezdés d) pont)

Személyes adat kezelése lehetséges, ha ez az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. Ezen jogalapon csak akkor és addig folytatható adatkezelés, ha az egyéb jogalapon nem végezhető, és az szükségesnek és arányosnak mutatkozik [GDPR (46) preambulumbek.]. Személyes adat kezelhető, ha ez az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges, különösen, ha az érintett nem képes hozzájárulásának megadására, de a védelem sürgős és elengedhetetlen.

Alkalmazott adatkezelések:

- **Baleset vagy egészségügyi vészhelyzet:** Ha Ön balesetet szenved vagy egészségügyi vészhelyzetbe kerül a Vállalkozás területén, akkor az egészségügyi ellátáshoz szükséges személyes adatait (pl. név, TAJ szám, elérhetőségek) kezelhetjük az Ön vagy mások életének, testi épségének védelme érdekében.
- **Természeti katasztrófa vagy más vészhelyzet:** Rendkívüli helyzetekben (pl. természeti katasztrófa, tűz), amennyiben az szükséges az Ön vagy mások életének, testi épségének védelméhez, kezelhetjük az elérhető személyes adatokat (pl. név, elérhetőség) a mentés, segítségnyújtás vagy tájékoztatás érdekében.

III. rész

AZ ADATKEZELÉSRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK

A Vállalkozás ügyintézői a feladataik ellátása körében személyes adatot csak a hatályos hazai és uniós jogszabályok és jelen szabályzat előírásainak betartásával kezelhetnek.

Különös gondot kell fordítani az adatvédelmi szabályok betartására a 16. életévüket be nem töltött személyes adatainak kezelése során.

A Vállalkozás munkatársai fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartoznak a munkavégzésük során tudomásukra jutott személyes adatok jogszerű kezeléséért.

A Vállalkozás a feladatellátása során kezelt személyes adatokat az adott ügýtípusra vonatkozó ágazati jogszabályok, illetve a mindenkori iratkezelési szabályoknak megfelelő időtartamig tárolja.

Személyes adatot tartalmazó iratról papír alapú, illetve digitális másolatot készíteni kizárólag igazolható célból lehet. A másolatot a másolatkészítés céljának eléréséig, de legfeljebb az eredeti irat selejtezéséig lehet őrizni.

A Vállalkozásnál alkalmazandó informatikai biztonsági és adatvédelmi szabályokról, ügyiratokkal kapcsolatos adatvédelmi szabályozásról, valamint Vállalkozás alkalmazásában állók személyes adatait tartalmazó közszolgálati nyilvántartással összefüggő adatvédelmi, informatikai-biztonsági szabályokról külön szabályzatok rendelkeznek.

Az érintetteket a Vállalkozás a leglapvetőbb adatvédelmi szabályokról, a jelen szabályzatban foglaltakról és az általuk igénybe vehető jogorvoslati lehetőségekről

a) a Vállalkozás weboldalján;

b) munkatársain keresztül

tájékoztatja.

A Vállalkozás biometrikus adatokat nem kezel.

A Vállalkozás harmadik országba a VI. részben leírtak szerint továbbít adatokat.

A Vállalkozás automatizált döntéshozatalt nem végez.

IV. RÉSZ

AZ ÉRINTETTEK JOGAI

IV /1. Tájékoztatáshoz való jog

Az érintettek részére - ún. proaktív módon (előzetesen) - megfelelő tájékoztatást kell nyújtani az adatkezelés tényéről és az adatkezeléssel kapcsolatos egyéb információkról, így különösen:

- az adatkezelő személyéről, elérhetőségeiről és képviselőjéről;
- az adatkezelés céljáról és jogalapjáról;
- a kezelt személyes adatok kategóriáiról;
- az esetleges külföldi adattovábbítás tényéről és körülményeiről;
- az adattárolás időtartamáról;
- az adatkezelés időtartamáról;
- az érintetti jogokról;
- hozzájáruláson alapuló adatkezelés esetén a hozzájárulás visszavonásának lehetőségéről és módjáról;
- amennyiben az adatok nem az érintettől származnak, az adatok forrásáról;
- az adatvédelem érdekében megtett technikai és szervezési intézkedésekről;
- az érintett rendelkezésére álló jogorvoslati lehetőségekről;
- az adatvédelmi tisztviselő személyéről és elérhetőségeiről.

A tájékoztatást közérthető módon kell nyújtani. Szükség esetén az érintett rendelkezésére kell bocsátani a hatályos nemzeti és európai adatvédelmi jogszabályokat és a Vállalkozás adatvédelmi tárgyú szabályzatait.

