Properon Kft

1148 Budapest, Lengyel utca 15.
Tel.: 06/1 470-80-40 Fax: 06/1 470-80-45
E-mail: info@properon.hu

ADATVÉDELMI SZABÁLYZAT

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 szóló (általános adatvédelmi rendelet - GDPR) előírásai, valamint az információról szóló 2011.évi CXII. törvény (Infotv) előírásainak alapján jelen szabályzat rögzíti Társaságunk feladatait a megfelelő adatkezelés érdekében.

Társaságunk elkötelezett, hogy olyan összetett és biztonságos informatikai környezetet alakítson ki és működtessen, olyan védelmi képességekkel rendelkező, megfelelő technikai eszközöket vegyen igénybe, és olyan szervezeti-szervezési intézkedéseket hajtson végre, amelyek segítségével kellő biztonsággal, ugyanakkor rugalmassággal, működési környezetének, jogszabályi előírásokból fakadó kötelezettségeinek eleget téve tudja kezelni a rábízott és saját információkat, amelyekkel biztosítani tudja az adatkezelésével érintett természetes személyeknek a személyes adatkezelése során az előírt és elvárható védelmét.

Fentiek alapján Társaságunk az alábbi szabályozással, intézkedésekkel biztosítja a személyes adatok kezelésének bizalmasságának, integritásának rendelkezésre állását és megbízhatóságát.

1. Általános rendelkezések (hatály, értelmező rendelkezések)

1.1 Adatkezelési szabályzat hatálya az IBSZ hatályával egyezik.

1.1.1 Szervezeti hatály

A Szabályzat hatálya kiterjed Társaságunk valamennyi szervezeti egységére, továbbá a velünk szerződéses jogviszonyban álló valamennyi szervezetre, amelynek munkavállalói, vagy alvállalkozói, netán általuk megbízott személyek az általunk által használt rendszerekhez, illetve az azokon tárolt adatokhoz hozzáféréssel rendelkeznek. Kötelességünk, hogy ezen szervezeteknek legyen módjuk a rájuk vonatkozó elvárások és kötelezettségek megismerésére.
Szabályzatunkban foglaltak érvényre juttatása érdekében a szabályozás előírásainak betartását minden olyan külső partnerrel kötött szerződésben és megállapodásban kötelezően elő kell írni, amelynek keretében a külső partner (beleértve annak munkavállalóit, alvállalkozóit, illetve az általa meghívott személyeket) a szabályozás hatálya alá eső helyen munkát végez, szállít vagy Társaságunk adataival, adatállományaival, rendszereivel, hálózatával, illetve hálózati eszközeivel bármiféle közvetlen, vagy közvetett kapcsolatban áll.

1.1.2 Személyi hatály

Az elfogadott Adatvédelmi Szabályzat vonatkozik:

- Társaságunk valamennyi alkalmazottjára,
- közreműködő munkatársainkra (akár milyen foglalkoztatási jogviszonyban, akár eseti jelleggel is állnak), képviselőnkre, vezetőinkre,
- a velünk szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás, vagy titoktartási

nyilatkozatok alapján, továbbá az alkalmazott rendszerek felhasználóira, fejlesztőire, üzemeltetőire.

Az Adatvédelmi Szabályzat előírásainak érvényesülését a szerződések tartalmának megfelelő kialakításával kell biztosítani és megvalósítani.

1.1.3 Tárgyi hatály

Jelen Adatvédelmi Szabályzat tárgyi hatálya kiterjed a Társaságunk által használt valamennyi rendszerre, ezen belül kiemelten minden olyan informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a Társaságunknál keletkező, illetve felhasznált érintett (személyes) adatokat, információkat.

1.2 Érvényesség és kötelező felülvizsgálat rendje

Jelen Adatvédelmi Szabályzat elfogadásától a következő változat elfogadásáig marad érvényben.

