

Hatályos: 2021. 01. 02. napjától

A Cryptic Consulting Korlátolt Felelősségű Társaság (a továbbiakban: Adatkezelő) belső adatkezelési folyamatainak nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi Adatvédelmi és adatbiztonsági szabályzatot (továbbiakban: Belső Szabályzat) alkotja.

Adatkezelő: Cryptic Consulting Kft.
Székhelye: 6726 Szeged, Pipacs utca 4.
Cégjegyzékszám: 06 09 020983
Adószám: 24856025-2-06
Elektronikus elérhetősége: info@cryptic.hu
Képviseli: Hézső Bence Dániel ügyvezető

Preambulum

A jelen Belső szabályzatot Adatkezelő egyéb szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fenn a jelen Belső szabályzat rendelkezései és a bármely más szabályzat előírásai között, úgy abban az esetben jelen Belső szabályzat rendelkezései az irányadók.

Jelen szabályzat célja, hogy ismertesse az Adatkezelő munkavállalóival, megbízottjaival és a rendszerek felhasználóival a személyes adatok kezelése során érvényesítendő szabályokat és eljárásokat.

Az adatkezelési műveleteket Adatkezelő úgy tervezi meg és hajtja végre, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. A technika mindenkori fejlettségére tekintettel – megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek.

Az Adatkezelő adatfeldolgozó igénybevétele esetén gondoskodik arról, hogy a kiválasztott adatfeldolgozó a személyes adatok védelme érdekében megtegye a szükséges intézkedéseket, valamint kövesse Adatkezelő szabályzatait és egyedi utasításait.

1. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

Adatkezelő célja, hogy biztosítsa az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE 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 (általános adatvédelmi rendelet a továbbiakban: "GDPR") rendelkezéseinek megfelelő adatkezelést.

Jelen Belső szabályzattal Adatkezelő biztosítani kívánja az adatvédelmi nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, továbbá meg kívánja akadályozni a személyes adatokhoz való jogosulatlan hozzáférést, és azok jogosulatlan megváltoztatását, illetve nyilvánosságra hozatalát.

A Belső Szabályzat tárgyi hatálya kiterjed a Társaság minden, jogilag nem önálló szervezeti egységénél folytatott valamennyi olyan folyamatra, amely során a személyes adat kezelése megvalósul.

2. FOGALMAK

A jelen Belső szabályzat fogalmi rendszere megegyezik a GDPR-ban meghatározott értelmező fogalommagyarázatokkal, így különösen:

adatbiztonság: az egyes személyes adatok integritásának és bizalmosságának gyakorlati, informatikai és egyéb technikai jellegű védelme – függetlenül az adat jogi minősülésétől és információtartalmától, továbbá a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége, melyek alapján az adatkezelés kockázati tényezői – és ezzel a fenyegetettség – a szervezési, műszaki megoldásokkal és intézkedésekkel a legkisebb mértékűre csökkenthető

adatkezelés: az alkalmazott eljárástól függetlenül (manuális vagy számítógépen történő adatkezelés) az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése

adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, 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 általa megbízott adatfeldolgozóval végrehajthatja; ha az adatkezelés céljait és eszközeit az uniós vagy a nemzeti jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy nemzeti jog is meghatározhatja

adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi, személyes adatokat kezel

ánnevesítés: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat amely konkrét természetes személyre vonatkozik feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezeti intézkedések megtételével biztosított, hogy az azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni

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, kivéve azon közhatalmi szerveket, amelyek egy egyedi vizsgálat keretében az uniós vagy a nemzeti joggal összhangban férhetnek hozzá személyes adatokhoz, ha az említett adatok e közhatalmi szervek általi kezelése során az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályokat betartják

harmadik fél: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval, vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak

az érintett hozzájárulása: az érintett akaratának önkéntes konkrét és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez;

adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan nyilvánosságra hozatalát vagy azokhoz jogosulatlan hozzáférését eredményezi

genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered

biometrikus adat: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

egészségügyi adat: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

vállalkozás: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat és egyesületeket is.

vállalkozáscsoport: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások.

“felügyeleti hatóság” egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv.

érintett felügyeleti hatóság: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint:

az adatkezelő vagy adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel,

az adatkezelés jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érinthet a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket, vagy

panaszt nyújtottak be az említett felügyeleti hatósághoz.