IV/2. Hozzáféréshez való jog

Az érintett részére - megkeresés esetén -visszajelzést kell adni az adatkezelés során

- a kezelt személyes adatok köréről;
- az adatkezelés céljáról;
- a kezelt személyes adatok kategóriáiról;
- a személyes adatok címzettjeiről vagy a címzettek kategóriáiról;
- az esetleges külföldi adattovábbítás tényéről és körülményeiről;

- az adattárolás időtartamáról;
- az érintetti jogokról;
- az adatok forrásáról;
- az érintett rendelkezésére álló jogorvoslati lehetőségekről;

A visszajelzést közérthető módon kell nyújtani. Szükség esetén az érintett rendelkezésére kell bocsátani a hatályos nemzeti és európai adatvédelmi jogszabályokat és a Vállalkozás adatvédelmi tárgyú szabályzatait.

IV/3. Helyesbítéshez való jog

A pontos és naprakész adatkezelés elvének érvényesítése érdekében az érintett kérésére a Vállalkozás haladéktalanul köteles helyesbíteni a rá vonatkozó pontatlan személyes adatokat.

Az érintett kérésére a Vállalkozás haladéktalanul köteles a hiányos személyes adatokat kiegészíteni, ezen kötelezettség teljesítése során azonban figyelemmel kell lenni a célhoz kötöttség és az adattakarékosság elvére.

Amennyiben a helyesbítést az érintett kérte, a helyesbítés megtörténtéről, illetőleg esetleges elutasításáról - az elutasítás indokaival együtt - haladéktalanul, de legkésőbb a kérelem beérkezésétől számított 30 napon belül dokumentált módon értesíteni kell.

Amennyiben a Vállalkozás a helyesbíteni vagy kiegészíteni kért személyes adatot adatkezelő vagy többes adatkezelés esetén másik adatkezelő részére átadta, haladéktalanul tájékoztatni kell az adatfeldolgozót, illetőleg a másik adatkezelőt az adat helyesbítéséről, illetőleg kiegészítéséről, kivéve ha ez lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatni kell ezen címzettekről.

IV /4. Törléshez (elfeledtetéshez) való jog

Az érintett kérésére a Vállalkozás indokolatlan késedelem nélkül köteles törölni a rá vonatkozó személyes adatokat (törléshez való jog), ha az alábbi indokok valamelyike fennáll:

- a) a személyes adatok kezelésére már nincs szükség abból a célból, amelyből az adatokat kezelték;
- b) hozzájáruláson alapuló adatkezelés esetén hozzájárulását az érintett visszavonja, feltéve, hogy az adatkezelésnek nincs más jogalapja;
- c) az érintett tiltakozik az automatizált adatkezelés ellen, feltéve, hogy nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- d) a Vállalkozás a személyes adatokat jogellenesen kezelte;
- e) a személyes adatokat a Vállalkozásra alkalmazandó nemzeti vagy európai jogszabályban előírt jogi kötelezettség teljesítéséhez törölni kell.

Törlés esetén biztosítani kell, hogy a törölt adat az elektronikus rendszerekben se lehessen visszaállítható.

A törlés megtörténtét jegyzőkönyvezni kell. A jegyzőkönyvet úgy kell kitölteni, hogy abban a törölt személyes adatok ne szerepeljenek (a jegyzőkönyv csak utaljon az adatok körére). A jegyzőkönyvet haladéktalanul el kell juttatni az adatvédelmi tisztviselő részére, aki a törlési jegyzőkönyveket iktatott ügyiratban nyilvántartja.

Amennyiben a törlést az érintett kérte, a törlés megtörténtéről, illetőleg esetleges elutasításáról - az elutasítás indokaival együtt - haladéktalanul, de legkésőbb a kérelem beérkezésétől számított 30 napon belül dokumentált módon értesíteni kell.

Amennyiben a Vállalkozás törölni kért személyes adatot adatkezelő vagy többes adatkezelés esetén másik adatkezelő részére átadta, haladéktalanul tájékoztatni kell az adatfeldolgozót, illetőleg a másik adatkezelőt az adat törléséről, kivéve ha ez lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatni kell ezen címzettekről.

Amennyiben a Vállalkozás korábban nyilvánosságra hozta a személyes adatot, és azt - a GDPR és jelen szabályzat alapján - törölni kell, az elérhető technológia és a megvalósítás költségeinek figyelembe vételével meg kell tenni az ésszerűen elvárható lépéseket - ideérve a technikai intézkedéseket is - annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, hogy az érintett kérelmezte a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését (elfeledtetéshez való jog).

IV /5. Az adatkezelés korlátozásához (zárolásához) való jog

Az érintett kérésére a Vállalkozás haladéktalanul korlátozza az adatkezelést, ha

- az érintett vitatja a személyes adatok pontosságát (a korlátozás arra a legrövidebb időtartamra vonatkozik, amely lehetővé teszi, hogy a Vállalkozás ellenőrizze a személyes adatok pontosságát);
- a Vállalkozás az adatokat jogellenesen kezeli, de az érintett nem kérte azok törlését, csak azok korlátozását;
- a Vállalkozásnak - az adatkezelés céljára figyelemmel - már nincs szüksége a személyes adatokra, de az érintett igényli azokat védendő magánérdekből;
- az érintett tiltakozott az adatkezelés ellen (a korlátozás arra a legrövidebb időtartamra vonatkozik, amely lehetővé teszi, hogy a Vállalkozás ellenőrizze, hogy a Vállalkozás indokai elsőbbséget élveznek-e az érintett jogos érdekeivel szemben).