Szabályzatunk felülvizsgálatára az alábbiak szerint kerül sor:

- évente egy alkalommal, a belső felülvizsgálatok során,
- minden olyan esetben, amikor a leírtakhoz képest jelentős változás történik.

A mindenkori felülvizsgálat végrehajtása az Informatikai vezető, és az adatvédelmi megbízott közös feladatát jelenti, munkájukat az ügyvezető hagyja jóvá.

1.3 Kapcsolódó dokumentumok

Jelen Adatvédelmi Szabályzat alapját képező dokumentumok:

- EU rendelet 1.sz. melléklet
- AIM iránymutatás 2.sz. melléklet
- Társaságunkra vonatkozó EU cikkek rövid bemutatása 3-sz. melléklet

2. Informatikai biztonsági politika

2.1. informatikai biztonsági politika

Társaságunk vezetése elkötelezi magát a szervezetünk informatikai rendszerei által kezelt információvagyon

- bizalmasságának
- hitelességének
- sértetlenségének
- rendelkezésre állásának
- és funkcionalitásának megőrzésére és fenntartására,

ennek érdekében szükséges informatikai biztonsági döntéseket meghozza, minden érdemi intézkedést megtesz, a biztonságos rendszer működéséhez szükséges erőforrásokat biztosítja, a végrehajtást ellenőrzi.

2.2. Informatikai biztonsági kockázatkezelés:

Az informatikai és adatvédelmi intézkedéseinkkel minden esetben arra törekszünk, hogy azok

- teljes körűek legyenek, azaz a rendszer összes elemére kiterjednek,
- zártak, azaz minden észszerűen, elvárhatóan előrelátható fenyegetést figyelembe vegyenek,
- folytonosak legyenek, azaz a változó körülmények és követelmények mellett is megszakítás nélkül megvalósuljanak.

Ennek érdekében szükséges lépések nem teljes körű felsorolása:

- biztonsági mentések titkosítása
- szünetmentes tápegységek
- adatbázisok vizsgálata

- WiFi hálózat fejlesztése, biztonság növelése
- Adatszivárgás elleni védelem (DLP) kialakítása
- titkosítási rendszer
- Hozzáférési jogosultságok kezelése
- digitális aláírási rendszer, stb.

3. Védelmi környezet biztosítása:
Társaságunk elkötelezett, hogy olyan összetett védelmi környezetet alakítson ki, mely segítségével kellő biztonsággal, ugyanakkor rugalmassággal tudja kezelni a reá bízott és saját információkat. A védelmi környezet mind térben, mind technológiai, szabályozási, ellenőrzési, dokumentálási funkciói révén megteremti a szervezet zárt, teljes körű, folyamatos és a kockázatokkal arányos információvédelmét.

3.1. Fizikai és környezeti biztonság:
Társaságunk megelőzi az információs vagyon elvesztését, sérülését vagy veszélyeztetését, valamint a munkatevékenységek megszakadását úgy, hogy az információs vagyont fizikailag védi a biztonsági fenyegetésektől és a környezeti veszélyektől. Az információt és az információ feldolgozó eszközöket megvédi az illetéktelenek által nyilvánosságra hozataltól, lopástól, módosítástól, megsemmisítéstől.
Ennek érdekében létrehozott rendszer főbb elemei a következők:

- Társaságunk székhelyén a belépés ellenőrzött.
- Irodai beléptető rendszer (kártyás), név szerinti. Minden folyosó kamerával megfigyelt terület.
- Az irodaépület védelme riasztó rendszerrel, biztosító által elfogadott zárszerkezetű bejárati ajtókkal, ablakok vasrácsos védelmével került megvalósításra.
- Az IT-központ védelme további mechanikai védelmet kapott a riasztó rendszer mellett. A szerver-helyiségbe a belépés csak az informatikai vezető jelenlétében lehetséges, a helyiség kamerával megfigyelt terület.
- Az egyes helyiségeket kézi zárrendszer védi.