A személyes adatok határokon átnyúló adatkezelése az unióban megvalósuló olyan adatkezelés, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor, vagy az Unióban megvalósuló olyan adatkezelés, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érinthet érintetteket.

releváns és megalapozott kifogás: azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel, a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlásra jelentett kockázatok jelentőségét.

az információs társadalommal összefüggő szolgáltatások: a 2015/1535/EU Európai Parlamenti és Tanácsi irányelv 1. cikk (1) bekezdésének (b) pontja értelmében vett szolgáltatás.

nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.

statisztikai adat: meghatározott természetes személlyel kapcsolatba nem hozható leíró adat;

személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális, vagy szociális azonosságára jellemző ismeret – valamint az adatból levonható, az érintettre vonatkozó következtetés

“nyilvántartó rendszer”: személyes adat – nyilvántartó rendszer személyes adatok bármely strukturált, funkcionálisan vagy földrajzilag centralizált, decentralizált vagy szétszórt állománya, amely meghatározott ismérvek alapján hozzáférhető

személyazonosító adat: a családi és utónév, leánykori név, a nem, a születési hely és idő, az anya leánykori családi és utóneve, a lakóhely, a tartózkodási hely, a társadalombiztosítási azonosító jel (a továbbiakban: TAJ szám) együttesen vagy ezek közül bármelyik, amennyiben alkalmas vagy alkalmas lehet az érintett azonosítására

az adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

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 helyzetéhez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

3. AZ ADATKEZELÉSEK SZABÁLYAI

Mivel az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, ezért Adatkezelő eljárásai során csak és kizárólag a hatályos jogszabályi előírásoknak megfelelően végez adatkezelést.

Személyes adat kezelésére csak jog gyakorlása vagy kötelezettség teljesítése érdekében, célhoz kötötten van lehetőség. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének. Adatkezelő által kezelt személyes adatok magáncélra való felhasználása tilos.

Adatkezelő személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezel, a cél eléréséhez szükséges minimális mértékben és ideig. Az adatkezelés minden szakaszában meg kell felelnie a célnak – és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerülnek. A törlésről Adatkezelő az adott személyes adatot ténylegesen kezelő munkavállalója által gondoskodik. A törlést a munkavállaló felett munkáltatói jogköröket ténylegesen gyakorló személy és – amennyiben Adatkezelőnél kinevezésre vagy megbízásra került, úgy – a belső adatvédelmi felelős ellenőrizheti. Amennyiben ilyen személy megbízásra vagy kinevezésre kerül, úgy neve és elérhetősége a jelen Belső szabályzat 1. számú mellékletében található.

Adatkezelő személyes adatot csak az érintett előzetes – különleges személyes adat esetén írásbeli – hozzájárulása vagy törvény, illetve törvényi felhatalmazás, vagy szerződéses kötelezettség teljesítése alapján kezel.

Adatkezelő az adat felvétele előtt minden esetben közli az érintettel az adatkezelés célját, valamint az adatkezelés jogalapját.

Adatkezelő szervezeti egységeinél adatkezelést végző alkalmazottak és Adatkezelő megbízásából az adatkezelésben résztvevő, annak valamely műveletét végző szervezetek alkalmazottai kötelesek a megismert személyes adatokat üzleti titokként megőrizni. A személyes adatokat kezelő és az azokhoz hozzáférési lehetőséggel rendelkező személyek kötelesek Titoktartási nyilatkozatot tenni, amelyet a jelen Belső szabályzat 3. számú melléklete tartalmaz.

Ha a Belső szabályzat hatálya alatt álló személy tudomást szerez arról, hogy Adatkezelő által kezelt személyes adat hibás, hiányos vagy elévült, köteles azt helyesbíteni vagy annak helyesbítését az adat rögzítéséért felelős személynél kezdeményezni.

Adatkezelő a vezető tisztségviselője vagy – amennyiben kinevezésre vagy megbízásra került – a belső adatvédelmi felelőse útján nyilvántartást vezet az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából (10. számú melléklet). A nyilvántartás tartalmazza a kezelt személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat. A bekövetkezett adatvédelmi incidensről Adatkezelő az adatvédelmi incidenssel érintett szervezeteket, személyeket értesíti, akikről listát vezet (11. számú melléklet).