Korlátozás esetén az adatkezelést ténylegesen végző Vállalkozási szervezeti egység vezetője az adatvédelmi tisztviselővel - és szükség esetén az informatikai rendszer üzemeltetőjével - való konzultációt követően jelöli ki a felelősöket és ad utasítást a korlátozás végrehajtására.

Korlátozás esetén biztosítani kell, hogy a törölt adat az elektronikus rendszerekben is korlátozásra kerüljön.

A korlátozás megtörténtét jegyzőkönyvezni kell. A jegyzőkönyvet úgy kell kitölteni, hogy abban a korlátozás alá eső személyes adatok ne szerepeljenek (a jegyzőkönyv csak utaljon az adatok körére). A jegyzőkönyvet haladéktalanul el kell juttatni az adatvédelmi tisztviselő részére, aki a korlátozási jegyzőkönyveket iktatott ügyiratban nyilvántartja.

Amennyiben a korlátozást az érintett kérte, a korlátozás megtörténtéről, illetőleg esetleges elutasításáról - az elutasítás indokaival együtt - haladéktalanul, de legkésőbb a kérelem beérkezésétől számított 30 napon belül dokumentált módon értesíteni kell.

Amennyiben a Vállalkozás a korlátozni kért személyes adatot adatkezelő vagy többes adatkezelés esetén másik adatkezelő részére átadta, haladéktalanul tájékoztatni kell az adatfeldolgozót, illetőleg a másik adtakezelőt az adat korlátozásáról, kivéve ha ez lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére tájékoztatni kell ezen címzettekről.

IV/6. Adathordozhatósághoz való jog

Az érintett kérésére a Vállalkozás a rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban rendelkezésére bocsátja, feltéve hogy

- az adatkezelés hozzájáruláson vagy szerződésen alapul és
- az adatkezelés automatizált módon történik.

IV/7. Tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozzon személyes adatainak közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladattal kapcsolatos kezelése vagy az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése kapcsán végzett adatkezelés ellen.

Ha a Vállalkozás a tiltakozás megalapozottságát megállapítja, az adatkezelést megszünteti.

Tiltakozás esetén az adat akkor kezelhető tovább, ha a Vállalkozás bizonyítani tudja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival, szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Az érintett tiltakozása esetén - az esetleges elutasítás indokaival együtt - haladéktalanul, de legkésőbb a tiltakozás beérkezésétől számított 30 napon belül dokumentált módon értesíteni kell az érintettet.

IV/8. A felügyeleti hatóságnál való bejelentés joga

A felügyeleti hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

A felügyeleti hatóság

elnevezése: Nemzeti Adatvédelmi és Információszabadság Hatóság;

székhelye: 1125 Budapest, Szilágyi Erzsébet fasor 22/C. ;

telefonszáma: 1/391-1400;

faxszáma: 1/391-1410;

elektronikus levélcíme: ugyfelszolgalat@naih.hu

IV/9. Bírósági jogérvényesítés

Az érintett a Vállalkozás ellen bírósághoz fordulhat, ha megítélése szerint a Vállalkozás, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli.

A perben a Gyulai Törvényszék jár el, de az megindítható az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is.

A Gyulai Törvényszék

székhelye: 5700 Gyula, Béke sgt. 38. ;

telefonszáma: 66/562-200.

V. RÉSZ

EGYES SPECIÁLIS ADATKEZELÉSEKRE VONATKOZÓ SZABÁLYOK

V /1. Személyazonosításra és személyazonosító okmányokra vonatkozó rendelkezések

Az érintettek azonosítására kizárólag a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvényben meghatározott személyazonosság igazolására alkalmas hatósági igazolvány (a továbbiakban: személyazonosító okmány) valamelyikének bemutatásával vagy a személyazonosító jel helyébe lépő azonosítási módokról és az azonosító kódok használatáról szóló 1996. évi XX. törvényben meghatározott valamely azonosítási mód alkalmazásával történhet.

A tizenegy számjegyből álló személyi azonosító törvényi felhatalmazás nélkül még az érintett kifejezett hozzájárulása esetén sem kezelhető.

A szükségesség és az adattakarékosság elvére figyelemmel kizárólag akkor készíthető fénykép vagy másolat személyazonosító okmányról, ha azt jogszabály kötelezően előírja. A másolás előtt fel kell hívni az érintett figyelmét az iratmásolás tényére.

V /2. Kép- és hangrögzítő eszközök használata

Figyelemmel arra, hogy a képmás és a hangfelvétel vonatkozásában is alkalmazni kell a hatályos nemzeti és európai adatvédelmi jogszabályokat; képmás és hangfelvétel rögzítése a Vállalkozási munkavégzés során kizárólag akkor lehetséges, ha annak elkészítése szükséges és arányos, és annak elkészítéséhez az adatkezelő megfelelő joggalappal rendelkezik.