A személyes adatok tárolása és/vagy feldolgozása az így védett irodahelyiségekben történik.
Takarítók épületbe belépését egyedi kód biztosítja, név szerinti nyilvántartással.
Szerver helyiség és munkaügyi iroda takarítása csak az informatikai vezető, vagy a munkaügyi dolgozók jelenlétében történik, ezen helyiségekre vonatkozóan belépési kód kiadása takarítók számára nincsen, az ott dolgozók távollétében ezen irodák zárva vannak.

A munkaügyi kiléptetések során a kilépőlap az informatikai vezetővel is aláíratásra kerül, és a kilépést követően a kiadott jogosultságok megvonásra kerülnek.

3.2. Üzemeltetés biztonsága:
Társaságunk gondoskodik az információ feldolgozó eszközök pontos és biztonságos működéséről dokumentált üzemeltetési eljárások betartásával és betartatásával, a változások ellenőrzésével, a meghibásodások kockázatának minimalizálásával, rosszindulatú szoftverek elleni védekezéssel, az információfeldolgozás rendszergazda által történő állandó felügyeletével, valamint olyan hálózatok biztonsági menedzselésével, amelyek túlnyúlnak a szervezet határain.
A céges hálózatot, a szervert tűzfal védi a nyilvános hálózattól. Szoftvereink frissítéséről folyamatosan gondoskodunk, DHCP szerverünk csak a megbízható eszközöket engedi csatlakozni a hálózatra.

3.3. Adatbázis biztonsága, mentések, rendelkezésre állás:

Backup-ok gyakorisága: napi időközönként, este 23:00-kor, heti, havi és éves biztonsági mentés áll rendelkezésre.
Biztonsági adathordozók őrzése a backup helyszíntől 50 km-re történik.
Társaságunk IT központjának esetleges teljes megsemmisülését követő újra indulási idő meghatározása: 5 nap.
Az informatikai rendszer karbantartását végző vállalkozók csak Magyarország területén dolgoznak.
Működik valós idejű felhő szolgáltatás (Onedrive) ahová adatainkról biztonsági mentés készül.
Az elektronikus naplózást az IBSz biztosítja.

3.4. Személyes biztonság

Társaságunk gondoskodik arról, hogy az információ feldolgozó eszközöket használók tudatában legyenek az információ biztonságát fenyegető tényezőknek és a kialakított védelmi környezetnek. Gondoskodik továbbá arról, hogy a biztonságot sértő események és zavarok okozta kár minimális legyen. Ennek érdekében megtett intézkedési többek között a következők.

Egyedi korlátozások: Munkatársak egyedi céges email-címet kapnak, saját jelszóval védve.
Jelszó bonyolultság előírása: minimum 8 karakter, minimum 3 féle karakterrel (kisbetű, nagybetű, szám).
Képernyők automatikus zárolása: 10 perc után
SPAM-szűrésre a GFI Mail Essential programot használjuk.
Víruskeresők alkalmazása: szerveren ESET File security az adatok, adatbázisok védelmére, valamint AVG Business a rendszer és portok védelmét szolgálja.
Vírusvédelem a szervereken, automatikusan és szükség esetén, egyedileg manuálisan is alkalmazható. Vírusvédelem egyedi munkaállomásokon (asztali számítógépeken, laptopokon) Norton Security teljeskörű dédelem.
Biztonsági frissítések, mentések IBSZ szerint.
Elvárt: merevlemez titkosítás biztosítása.
Okostelefonok, táblagépek, adathordozók esetében jelszavas feloldási védelem szükséges.

3.5. Hozzáférés szabályozása, ellenőrzése:

Társaságunk az információhoz és az üzleti folyamatokhoz való hozzáférést az üzleti és biztonsági követelmények alapján ellenőrzi oly módon, hogy a hozzáférés-ellenőrzés figyelembe veszi az információ terjesztés és a felhatalmazás szabályait.
Ennek érdekében a jogosultságok kiosztása a munkavégzéshez szükséges mértékű jogosultságok megadásával történik.