Adatkezelő megbízásából adatfeldolgozó tevékenységet végző természetes vagy jogi személyekre, illetve jogi személyiséggel nem rendelkező szervezetekre vonatkozó adatvédelmi kötelezettségeket az adatfeldolgozóval kötött megbízási szerződésben érvényesítendőek. Az adatfeldolgozóval a Adatkezelő a GDPR által előírt Adatfeldolgozó szerződést köt, amely jelen Belső szabályzat 5. számú melléklete. Az egyéb szerződésekbe felveendő adatkezelési pontokat jelen Belső szabályzat 4. számú melléklete tartalmazza.

4. A TÁRSASÁG ADATVÉDELMI RENDSZERE

Adatkezelő mindenkori vezető tisztségviselője Adatkezelő sajátosságainak figyelembe vételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységekre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt.

A Belső szabályzatban előírtak betartatásáért a feladatkörében minden érintett szervezeti egység vezetője felelős.

Adatkezelő munkatársai munkájuk során gondoskodnak arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, és megsemmisíthető.

Adatkezelő adatvédelmi rendszerének felügyeletét a vezető tisztségviselő látja el.

A vezető tisztségviselő az adatvédelemmel kapcsolatosan:

- felelős az érintettek a Rendeletben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
- felelős a Társaság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
- felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
- vizsgálatot rendelhet el;
- kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait.

5. ADATBIZTONSÁGI SZABÁLYOK

Fizikai védelem

A papíralapon kezelt személyes adatok biztonsága érdekében Adatkezelő az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyónvédelmi berendezéssel ellátott helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékes személyek férhetnek hozzá;
- Adatkezelő adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- a Társaság adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági rendelkezéseket alkalmazza a Társaság.
- Amennyiben a papíralapon tárolt személyes adat kezelésének célja megvalósult, úgy Adatkezelő intézkedik a papír megsemmisítéséről. Ebben az esetben Adatkezelő kijelöl egy munkavállalót, aki a megsemmisítésért felelős. A megsemmisítésért felelős munkavállaló a megsemmisítéssel érintett szervezeti egység bevonásával állítja össze a megsemmisítendő iratcsomagot. A megsemmisítésen háromtagú megsemmisítési bizottság köteles részt venni. A megsemmisítésről jegyzőkönyvet kell felvenni. A bizottság tagjai személyesen ellenőrzik, hogy valóban azok az iratok kerülnek megsemmisítésre, amelyeket a jegyzőkönyvben feltüntettek.
- Amennyiben a személyes adatok adathordozója nem papír, hanem más fizikai eszköz, úgy a fizikai eszköz megsemmisítésére a papíralapú adatkezelésre vonatkozó megsemmisítés szabályai irányadóak.

Informatikai védelem

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében Adatkezelő, összhangban a hatályos belső informatikai rendelkezések előírásaival, az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezelés során használt számítógépek Adatkezelő tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír Adatkezelő;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről Adatkezelő rendszeresen, illetve indokolt esetben gondoskodik;
- az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a hálózaton tárolt adatok biztonsága érdekében a szerveren folyamatos tükrözéssel kerüli el a Adatkezelő az adatvesztést;

- a személyes adatokat tartalmazó adatbázisok aktív adataiból mágneses adathordozóra napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik;
- a lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncéldobozban tűzbiztos helyen és módon tárolt;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

Szerverek biztonsága

A Társaság által kezelt személyes adatok áramlását elektronikus módon szerverek segítségével valósítják meg, fizikai tárolásukat pedig adattárolók segítségével. Mind az adattárolókat mind pedig a szervereket külön erre a célra kialakított helyiségben kell elhelyezni.

Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetők legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. Ezen adatok naprakészége nagymértékben hozzásegíti Adatkezelőt a tőle elvárt, illetve általa elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében Adatkezelő az alábbi jogosultságkezelési előírásokat, alapelveket alkalmazza:

- Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján az informatikáért felelős személy végzi
- A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.
- El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására nem igényt tartó személyek.
- Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az adatkezelő vezető tisztségviselője vagy akadályoztatása esetén helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.
- Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

Jogosultságkezelési folyamat

Az informatikáért felelős személy minden esetben konzultál a megrendelő lapon szereplő jogosultság megadásáról vagy módosításáról annak indokoltságának tekintetében a jogosultság birtokosával és az igénylő feletti munkáltatói jog gyakorlójával. A jogosultság megadásával vagy módosításával kapcsolatosan a vezető tisztségviselőnek és az igénylő feletti munkáltatói jog gyakorlójának vétőjoga van.

A megszületett döntést követően az informatikáért felelős személy által kijelölt munkatárs beállítja a jogosultságokat, amelyről visszaigazolást küld az igénylő felé.

A jogosultság birtokosának munka vagy egy jogviszonya megszűnésével közvetlen felettesének kötelessége értesíteni az informatikáért felelős személyt, valamint a munkáltatói jogok gyakorlóját a jogosult eddig birtokolt jogosultságainak törlése érdekében.

A jogosultság megszűnése esetén a jogosult felettese a megszüntetési kérelmet elektronikus módon vagy papír alapon a jogosultságkezelési megrendelőlapra küldi meg az informatikáért felelős személynek, aki gondoskodik a jogosultság törléséről. Ezt követően az informatikáért felelős személy vagy az általa megbízott munkatárs visszajelzést küld a törlést kezdeményezőnek.

Áthelyezés esetén a korábbi munkakör feletti munkáltatói jogokat gyakorló felettes és az új munkakör feletti munkáltatói jogokat gyakorló felettes egyetemlegesen kötelesek gondoskodni a régi jogosultságok törlésének, módosításának vagy új jogosultságok felvételének kezdeményezéséről.

Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

6. AZ ÉRINTETTEK JOGAINAK ÉRVÉNYESÍTÉSE

Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését Adatkezelő feltüntetett elérhetőségein.

Adatkezelő a beérkezett kérelmet, illetve tiltakozást köteles a beérkezéstől számított három napon belül áttenni az adatkezelés szempontjából feladat- és hatáskörrel rendelkező szervezeti egység vezetőjéhez.

A feladat- és hatáskörrel rendelkező szervezeti egység vezetője az érintett személyes adatának kezelésével összefüggő kérelmére az érkezésétől számított legkésőbb 30 – tiltakozási jog gyakorlása esetén 15 – napon belül írásban, közérthető formában választ ad.

A tájékoztatás kiterjed a GDPR 13 és 14. cikk szerinti tájékoztatás szerinti információkra és a 15-22. és 34. cikk szerinti tájékoztatásra.

A tájékoztatás főszabály szerint ingyenes, költségtérítést Adatkezelő csak a GDPR 12. cikk (5) bekezdésében meghatározott esetben számíthat fel.

Adatkezelő kérelmet csak a GDPR. 23. cikkben meghatározott okokból utasít el, erre csak indoklással, a rendeletben meghatározott tájékoztatással, írásban kerül sor.

A valóságnak nem megfelelő adatot az adatot kezelő szervezeti egység vezetője – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – helyesbíti, a GDPR 16. cikk szerint, meghatározott okok fennállása esetén intézkedik a kezelt személyes adat törlése iránt.

Az érintett személyes adatának kezelése elleni tiltakozásának elbírálási időtartamára – de legfeljebb 5 napra – az adatkezelést az adatkezelést végző szervezeti egység vezetője felfüggeszti, a tiltakozás megalapozottságát megvizsgálja és döntést hoz, amelyről a kérelmezőt írásban tájékoztatja.

Adatkezelő az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével másnak okozott kárt, illetve az általa vagy az általa igénybe vett adatfeldolgozó által okozott személyiségi jog megsértése esetén jogerősen megítélt sérelemdíjat is megtéríti. Az adatkezelő mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának megsértését az adatkezelés körén kívül eső elháríthatatlan ok idézte elő. Ugyanígy nem téríti meg a kárt, amennyiben az a károsult szándékos vagy súlyosan gondatlan magatartásából származott.

Az érintett jogorvoslati lehetőséggel, illetve panasszal élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (1024 Budapest, Szilágyi Erzsébet fasor 22/C.) vagy lakóhelye vagy tartózkodási helye szerint illetékes törvényszéknél.