Kép- és hangrögzítő eszköz használata esetén tájékoztatni kell a kép-, illetve hangrögzítés tényéről az érintetteket, vagy - hozzájárulás jogalapja esetén - bizonyítható módon be kell szerezni az érintett hozzájárulását a kép-, illetve hangfelvétel készítéséhez.

A munkavégzés során kép- és hangfelvételt elsősorban a Vállalkozás tulajdonában lévő technikai eszközzel (fényképezőgép, videokamera, diktafon, számítógép, táblagép, mobiltelefon stb.) kell elkészíteni.

Amennyiben a kép-, illetve hangfelvétel nem a Vállalkozás tulajdonában lévő technikai eszközzel (magántulajdonban lévő technikai eszközzel) készül, a lehető legrövidebb időn belül gondoskodni kell a kép-, illetve hangfelvétel Vállalkozási adathordozóra vagy technikai eszközre történő másolásáról, egyidejűleg a magántulajdonban lévő technikai eszközről a kép-, illetve hangfelvételt oly módon kell törölni, hogy az többé ne legyen helyreállítható.

Személyes adatokat tartalmazó kép- és hangfelvétel kizárólag akkor hozható nyilvánosságra, ha ezt jogszabály kifejezetten lehetővé teszi vagy az érintett ahhoz bizonyítható módon előzetesen hozzájárul.

A Vállalkozás tulajdonában lévő kép-, illetve hangrögzítő technikai eszközt az azt használó Vállalkozási munkatárs kizárólag akkor adhat át más részére, ha az eszközön vagy az abba helyezett adathordozón nincs személyes adatokat tartalmazó kép- vagy hangfelvétel.

A személyes adatokat tartalmazó kép-, illetve hangfelvétel kizárólag addig őrizhető meg, amíg az alábbi körülmények mindegyike fennáll:

- a) az adatkezeléshez szükséges jogalap fennáll;
- b) a kép- és hangfelvétel őrzése szükséges és arányos;
- c) az adott ügy ügyiratának selejtezési ideje be nem következik.

A Vállalkozás a személyes vagy online megbeszéléseket (pl. értekezletek, tárgyalások, interjúk) esetenként videó- és/vagy hangfelvétellel rögzíti. A felvételek készítésének célja lehet a megbeszélés dokumentálása, a későbbi visszahallgatás vagy a résztvevők tájékoztatása.

Jogalap

A felvételek készítésének jogalapja a résztvevők önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulása. A hozzájárulást a résztvevők szóban vagy írásban adhatják meg a megbeszélés megkezdése előtt.

Tájékoztatás a felvételtől

A videó- és/vagy hangfelvétellel készítésének tényére az ülést vezető személy vagy a hangfelvételt készítő munkatárs köteles felhívni a jelenlévők figyelmét a megbeszélés megkezdése előtt. A tájékoztatásnak tartalmaznia kell a felvétel célját, a tárolás időtartamát és az érintettek jogait a felvétellel kapcsolatban.

A videó- és/vagy hangfelvétellel készítésének tényét lehetőség szerint a megbeszélés meghívójában is szerepeltetni kell, hogy a résztvevők előre tájékozódhassanak erről.

Az érintettek jogai

A résztvevőknek joguk van:

- **Hozzájárulásukat bármikor visszavonni:** A résztvevők bármikor visszavonhatják hozzájárulásukat a felvétel készítéséhez. Ebben az esetben a felvételt a továbbiakban nem szabad készíteni, és a már elkészült felvételt törölni kell.
- **Hozzáféréshez:** A résztvevők kérhetik a róluk készült felvételhez való hozzáférést, és kérhetik annak másolatát.
- **Helyesbítéshez:** Ha a felvétel pontatlan vagy hiányos, a résztvevők kérhetik annak helyesbítését.
- **Törléshez:** A résztvevők kérhetik a róluk készült felvétel törlését, ha az adatkezelés jogellenes, vagy az érintett érdekei vagy alapvető jogai és szabadságai elsőbbséget élveznek a Vállalkozás jogos érdekeivel szemben.
- **Korlátozáshoz:** A résztvevők kérhetik a róluk készült felvétel kezelésének korlátozását, ha vitatják a felvétel pontosságát, vagy az adatkezelés jogellenes, de a törlést nem kérik.

Adatbiztonság

A Vállalkozás gondoskodik a felvételek biztonságos tárolásáról, és megteszi a szükséges technikai és szervezési intézkedéseket az adatok védelme érdekében. A felvételekhez csak az arra jogosult személyek férhetnek hozzá.

V/3. Telefonbeszélgetések rögzítése

Vállalkozási munkavégzés során telefonbeszélgetést rögzíteni csak indokolt esetben, a telefonbeszélgetésben részt vevő minden fél előzetes tájékoztatását követően lehet.