3.6. Titoktartás biztosítása

Olyan munkavégzés esetén, ahol személyes adatok feldolgozása lehetséges, Társaságunk köteles az ilyen munkát végző személlyel, alvállalkozóval titoktartási szerződést kötni, a munkaszerződés mellékleteként. A titoktartási megállapodás alapján nevezettek kötelezik magukat a személyes adatok bizalmas kezelésére, a távközlési titok betartására.
Az ezen területen igénybe vett minden olyan alvállalkozó esetén, melynek hozzáférése lehet a személyes adatokhoz, Társaságunk köteles a magára nézve vállalt kötelezettségek vállalásáról felelősen és cégszerűen nyilatkoztatni, (mely szerint ugyanúgy betartják az előírt műszaki, szervezeti intézkedéseket, mint Társaságunk), továbbá a titoktartási kötelezettséget vállaltatni vele.

A titoktartási kötelezettségre kötelezett dolgozók adatvédelmi képzése Társaságunk kötelessége, melyért az ügyvezető felelős.
A belépő dolgozók tájékoztatásáért, a titoktartási kötelezettségről való informálásáért, erre vonatkozó munkaszerződésben (annak mellékleteként) a Munkaügyi vezető a felelős.

A hálózatszerelési területen dolgozók - még a vezetői beosztásban lévők sem- jellemzően nem kerülnek személyes adatokkal szembe munkavégzésük során. Kivételt képez, ha a megrendelő magánszemély, ám ez munkavégzésünk során kivételes eset.
Ezen esetben a magánszemély adatai a szerződéskötéshez szükségesek, és kezelésüket ez IBSZ szabályozza.

A fogyasztásmérő területen dolgozók találkoznak a Megrendelők adatállományból származó személyes adatokkal. Az irodai, adatrögzítést végzők az adatállománnyal, a szerelést végző munkavállalók, alvállalkozók munkavállalói a munkalapokon szereplő adatokkal. Ezen területre vonatkozó szabályozást az 5.4.pont rögzíti.

3.7. Adatfeldolgozók foglalkoztatása
Társaságunk adatokat átadhat feldolgozásra, szerződéses jogviszonyban más Adatkezelőknek, pl. könyvelésre, banki utalásra, munkaügyi ügyintézésre. Szerződésében mindig kiköti az adatkezelés biztonságát, GDPR előírások és szabályzatának való megfelelőségét, bármely adatkezelési incidens haladéktalan bejelentését.

3.8. Otthoni és/vagy mobil munkavégzés szabályozása
Társaságunk munkatársai munkavégzésünk során (e-napló helyszíni vezetése, munkavégzés fotókkal való dokumentálása érdekében, helyszíni oktatások végzésekor, stb.) mobil munkavégzést végeznek. Ugyanez teljesítési segédeink (alvállalkozók) esetében is előfordul.
A „távoli elérésre” és a mobil munkaeszközökre vonatkozó IBSZ előírásai biztosítják az informatikai biztonságot ezen munkavégzés során.

3.9. Törlés, iratmegsemmisítés:
Az iratmegsemmisítéseket erre szakosodott vállalkozások igénybe vételével, a jogszabályi, iratkezelési előírásoknak megfelelően végezzük.
Az egyéb adathordozók megsemmisítését az informatikai vezető szervezi.

4. Információs rendszerek:

4.1. Információs rendszerek beszerzése, fejlesztése és fenntartása:
Az új információs rendszerek beszerzését, vagy a meglévő információs rendszerek fejlesztését, fenntartását Társaságunk úgy végzi, hogy az információbiztonság valamennyi alapelve az információs rendszerekben megvalósuljon.
Informatikai vezetőnk figyelemmel kíséri a technikai fejlődésből adódó lehetséges újabb kockázatokat, és az azokat felszámoló védelmi megoldásokat, a meglévő rendszerek korszerűsítésére, javítására, felújítására, cseréjére, új eljárás bevezetésére javaslatot tesz az ügyvezető felé. A kialakított védelmi környezetet ezeknek megfelelően folyamatosan felügyeli, értékeli, és fejleszti.