7. A TÁRSASÁGNÁL MEGVALÓSULÓ ADATKEZELÉSEK

Az adatkezelések helye: 6726 Szeged, Pipacs utca 4.

Kezelt adatok köre:

- Szolgáltatás igénybevétele során kezelt adatok
- Számlázási adatok
- Munkaügyi adatkezelés

8. PANASZKEZELÉS

Az ügyfél az Adatkezelő illetve az Adatkezelő érdekében vagy javára eljáró személynek a szolgáltatással közvetlen kapcsolatban álló magatartására, tevékenységére vagy mulasztására vonatkozó panaszát szóban, vagy írásban közölheti az Adatkezelővel.

Szóbeli panasz

A szóbeli panaszt azonnal meg kell vizsgálni, és szükség szerint orvosolni kell.

Ha az ügyfél a panasz kezelésével nem ért egyet, vagy a panasz azonnali kivizsgálása nem lehetséges, az Adatkezelő a panaszról és az azzal kapcsolatos álláspontjáról haladéktalanul köteles jegyzőkönyvet felvenni, és annak egy másolati példányát:

* személyesen közölt szóbeli panasz esetén helyben az ügyfélnek átadni,

telefonon vagy egyéb elektronikus hírközlési szolgáltatás felhasználásával közölt szóbeli panasz esetén a fogyasztónak legkésőbb 30 napon belül köteles érdemi válasszal egyidejűleg megküldeni.

A panaszról felvett jegyzőkönyvnek tartalmaznia kell az alábbiakat:

az ügyfél neve, lakcíme,

a panasz előterjesztésének helye, ideje, módja,

az ügyfél panaszának részletes leírása, az ügyfél által bemutatott iratok, dokumentumok és egyéb bizonyítékok jegyzéke,

az Adatkezelő nyilatkozata az ügyfél panaszával kapcsolatos álláspontjáról, amennyiben a panasz azonnali kivizsgálása lehetséges,

a jegyzőkönyvet felvevő személy és – telefonon vagy egyéb elektronikus hírközlési szolgáltatás felhasználásával közölt szóbeli panasz kivételével – az ügyfél aláírása,

a jegyzőkönyv felvételének helye, ideje,

telefonon vagy egyéb elektronikus hírközlési szolgáltatás felhasználásával közölt szóbeli panasz esetén a panasz egyedi azonosítószáma.

Az írásbeli panaszt az Adatkezelő – ha az Európai Unió közvetlenül alkalmazandó jogi aktusa eltérően nem rendelkezik – a beérkezését követően 30 napon belül köteles írásban érdemben megválaszolni és intézkedni annak közlése iránt. A panaszt elutasító álláspontját az Adatkezelő indokolni köteles.

A válaszadási határidő helyszíni vizsgálat vagy valamely hatóság megkeresésének szükségessége esetén egy alkalommal legfeljebb tizenöt nappal meghosszabbítható.

A válaszadási határidő meghosszabbításáról és annak indokáról a bejelentőt írásban, a válaszadási határidő letelte előtt tájékoztatni kell.

Az Adatkezelő vezetője, illetve az általa megbízott ügyintéző a panaszt (bejelentőt) meghallgathatja, ha a panasz, illetve bejelentés kivizsgálása azt szükségessé teszi.

Az Adatkezelő a panaszról felvett jegyzőkönyvet és a válasz másolati példányát öt évig köteles megőrizni, és azt az ellenőrző hatóságoknak kérésükre bemutatni.

A panasz elutasítása esetén az Adatkezelő köteles az ügyfelet írásban tájékoztatni arról, hogy panaszával – annak jellege szerint – mely hatóság vagy a békéltető testület eljárását kezdeményezheti.

Meg kell adni az illetékes hatóság, illetve az Adatkezelő székhelye szerinti békéltető testület levelezési címét.

Írásbeli panasz

Postai úton: 6726 Szeged, Pipacs utca 4.

Emailen: info@cryptic.hu

Írásbeli panasz esetén a panasz elbírálásához szükséges a konkrét ügy pontos leírása, több kifogás esetén azok, illetve indokaik elkülönített rögzítése, továbbá a határozott igény megjelölését és a panaszban foglaltakat alátámasztó dokumentumok másolatát is mellékelni kell a beadványhoz. Amennyiben a panaszban voltak előzményei, az ezekkel kapcsolatos információkat is meg kell adni.