V/4 A Vállalkozás munkatársairól harmadik személy által készített kép-, illetve hangfelvétel

A Vállalkozás munkatársairól harmadik személyek (pl. fotósok, újságírók) készíthetnek kép- és hangfelvételeket a Vállalkozás nevében vagy a Vállalkozás rendezvényein. A felvételek készítéséhez és felhasználásához a Vállalkozás kéri az érintett munkavállalók hozzájárulását.

A Vállalkozás a felvételeket kizárólag a következő célokra használhatja fel:

- a) **Marketing és promóciós célok:** A vállalkozás arculatának, termékeinek vagy szolgáltatásainak népszerűsítése online platformokon (pl. weboldal, közösségi média), nyomtatott anyagokban (pl. broszúrák, szórólapok) vagy egyéb reklámanyagokban.
- b) **PR és kommunikációs célok:** A vállalkozás tevékenységének, eredményeinek vagy rendezvényeinek bemutatása sajtóközleményekben, cikkekben, interjúkban vagy vállalati prezentációkban.
- c) **Belső kommunikációs célok:** A munkatársak tájékoztatása, motiválása vagy elismerése vállalati hírlevelekben, intranetes oldalakon vagy belső rendezvényeken.
- d) **Oktatási és képzési célok:** A munkatársak szakmai fejlődésének támogatása oktatóanyagokban, tréningeken vagy bemutatókon.
- e) **Dokumentációs célok:** A vállalkozás történetének, rendezvényeinek vagy projektjeinek megőrkítése archív célokra.

A felvételeket a Vállalkozás a cél eléréséhez szükséges ideig, de legfeljebb 5 évig tárolja. A tárolási idő lejártá után a felvételeket törölni kell.

A munkavállalók bármikor kérhetik a róluk készült felvételek törlését vagy korlátozását.

V/5. Elektronikus levéllel (e-mail) kapcsolatos rendelkezések

Figyelemmel arra, hogy a munkavégzés során küldött és kapott elektronikus levelek tartalmaz(hat)nak személyes adatot, és az érkező elektronikus levelek küldőinek, illetve az elküldött elektronikus levelek címzettjeinek az elektronikus levélcíme is személyes adatnak minősül(het), az elektronikus levelek küldése és fogadása során is messzemenőkéig figyelemmel kell lenni a hatályos hazai és uniós adatvédelmi jogszabályok betartására.

Munkavégzésre kizárólag vállalati (...@bcsenergia.hu vagy egyéb, az ügyvezető vagy cégvezető által engedélyezett végződésű) elektronikus levélcím használható.

Abban az esetben, ha a vállalkozás munkatársai több érintett számára küldenek elektronikus levelet, azt úgy kötelesek megtenni, hogy az érintettek egymás – személyes adatnak minősülő – elektronikus levélcímét ne ismerjék meg (az elektronikus levelet külön küldeményként vagy a "titkos másolat" (BCC) funkció, illetve hasonló, az e-mail címek elrejtését biztosító funkció alkalmazásával küldve). Kivételt képez ez alól az érintettek előzetes írásbeli hozzájárulása elektronikus levélcímük megosztásához az adott ügykörben (pl. közös projekt, rendezvény, megbeszélés).

Elektronikus levélben személyes adatot tartalmazó közlemény kizárólag akkor küldhető, ha a munkatárs megbizonyosodott arról, hogy a címzettként megjelölt elektronikus levélcím használója jogosult a közleményben található személyes adatok megismerésére (pl. személyazonosság igazolásával, munkaköri leírás alapján, előzetes megállapodás szerint).

V/6. papírhulladék kezelése

A munkavégzés során keletkező, személyes adatot tartalmazó papírhulladék a „normál” (kommunális) irodai hulladékgyűjtő edényzetbe kizárólag akkor helyezhető, ha azon minden személyes adat - iratmegsemmisítő gép igénybe vételével vagy más módon történő - felismerhetlenné tételéről gondoskodtak.

Amennyiben a személyes adat felismerhetlenné tételéről annak mennyisége miatt vagy bármely más oknál fogva nem lehet gondoskodni, a papírhulladékot elkülönítetten (papírzsákban) kell kezelni, és a csomagoláson (papírzsákon) fel kell tüntetni az iratok bizalmas jellegét. A papírzsákot lezárva kell átadni a megsemmisítést végző Vállalkozási munkatársnak vagy vállalkozónak.

A Vállalkozási papírhulladék megsemmisítésére kizárólag olyan vállalkozóval köthető szerződés, amely teljesíteni tudja a hatályos hazai és uniós adatvédelmi jogszabályokban az adatfeldolgozókra vonatkozó előírásokat.

V /7. Számítástechnikai adathordozó kezelése

Számítástechnikai adathordozó eszközöket (cd, dvd, pendrive, küldő merevlemez, SD kártya stb.) az informatikai biztonsági szabályzatban előírtak, továbbá környezetvédelmi szempontok alapján „normál” (kommunális) hulladékgyűjtő edényzetbe helyezni nem lehet.