4.2. Az üzletmenet folyamatosságának menedzselése, követelményeknek való megfelelés:
Társaságunk célja a törvényes, jogszabályoknak, szerződéses kötelezettségnek megfelelő működés, amelynek szerves része az információvédelem biztosítása, a személyes adatok védelmének előírások szerinti kezelése is.
Működési célunk továbbá meggátolni az üzleti tevékenységek megszakadásait és megvédeni a kritikus üzleti folyamatokat a nagyobb meghibásodások és katasztrófák hatásaitól.
Ezt szolgálja az IBSZ is.

4.3. Információbiztonsági incidensek kezelésére IBSZ szerint:
Az információbiztonsággal összefüggő incidenseket következetes és hatékony folyamat keretében kezeli, az egyértelmű felelősségek megjelölésével.

4.4. Az IBSZ-ben deklarált információvédelmi alapelveink közül kiemeljük a leglényegesebbeket.
Az informatikai biztonság területén Társaságunk az alábbi alapelveket és védelmi célkitűzéseket kívánja következetesen érvényesíteni:

- Hitelesség biztosítása, annak érdekében, hogy a belső és külső hálózatainkban, kapcsolatainkban a partnerek kölcsönösen és kétségtelenül felismerjék egymást és ezen állapotot a kapcsolat egész idejére fennmaradjon.
- Bizalmasság biztosítása az általunk kezelt, felhasznált adatokhoz való hozzáférés tekintetében, (mind a szervereken, mind az egyedi munkaállomásokon történő adathozzáférések, mind az adatkezeléseknél felhasznált adathordozók kezelése, valamint a kommunikáció során).
- Sértetlenség biztosítása az általunk kezelt adatvagyonra vonatkozóan, az adatkezelés, adattárolás és a kommunikáció során egyaránt.
- Ennek érdekében a nálunk megvalósuló adatkezelések és feldolgozások során követelmény, hogy munkatársaink a pontos és helyes információkat az elvárható legnagyobb pontossággal és megbízhatósággal dolgozzák fel, a titoktartás betartásával, az adatok sértetlenségének megőrzésével a feldolgozás teljes folyamata során.
- Működőképesség fenntartása Társaságunk informatikai rendszereire és rendszerelemeire vonatkozóan, időben, mennyiségben, minőségben, rendelkezésre álló időt tekintve egyaránt, és ennek érdekében a szükséges technikai feltételek, eszközök és képzett személyezt biztosítása.

4.5. Adatvédelmi megbízott kijelölése:
Adatfeldolgozó adatvédelmi kontakt személye: Farkas Dorottya, adatvédelmi megbízott.
Mobil: 0036-70-336-3338.

5. Adatkezelési tevékenységek és nyilvántartásuk:

5.1. Munkavállalók személyes adatainak kezelése:
Munkaügyi szabályzatban és Munkavállalói tájékoztatóban rögzítettek szerint.

5.2. Szerződésekben magánszemély megrendelők személyes adatainak kezelése:
IBSZ szerint

5.3. Web-oldal kapcsán érkező személyes adatok kezelése:
adatvédelmi tájékoztató szerint

5.4. Pályázat során, közös ajánlattétel, konzorcium esetében
Társaságunknál, közös ajánlattevő vállalkozás, alvállalkozók esetében akár a Megrendelő(k) adatállományából, akár saját nyilvántartásból adatokat kimásolni, kivonatolni, kinyomtatni, pályázati alkalmasság biztosítása, munkavégzés érdekében kiadni csak az ügyvezető jogosult a konzorcium vezetőjével egyeztetve a pályázatíró Adatfeldolgozó részére.
Társaságunk és alvállalkozói ezen munkatársakkal titoktartási megállapodást írtak alá a munkaszerződésük részeként, amely nemcsak az adatkezelés teljes folyamatát, hanem munkavégzésük teljességét tekintve kötelező érvényű.