Az írásbeli panasz érvényességi kelléke a bejelentő aláírása. Az írásbeli panasz képviselő vagy meghatalmazott útján való benyújtása esetén, a panaszkérelemnél a meghatalmazottként eljáró természetes személy nevét is fel kell tüntetni, továbbá a kérelemhez csatolni kell a meghatalmazott aláírásával ellátott – legalább két tanú által aláírt, illetve saját kezűleg írt és aláírt – eredeti meghatalmazást.

Írásbeli panasz esetén az Adatkezelő a panaszügyet érdemben megvizsgálja és a panasszal kapcsolatos álláspontját és érdemi döntését/intézkedését pontos indoklással ellátva, a panasz közlését követő 3 napon belül írásban megküldi a bejelentő részére.

Az Adatkezelő a panaszkezelés során igyekszik a legrövidebb határidők betartásával eljárni és biztosítja, hogy döntése során a hatályos jogszabályok szerint vizsgálja ki, orvosolja, vagy utasítsa el a panaszt. Panaszügyben hozott döntését közérthetően és egyértelműen indokolva, valamennyi felvetett problémára reagálva küldi meg a bejelentő részére.

Az Adatkezelő a panaszkezelés során különösen az alábbi adatokat kérheti az ügyféltől:

- neve;
- ügyfélszám;
- lakcíme, székhelye, levelezési címe;
- telefonszáma;
- értesítés módja;
- panasszal érintett szolgáltatás
- panasz leírása, oka;
- panaszos igénye;
- a panasz alátámasztásához szükséges, az ügyfél birtokában lévő olyan dokumentumok másolata, amely a szolgáltatónál nem áll rendelkezésre;
- meghatalmazott útján eljáró ügyfél esetében érvényes meghatalmazás;
- a panasz kivizsgálásához, megválaszolásához szükséges egyéb adat.

A panaszt benyújtó ügyfél adatait a GDPR rendelkezéseinek megfelelően kell kezelni.

adatkezelés célja: panaszok rögzítése, kivizsgálása, elbírálása

kezelt adatok köre: az ügyfél neve; lakcíme, levelezési címe, a panasz előterjesztésének helye, ideje, módja, az ügyfél panaszának részletes leírása, az ügyfél által bemutatott iratok, dokumentumok és egyéb bizonyítékok és azok jegyzéke, a jegyzőkönyvet felvevő személy és a személyesen közölt szóbeli panasz esetén az ügyfél aláírása, a jegyzőkönyv felvételének helye, ideje, az ügyféllel való kapcsolattartási e-mail cím, telefonszám.

adatkezelés jogalapja: a Rendelet szerinti érintetti hozzájárulás a fogyasztóvédelemről szóló 1997. évi CLV. törvény 17/A-C. §-ban meghatározott jogalappal adattárolás határideje: a Társaság a panaszról felvett jegyzőkönyvet és a válasz másolati példányát öt évig megőrzi [Fgytv. 17/A. § (7) és 17/B. § (3)].

adattárolás módja: elektronikusan és papíralapon

9. ADATFELDOLGOZÁS, ADATTOVÁBBÍTÁS

Adatkezelő Adatfeldolgozónak adott utasításainak jogszerűségéért az Adatkezelő felel. Adatkezelő Adatfeldolgozónak csak írásban adhat utasítást.

Adatfeldolgozó az Adatkezelő rendelkezése szerint vehet igénybe további adatfeldolgozót.

Adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az Adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

Adatfeldolgozó köteles Adatkezelő Adatvédelmi és adatbiztonsági szabályozásának előírásait betartani, az abban foglaltak szerint ellátni az adatkezeléshez kapcsolódó feladatát.

Adatfeldolgozó köteles Adatkezelő Adatvédelmi és adatbiztonsági szabályozásának előírásai szerinti adatbiztonsági követelményeket betartani.

10. FELELŐSSÉG

Amennyiben Adatfeldolgozó tevékenységének ellátása során a szolgáltatási szerződés előírásainak betartásával jár el, úgy Adatfeldolgozó tevékenységéért Adatkezelő úgy felel, mintha maga járt volna el. Amennyiben Adatfeldolgozó tevékenységével kárt okoz az érintettnek vagy harmadik személynek, úgy az érintett vagy harmadik személy felé helytállási kötelesség Adatkezelőt terheli.

