

1. sz. melléklet

I. Alkalmazási kör

Az általános adatvédelmi rendelet (GDPR) értelmében bármely jogalany, amely akár saját maga részére, akár más részére személyes adatot gyűjt, dolgoz fel, vagy használ fel, köteles meghozni azokat a technikai és szervezeti intézkedéseket, amelyek szükségesek a törvényben foglalt adatvédelmi szabályok betartásának biztosításához. Jelen dokumentum felsorolja azokat a biztosítékokat, amelyeket a Társaság a GDPR 28. Cikkének értelmében bevezetett.

II. Adatvédelmi intézkedések a Társaságnál

1. Kötelezettségek

1.1. A Társaság köteles megtenni valamennyi célú és jogalapú adatkezelése, adatfeldolgozása vonatkozásában azokat a technikai és szervezési intézkedéseket és eljárási szabályokat a személyes adatok biztonsága érdekében, amelyek biztosítják, hogy a felvett, tárolt, illetve kezelt adatok védettek legyenek a véletlen vagy jogellenes megsemmisítés, elvesztés, megváltoztatás, sérülés, jogosulatlan nyilvánosságra hozatal vagy az azokhoz való jogosulatlan hozzáférés ellen. Jelen kötelezettségvállalást Adatkezelő az adatkezelési tevékenységben részt vevő összes munkavállalója részére előírja.

A Társaság kötelezi továbbá magát arra is, hogy minden olyan harmadik felet, akiknek az adatokat az Érintettek hozzájárulása alapján továbbítja vagy átadja, felszólítja, hogy eleget tegyenek az adatbiztonság követelményének.

1.2. A Társaság által kezelt adatokat kizárólag Adatkezelő, valamint alkalmazottai, illetve az általa igénybe vett adatfeldolgozó(k) ismerhetik meg, azokat Adatkezelő harmadik, az adat megismerésére jogosultsággal nem rendelkező személynek nem adhatja át.

2. Alkalmazott biztonsági intézkedések

2.1. Az Adatkezelő a személyes adatok kezeléséhez a szolgáltatás nyújtása során alkalmazott informatikai környezetet oly módon biztosítja, hogy

- az érintett által megadott személyes adatokat csak és kizárólag a jelen szabályzatban meghatározott adatokkal és módon kapcsolja össze,
- gondoskodik arról, hogy a személyes adatokhoz az Adatkezelőnek csak olyan munkatársai férjenek hozzá, akiknek ez munkaköri kötelezettségükből fakadó feladatuk ellátásához elengedhetetlenül szükséges,
- az adatokról biztonsági mentés készül.

2.2. Az Adatkezelő az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

- A jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver és hardver eszközök védelméről, illetve a fizikai védelemről (hozzáférés védelem, hálózati védelem);
- Az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről



ADATFELDOLGOZÓI MEGÁLLAPODÁS

(tükrözés, biztonsági mentés);

- Az adatállományok vírusok elleni védelméről (vírusvédelem);
- Az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról (archiválás, tűzvédelem)

2.3. Digitális adatkezelés:

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az Adatkezelő az alábbi intézkedéseket alkalmazza:

- minden, az adatkezelés során használt számítógép a Társaság tulajdonát képezi, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír;
- a számítógéphez és az azon elérhető adatokhoz csak érvényes azonosítható jogosultsággal (az Érintett nevével és egyedi jelszóval) lehet hozzáférni; a hozzáférést biztosító jelszavak rendszeresen lecserélésre kerülnek;
- a Társaság hálózati kiszolgáló gépén (szerver) tárolt adatokhoz csak érvényes, és megfelelő jogosultsággal lehet hozzáférni; minden adathoz csakis az annak kezelésére kijelölt személyek férhetnek hozzá, egyben a rendelkezésre álló informatikai eszközök alkalmazásával meggátolja, hogy esetlegesen illetéktelen személyek hozzáférjenek a szerverhez, hálózathoz;
- Társaság az adatok biztonságos tárolása érdekében a szerveren folyamatos tükrözéssel előzi meg az esetleges adatvesztést, emellett Társaság a központi szerver teljes adatállományára vonatkozóan napi, valamint plusz heti mentést is végez mágneses adathordozóra (a lementett adathordozó az erre kialakított és rendszeresített helyen és módon kerül biztonságos tárolásra);
- az adatokat tartalmazó fájlok az adatkezelés céljainak teljesülését követően, illetve ha adatkezelés határideje lejárt, jogalapja megszűnt visszaállíthatatlanul törlésre kerülnek;
- Társaság gondoskodik a hálózat folyamatos és hatékony vírusvédelemről.

2.5. Papíralapú dokumentumkezelés:

A papíralapon tárolt és kezelt személyes adatok megfelelő biztonsága érdekében a Társaság az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg; az aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá,
- az adatkezelést végző munkatárs kiemelten odafigyel arra, hogy az adatkezelési helyiségeket úgy hagyja el a munkavégzés során, hogy a kezelt dokumentumokat elzárja, illetve az adathordozót lezárja, amennyiben releváns az irodát bezárja; a munkavégzés befejeztével pedig a papíralapú adathordozót előírás szerűen elzárja;
- amennyiben Megbízótól papíralapon kapott személyes adatok Társaság által digitalizálásra kerülnek, a továbbiakban a digitálisan kezelt és tárolt dokumentumokra irányadó biztonsági szabályokat köteles rá alkalmaznia a munkavállalónak;
- Társaság a dokumentumokat jól zárható, tűzvédelmi és vagyonvédelmi berendezésekkel felszerelt, papíralapú dokumentumok tárolására alkalmas, száraz helyiségben tárolja.



Member of Russell Bedford International – a global network of independent professional services firms

Cím: 1117 Bp, Fehérvári út 50-52. | Tel: (+36) 1 33 44 279 | Fax: (+36) 1 29 90 474 | Web: www.icteuropa.hu

2.6. Fizikai belépés ellenőrzése - elektronikus beléptető rendszer:

- Munkaadó a személy- és vagyonvédelem érdekében elektronikus beléptetőrendszert alkalmaz Társaság székhelyén.
- A belépőkártyához a Munkavállaló nevét és a kártya számát rendelik hozzá, illetve a belépőkártyával kapcsolatban beállításra kerül az adott Munkavállalóhoz kapcsolódó belépési jogosultság.
- Az elektronikus beléptetőrendszer az alábbi adatokat rögzíti és kezeli (naplózza): melyik Munkavállaló, mikor, melyik be-, illetve kilépési ponton használja a kártyáját.

2.7. Munkavállalók által használt vállalati informatikai eszközök ellenőrzése:

A munkavállalók rendelkezésére bocsátott vállalati informatikai eszközöket -Munkavállaló előzetes tájékoztatása mellett – a Társaság IT részlege az adatbiztonság érdekében rendszeresen ellenőrzi.

3. Adatkezelő az adatbiztonság feltételeinek érvényesítése érdekében gondoskodik az érintett Munkatársak megfelelő felkészítéséről; meglévő és újonnan felvett Munkavállalói számára folyamatos oktatást biztosít az adatbiztonsági feladatok, ismeretek kapcsán.

4. Adatkezelő az általa kezelt adatok biztonsága érdekében alkalmazott intézkedések meghatározásakor figyelembe veszi a technika mindenkori aktuális fejlettségét és annak megfelelően gondoskodik informatikai rendszerének felülvizsgálatáról.

Budapest, 2018. május



Member of Russell Bedford International – a global network of independent professional services firms

Cím: 1117 Bp, Fehérvári út 50-52. | Tel: (+36) 1 33 44 279 | Fax: (+36) 1 29 90 474 | Web: www.icteuropa.hu