Ezen munkatársak körének nyilvántartása az ügyvezetőnél van, aki ezen jogosultságokat kilépések esetén haladéktalanul módosítjak, a kilépésekor a jogosultságok törlése felől a Munkaügyi vezető felé és az informatikai vezető bevonásával intézkedik. A jogosultság felülvizsgálata ügyvezető feladata, ennek rendszerességét ő jogosult biztosítani.

5.5. Vállalkozói szerződés alapján a munkavégzés érdekében szükséges személyes adatok kezelése jelen adatvédelmi szabályzat szerint.

Társaságunk, mint Megbízott, adatkezelési tevékenységet végez a fogyasztásmérő szerelések területén. Társaságunk felelőssége és kötelessége a megfelelő védelmi szint biztosítása olyan technikai és szervezési intézkedésekkel, melyek figyelembe veszik a feldolgozás körülményeit és céljait, valamint a biztonsági rések miatti lehetséges jogsértés várható bekövetkezési valószínűségét és súlyosságát, továbbá lehetővé teszik a lényeges jogsértések azonnali megállapítását.
Vállalt tevékenység végzése során Társaságunk rendszeresen ellenőrzi a belső folyamatait, valamint a technikai és szervezési intézkedéseket annak biztosítására, hogy az irányadó adatvédelmi jogban szereplő követelmények szerint történjen a felelősségi körébe tartozó adatfeldolgozás, és biztosított legyen bármely érintett személy jogainak védelme.

Adatfajták az adatkezelés során: név, iskolai végzettség, foglalkozás, ágazati vagy üzleti terület megnevezése, cím, születési dátum, időpont, elérhetőségi, kommunikációs adatok (telefon, email-cím, forgalmi, telephelyi és készlet/leltár adatok, egyedi kapcsolati adatok), Telemédia adatok (használati és készlet/leltár adatok) vagy elektronikus kommunikációs adatok (elektronikus kommunikációs tartalmak és adatok), a hálózat- és mérőhely üzemeltetésből származó fogyasztási és a hálózat állapotára vonatkozó adatok, továbbá esetenként az ügyféltörténet.
Az adatfeldolgozás jellege vegyes, részben kézi, részben nem automatizált elektronikus, a Megrendelő elektronikus rendszeréhez csatlakozva.
Érintett személyek adatai: munkavállalók, természetes személy ügyfelek, alvállalkozók (harmadik cégek és munkatársaik), kontaktszemélyek.

Társaságunk rögzíti, hogy ezen tevékenység, a vállalt megbízás teljesítése során feldolgozott adatokat önhatalmúlag sosem, hanem kizárólag a Megrendelő (Adatkezelő) dokumentált utasítása alapján javíthatja, törölheti, vagy feldolgozásukat korlátozhatja.
Amennyiben az adatfeldolgozással érintett magánszemély ezzel kapcsolatban közvetlenül Társaságunkhoz fordul, akkor kötelesek vagyunk, és a cégünk képviseletében eljáró ügyintéző köteles a megkeresést haladéktalanul a Megrendelőhöz továbbítani, ugyanakkor köteles cégünk a Megrendelőt az Érintett tájékoztatása érdekében, maradéktalanul segíteni a rendelkezésre álló információnkkal és dokumentumokkal.
Természetesen, ha a szolgáltatási terjedelem magában foglalja, úgy a törlés(i koncepció)t, az elfeledtetéshez való jogot, a helyesbítést, az adathordozhatóságot és a Megrendelő (Adatkezelő) dokumentált utasításával összhangban lévő tájékoztatást közvetlenül Társaságunk biztosítja.
Titoktartási kötelezettségre vonatkozó előírás: Titoktartási kötelezettség a GDPR 28. cikk (3) bek. 2. mondat b) pont, valamint 29. cikk és 32. cikk (4) bek. és/vagy az (esetleg irányadó) hírközlési titoktartási jogszabály, továbbá az elektronikus kommunikáció adatainak titokban tartási kötelezettségéről rendelkező jogszabály szerint.
Titoktartási kötelezettség előírása Társaságunkon belül:
Társaságunk tárgyi adatfeldolgozás végrehajtása, a vállalt feladat teljesítése során csak olyan személyeket foglalkoztathat,