Amennyiben Adatfeldolgozó túlterjeszkedi a szolgáltatási szerződésben meghatározott jogain, az adott túlterjeszkedésre vonatkozóan önálló adatkezelővé válik, és Adatkezelőnek, az érintettnek vagy harmadik személynek okozott kárért a károkozás általános szabályai szerint köteles helytállni.

Adatkezelővel szemben Adatfeldolgozó a teljes tevékenységének ellátásáért kártérítési felelősséggel tartozik, így különösen az elektronikus másolat szervezeti aláírással való ellátásáért, a tartalmi megfelelésért, valamint az Adatfeldolgozó által tárolt elektronikus másolatok folyamatos rendelkezésre állásáért.

Felek a szolgáltatási szerződés megsértéséből eredő, egymásnak okozott valamennyi vagyoni és nem vagyoni kárt a másik fél részére teljes mértékben kötelesek megtéríteni.

11. ADATVÉDELMI INCIDENS KEZELÉS

A jelen szabályzat hatály alá tartozó személyek, bármely, az Adatkezelő által vagy közreműködésével működtetett informatikai rendszer esetében haladéktalanul, de legkésőbb 12 órán belül kötelesek jelenteni az adatvédelemért felelős személy számára, ha adatvédelmi incidens gyanúja merül fel, vagy, ha biztos tudomása van arról, hogy adatvédelmi incidens történt.

A bejelentést elsősorban munkaidőben, telefonon keresztül kell megtenni, amelyet az adatvédelemért felelős személy kérésére elektronikus levél formájában is meg kell erősíteni.

Adatvédelmi incidens során alkalmazandó eljárásrend

Az adatvédelemért felelős személy és az egyéb érintett személyek a számukra jelzett, vagy saját hatáskörükben megállapított adatvédelmi incidens felderítése és súlyosságának megállapítása érdekében a jelen fejezetben foglaltak szerint kötelesek eljárni.

Adatvédelmi incidens kezelésének eljárása:

Az adatvédelemért felelős személy felveszi a kapcsolatot az adatvédelmi incidenssel érintett informatikai rendszer rendszergazdájával (amennyiben az incidens informatikai rendszert is érint).

Az adatvédelemért felelős személynek a felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

Alacsony szintű adatvédelmi incidens: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékos, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset estén.

Közepes szintű adatvédelmi incidens: a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékos, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset estén.

Magas szintű adatvédelmi incidens:

a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékos, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset estén, illetve az adatok körétől függetlenül minden olyan eset, amikor az incidensnek az érintettre hátrányos hatása valószínűsíthető, vagy a hátrányos következmény bekövetkezés mértéke biztos.

Alacsony szintű adatvédelmi incidens esetén az adatvédelemért felelős személy:

az érintett rendszer rendszergazdájával (amennyiben az incidens informatikai rendszert is érint) meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába.

Közepes szintű adatvédelmi incidens esetén:

az adatvédelemért felelős személy haladéktalanul, de legkésőbb 12 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személyön kívül a rendszergazda (amennyiben az incidens informatikai rendszert is érint) és Adatkezelő vezetője,
a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
az adatvédelemért felelős személy rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában.

Magas szintű adatvédelmi incidens esetén

az adatvédelemért felelős személy haladéktalanul, de legkésőbb 12 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személyön kívül a rendszergazda (amennyiben az incidens informatikai rendszert is érint) és Adatkezelő vezetője,
a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá amennyiben szükséges, meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről.

az adatvédelemért felelős személy rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában.

Az Adatkezelő az adatvédelemért felelős személy útján az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekről nyilvántartást vezet, amely tartalmazza az adatvédelmi incidenssel érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Amennyiben az érintett ezt kéri, az adatvédelemért felelős személy tájékoztatást ad az érintett személyes adatára is kiterjedő adatvédelmi incidensekkel kapcsolatban.

Tárhelyszolgáltató

Név: Rackforest Kft.

Levelezési cím: 1132 Budapest, Victor Hugo u. 18-22.

E-mail cím: info@rackforest.hu

Telefonszám: +36 1 211 0044