Számítástechnikai adathordozó megsemmisítésére kizárólag olyan vállalkozóval köthető szerződés, amely teljesíteni tudja a hatályos hazai és uniós adatvédelmi jogszabályokban az adatfeldolgozókra vonatkozó előírásokat.

A már nem használt, megrongálódott vagy megsemmisítésre szánt eszközöket a számítástechnikai adathordozó megsemmisítésére szerződött vállalkozó részére kell átadni, aki gondoskodik az eszközök megsemmisítéséről, illetőleg az azon tárolt adatok olvashatatlanná tételéről.

VI. RÉSZ

ADATFELDOLGOZÓK

VI/1. Adatfeldolgozók kiválasztása és szerződés-kötés

Az adatfeldolgozók kiválasztásánál a Vállalkozás elsődleges szempontja az adatkezelés biztonsága és az érintettek jogainak védelme. A Vállalkozás kizárólag olyan adatfeldolgozókkal köt szerződést, akik:

- Garanciákat nyújtanak a GDPR követelményeinek való megfelelésre.
- Megfelelő technikai és szervezési intézkedéseket alkalmaznak az adatok biztonsága érdekében.

A Vállalkozás a Google Drive szolgáltatást is igénybe veszi egyes dokumentumok tárolására. A Google, mint adatfeldolgozó a Google általános szerződési feltételei és adatvédelmi szabályzata szerint jár el, amelyek tartalmazzák a GDPR követelményeinek való megfelelésre vonatkozó garanciákat.

Az adatkezelés célja:

- Dokumentumok tárolása és megosztása a Vállalkozás munkatársai között.
- Együttműködés a dokumentumok használata közben.

A kezelt adatok köre:

- A Google Drive-on tárolt dokumentumokban szereplő személyes adatok.

Adatbiztonság:

- A Google Drive szolgáltatás a Google által biztosított biztonsági intézkedéseket alkalmazza az adatok védelme érdekében.

Adattovábbítás:

- A Google Drive szolgáltatás az Európai Unió területén kívülre is továbbíthat adatokat. A Google általános szerződési feltételei tartalmazzák az Európai Unióból az Egyesült Államokba történő adattovábbításra vonatkozó garanciákat, amelyek megfelelnek a GDPR követelményeinek, ideértve a Bizottság (EU) 2023/1795 végrehajtási határozatában (2023. július 10.) foglalt megfelelési határozatot az EU–USA adatvédelmi keretről.

Az érintettek jogai:

- Az érintettek a Vállalkozáshoz fordulhatnak a Google Drive-on tárolt adataikkal kapcsolatos jogaik gyakorlása érdekében (pl. hozzáférés, helyesbítés, törlés).

Felelősség:

A Vállalkozás, mint adatkezelő felelős a Google Drive-on tárolt adatokért, és gondoskodik arról, hogy az adatkezelés megfeleljen a GDPR előírásainak.

VII. RÉSZ

AZ ADATKEZELÉSI NYILVÁNTARTÁS

VII/1. Az adatkezelési nyilvántartás általános szabályai

A Vállalkozás adatkezelési tevékenységéről az adatvédelmi tisztviselő naprakész nyilvántartást vezet. Az adatvédelmi nyilvántartásba szükséges információkat az adatvédelmi tisztviselő kérésére a Vállalkozás szervezeti egységeinek vezetői és a Vállalkozás munkatársai haladéktalanul kötelesek megadni.

VII/2. Az adatkezelési nyilvántartás tartalma

Az adatkezelési nyilvántartás átlátható (táblázatos formában) tartalmazza az alábbi adatokat:

1. az adatkezelő neve, elérhetőségei; közös adatkezelés esetén a közös adatkezelő neve, elérhetőségei;
2. az adatkezelő (és közös adatkezelő) képviselőjének és adatvédelmi tisztviselőjének neve, elérhetőségei;
3. az adatkezelésben közreműködő Vállalkozási szervezeti egység;
4. az egyes adatkezelések célja;
5. a kezelt személyes adatok köre;
6. az adatkezelés jogalapja;
7. azon címzettek köre, akikkel a személyes adatokat közlik vagy közölni fogják;
8. amennyiben lehetséges, az adott adatok törlésére előírányzott határidők;
9. szükség esetén a megfelelő adatbiztonságot szolgáló technikai és szervezési intézkedések általános leírása;
10. egyéb megjegyzések.

VIII. RÉSZ

AZ ADATVÉDELMI INCIDENS

Adatvédelmi incidens esetén az adatkezelési tevékenységet tény legesen végző, illetőleg az adatvédelmi incidenst **észlelő munkatárs vagy vezető** haladéktalanul köteles jelezni az adatvédelmi incidens bekövetkezését felettesén keresztül az **ügyvezetőnek** és közvetlenül az **adatvédelmi tisztviselőnek**.