- akiket előtte titoktartásra kötelezett,
- és akikkel megismertette az adatvédelem számukra lényeges rendelkezéseit,
- a céges információbiztonság szabályait.

Kiemeljük azon lényeges szabályozást, hogy ezen tevékenységen dolgozó, valamennyi, Társaságunk irányítása alá tartozó, személyes adatokhoz hozzáférő személy a személyes adatokat kizárólag a Megrendelőnk utasításának megfelelően dolgozhatja fel, kivéve, ha uniós vagy tagállami jogon alapuló feldolgozási kötelezettség áll fenn.
Az ebből adódó titoktartási kötelezettség a Szerződés megszűnése után is fennáll határozatlan időtartamig, függetlenül az egyéb titoktartási kötelezettségektől. Ugyanez vonatkozik a hírközlési adatok titokban tartására is.
A titoktartási kötelezettség azt is magában foglalja, hogy a személyes adatokhoz, valamint az Megrendelő egyéb, bizalmasnak tekintendő információihoz kizárólag a Társaságunk vállalt szerződéses kötelezettségének teljesítésében részt vevő munkavállalói, ill. egyéb általunk jogszerűen, Megrendelőnk jóváhagyásával, a vonatkozó Szerződés teljesítéséhez igénybe vett teljesítési segédeink (alvállalkozók és alkalmazottai, foglalkoztatottjai) férhetnek hozzá.
Társaságunk az ezen tevékenység során igénybe vett munkavállalói létszámot, a velük létrejött hozzáférést a legszűkebb indokolt személyi körre köteles szűkíteni.
Ennek érdekében Társaságunk a következő Nyilvántartást vezeti: Társaságunk, mint Adatfeldolgozó által megadott, személyes adatokhoz hozzáférő személyeinek köre tételes, személyenkénti nyilvántartása:
Ennek vezetése, karbantartása, a kiléptetések kezelése, jogosultság visszavonása a munkáltatói jogokat gyakorló ügyvezető felelőssége.

Adatvédelmi ellenőrzés a tevékenység során:
Társaságunk köteles a Megrendelőt, mint Adatkezelőt haladéktalan tájékoztatni a felügyeleti hatóság esetleges ellenőrzéseiről és intézkedéseiről, amennyiben azok az érintett munkavégzésre vonatkoznak. Ez igaz azon esetre is, ha egy illetékes hatóság a személyes adatok feldolgozását érintő szabálysértési vagy büntetőeljárás keretében vizsgálatot végez Társaságunknál.
Adatvédelmi incidens bekövetkeztekor Társaságunk köteles a Megrendelő, mint Adatkezelő felé haladéktalanul jelenteni a bekövetkezett, Megrendelőt is érintő adatvédelmi incidenst, az ok megvizsgálása nélkül (ideértve az elvesztés vagy a jogellenes átadás vagy a tudomásszerzés eseteit).