A **munkatárs** az **adatvédelmi tisztviselő** kérésére haladéktalanul köteles - szükség esetén iratmásolat átadásával - tájékoztatást adni az adatvédelmi incidens körülményeiről

(különösen az érintett személyéről, a kezelt személyes adatok köréről, az adatvédelmi incidenst megvalósító cselekményről vagy mulasztásról, az adatvédelmi incidensről való tudomásszerzés módjáról).

Az **adatvédelmi tisztviselő** a felügyeleti hatóság (**Nemzeti Adatvédelmi és Információszabadság Hatóság**) e célra rendszeresített internetes felületén haladéktalanul, de legkésőbb az incidensnek az adatkezelő tudomására jutásától számított 72 órán belül köteles bejelenteni az adatvédelmi incidenst a felügyeleti hatóság részére, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Az **adatvédelmi tisztviselő** az adatvédelmi incidensről való tudomásszerzést, de legkésőbb az adatvédelmi incidensnek a felügyeleti hatóság részére történő bejelentését követően haladéktalanul köteles javaslatot tenni a szükséges adatvédelmi intézkedések megtételére az **ügyvezető**, valamint az adatkezelést ténylegesen végző **munkatárs** és annak közvetlen felettese részére. Az adatvédelmi tisztviselő szükség esetén az informatikai rendszer üzemeltetőjével, folytatott konzultációt követően tesz intézkedési javaslatot.

Szükség esetén az **adatvédelmi tisztviselő** megfelelő idő elteltével ellenőrzi a javaslata alapján elrendelt intézkedések teljesítését, az adatvédelmi incidensben érintett személyi kör adatainak kezelésére vonatkozó szabályok betartását, és az ellenőrzés tapasztalatairól tájékoztatja az **ügyvezetőt**.

Az **adatvédelmi tisztviselő** az adatvédelmi incidensekről nyilvántartást vezet, amely tartalmazza:

- a) az érintett személyes adatok körét;
- b) az adatvédelmi incidenssel érintettek körét és számát;
- c) az adatvédelmi incidens időpontját;
- d) az adatvédelmi incidens körülményeit, hatásait;
- e) a felügyeleti hatóság értesítésének idejét, illetőleg az értesítés elmaradásának indokolását;
- f) az adatvédelmi incidens orvoslására megtett intézkedéseket;
- g) egyéb megjegyzéseket.

IX. RÉSZ

AZ ADATVÉDELMI TISZTVISELŐ

IX/1. Az adatvédelmi tisztviselő kijelölése és jogállása

Az **ügyvezető** a munkatársak közül adatvédelmi tisztviselőt jelöl ki. Az adatvédelmi tisztviselő olyan köztisztviselő lehet, aki kellően ismeri a Vállalkozás működését, és megfelelő

szintű ismerettel rendelkezik nemzeti és európai adatvédelmi jogszabályok és gyakorlatok terén.

Az adatvédelmi tisztviselő nevét, telefonos elérhetőségét és elektronikus levélcímét kijelölését követően folyamatosan a www.bcsenergia.hu weboldalon (a továbbiakban: Vállalkozás weboldala) elérhetővé kell tenni.

Az adatvédelmi tisztviselő személyének vagy elérhetőségeinek változása esetén a változást haladéktalanul közölni kell a felügyeleti hatósággal.

Az adatvédelmi tisztviselő e minőségében közvetlenül az ügyvezetőnek tartozik felelősséggel, ezen tevékenységével összefüggésben kizárólag az ügyvezető utasíthatja.

Az adatvédelmi tisztviselő más minőségében végzett munkáját úgy kell megszervezni, hogy az adatvédelmi tisztviselő e minőségében végzett feladatait a GDPR és a jelen szabályzat rendelkezéseinek megfelelően maradéktalanul el tudja látni.

IX/2. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselő

- a) folyamatosan figyelemmel kíséri a személyes adatok kezelésével kapcsolatos jogszabályi változásokat, az adatvédelmi jog területét érintő egyedi hatósági és bírósági döntéseket, iránymutatásokat, erről rendszeresen tájékoztatja a Vállalkozás vezetését és szükség esetén a Vállalkozás munkatársait;
- b) szakmai tanácsot ad, segítséget nyújt az adatvédelemmel kapcsolatos jogszabályok értelmezésében a Vállalkozás munkatársai részére;
- c) szükség esetén - különösen a nemzeti, illetőleg európai adatvédelmi jogszabályok vagy jelen szabályzat rendelkezéseinek jelentős változása, továbbá a Vállalkozást érintő jelentős hatáskör- és feladatváltozás, továbbá szervezeti változás esetén - tájékoztatást ad a Vállalkozás munkatársai részére;
- d) az ügyvezetővel történő előzetes konzultációt követően ellenőrzi a GDPR, valamint az egyéb nemzeti és európai jogszabályok személyes adatok kezelésével kapcsolatos rendelkezéseinek betartását és jelen szabályzat hatályosulását;
- e) amennyiben a hatályos nemzeti és európai adatvédelmi jogszabályok szükségessé teszik, javaslatot tesz az ügyvezető részére jelen szabályzat módosítására, egyéb szabályzatok, illetőleg utasítások kiadásra vagy módosítására, előkészíti a kiadásra vagy módosításra kerülő szabályzatok, utasítások tervezetét;
- f) gondoskodik jelen szabályzatnak a Vállalkozási munkatársak részére történő folyamatos elérhetővé tételéről, valamint az adott ügyekben esetlegesen szükséges adatvédelmi tájékoztatók érintettek részére történő elérhetővé tételéről;

- g) szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, az ügyvezető megbízása alapján lefolytatja az adatvédelmi hatásvizsgálatot;
- h) együttműködik az informatikai rendszer üzemeltetőjével az adatvédelem és információbiztonság teljes körű biztosítása érdekében;
- j) vezeti és naprakészen tartja a Vállalkozás adatvédelmi nyilvántartását;
- j) együttműködik a felügyeleti hatósággal;
- k) adatvédelmi incidens esetén haladéktalanul jelenti a felügyeleti hatóságnak az adatvédelmi incidens bekövetkezését, és javaslatot tesz a j) egyező és az adatvédelmi incidensben érintett Vállalkozási szervezeti egység vezetője részére a szükséges intézkedések megtételére;
- l) az érintettek megkeresése esetén előkészíti az érintettek adatvédelemmel kapcsolatos megkereséseire adandó választ;
- m) minden év február 28. napj áig jelentést készít az ügyvezető részére az előző naptári évben elvégzett adatvédelmi tisztviselőként végzett tevékenységéről, tapasztalatairól, és ebben megfogalmazza a nemzeti és európai adatvédelmi jogszabályok hatályosulása érdekében szükséges munkaszervezési és belső szabályozási javaslatait.

X. RÉSZ

Rendszeres felülvizsgálat

A Vállalkozás elkötelezett az adatvédelmi szabályzat betartása és az adatkezelési gyakorlatának folyamatos fejlesztése mellett. Ennek érdekében rendszeres felülvizsgálatokat és auditokat végez az adatkezelési tevékenységeivel kapcsolatban.

Felülvizsgálatok:

Az adatvédelmi tisztviselő évente legalább egyszer felülvizsgálja a jelen szabályzatot és a Vállalkozás adatkezelési gyakorlatát. A felülvizsgálat célja annak biztosítása, hogy a szabályzat és a gyakorlat megfeleljen a hatályos jogszabályoknak és a Vállalkozás tevékenységének.

Korrekciós intézkedések:

A felülvizsgálatok és auditok során feltárt hiányosságok esetén a Vállalkozás haladéktalanul megteszi a szükséges korrekciós intézkedéseket.

Dokumentáció:

A felülvizsgálatok és auditok eredményeit, valamint a megtett korrekciós intézkedéseket dokumentálni kell.

XI. RÉSZ

Adatvédelmi hatásvizsgálat (DPIA)

GDPR 35. cikk

Ha a Vállalkozás olyan új adatkezelést tervez, amely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, adatvédelmi hatásvizsgálatot (DPIA - Data Protection Impact Assessment) kell végezni.

A GDPR szerint DPIA-t kell végezni különösen, ha az adatkezelés:

- új technológiák alkalmazását foglalja magában;
- nagy számban vagy különösen érzékeny adatok kezelésével jár (pl. egészségügyi adatok, bűnügyi adatok);
- az érintettek rendszeres és szisztematikus megfigyelését teszi lehetővé (pl. térfigyelő kamerák használata).

A DPIA folyamata:

1. A tervezett adatkezelés leírása
2. A szükségesség és arányosság értékelése
3. A kockázatok azonosítása és értékelése
4. A kockázatok kezelésére tervezett intézkedések meghatározása
5. Az adatvédelmi tisztviselő bevonása
6. A DPIA dokumentálása

A DPIA eredménye:

A DPIA eredménye alapján a Vállalkozás döntést hoz arról, hogy a tervezett adatkezelést milyen módon hajtja végre, vagy hogy egyáltalán végrehajtja-e.

Felelősség:

A DPIA elvégzéséért és dokumentálásáért az adatvédelmi tisztviselő felelős.

XII. RÉSZ

ZÁRÓ RENDELKEZÉSEK

XII/1. Adatvédelmi oktatás

A **munkatársak** a hatályos hazai és uniós adatvédelmi jogszabályok és jelen szabályzat megismerése céljából a munkavégzésre irányuló jogviszonyuk kezdetétől számított két hónapon belül, valamint kétévente - az adatvédelmi tisztviselő által tartott - adatvédelmi oktatáson kötelesek megjelenni, amelyet az **adatvédelmi tisztviselő** szervez.

XII/2. Hatályba lépés, közzététel

Jelen szabályzat 2024. május 21. napján lép hatályba.

Jelen szabályzat a Vállalkozás informatikai hálózatán, a www.bcsenergia.hu internetes oldalon és a Vállalkozás hirdetőtábláján kerül közzétételre.

Békéscsaba, 2024. május 21.

Kovács Gyula
ügyvezető

Szél Adrián
cégvezető