Jelen Adatkezelési Szabályzatban Társaságunk deklarálja, hogy az általa, dolgozói által megismert személyes adatokat nem használja fel semmilyen más célra, mint a Szerződés, Szerződés-módosítás és mellékletei jogszerű teljesítése, és nem adja tovább azokat harmadik fél részére. A Megrendelő tudomása nélkül nem készülhetnek másolatok, duplikátumok az adatokról, kivéve a biztonsági másolatokat, amennyiben azok szükségesek a szabályszerű adatfeldolgozáshoz, valamint azon adatokat, melyek szükségesek a törvényes megőrzési kötelezettségek teljesítéséhez.
A Szerződésben rögzített munkák elvégzését követően, vagy ezt megelőzően a Megrendelő (Adatkezelő) írásbeli felszólítására – legkésőbb azonban a Szerződés megszűnését követően – Társaságunk átadja a Adatkezelő részére a birtokába jutott összes dokumentumot, a feldolgozással és felhasználással kapcsolatosan rendelkezésre álló eredményeket, valamint a megbízási viszonyból eredően előálló adatállományokat, vagy Adatkezelő kérésére megsemmisíti azokat az adatvédelmi előírásoknak megfelelően. Ugyanez vonatkozik a teszt- és a selejtanyagokra is. A törlésről/megsemmisítésről szóló jegyzőkönyvet kérésre be kell mutatni az Adatkezelő részére. Kivétel ez alól azon adatok megőrzése, amelyeket a jogszabályi kötelezettség ír elő Társaságunk részére (garanciális idő, kötelező alkalmassági idő, számviteli törvény pl.). Ennek érdekében a megbízásnak és a jogszabályi előírásoknak megfelelő adatfeldolgozás igazolásául szolgáló dokumentumokat Társaságunknak meg kell őriznie a Szerződés lejártát követően az adott jogszabályi megőrzési határidőknek megfelelően (számviteli, adóellenőrzési, fogyasztóvédelmi, garanciális, kötelező jótállási idő, stb.)

Az adatok és dokumentumok kezelése az archiválás szabályai szerint valósul meg. A dokumentumok, adathordozók megsemmisítése dokumentált.

6. Adatkezelési tájékoztató és nyilvános adatkezelési anyagok, személyes adatok kezelésének alapelvei:

Adatkezelési tájékoztató és nyilvános adatkezelési anyagok, személyes adatok kezelésének alapelvei: IBSZ-ben rögzítve, mellékletekként csatolva

6.1. Adatkezelési tájékoztató a web-lapon nyilvánosan hozzáférhető.

6.2. Panaszkezelés, panaszokkal kapcsolatos adatkezelés

Panaszkezelés célja: panaszügyintézés, a panasszal érintett eset körülményeinek kivizsgálása, a panasz érdemi kezelése.

Adatkezelés jogalapja: panaszkezelésre vonatkozó jogi kötelezettség teljesítése (GDPR tv vonatkozó elírásai, Fvt, Ptk)

Érintett személyes adatok köre: Panasz benyújtójának panaszban megadott személyazonosító adatai (jellemzően: név, e-mail cím, lakcím), továbbá a panaszban foglalt személyes, bármilyen adatok, továbbá a Társaságunknál esetleg meglévő személyes adatok

Adatkezelés időtartama, törlés: a panaszügy lezárásától számított 5 év, amelynek elteltével az adatok törlésre, megsemmisítésre kerülnek, kivéve, ha más törvényi rendelkezés nem írja elő megőrzésüket.

Címzettek kategóriái: jogszabályban előírt címzettek, hatóságok, bíróságok, azok hivatalos megkeresésére, felhívására, jogszabály alapján akinek előírt, dokumentumarchiválási, irattárolási szolgáltatást nyújtó adatfeldolgozója részére adatfeldolgozási szerződés alapján; szerverszolgáltatást nyújtó adatfeldolgozó részére, adatfeldolgozási szerződés alapján, küldemények kézbesítését végző társaságok, mint adatfeldolgozók részére a kézbesítéshez szükséges adatokat (név és cím), adatfeldolgozási szerződés alapján.

Adatszolgáltatás elmaradásának következménye: A panaszhoz kapcsolódó valamennyi releváns adat szükséges a panasz kezeléséhez, a körülmények kivizsgáláshoz. Az adatszolgáltatás elmaradása, vagy hiányos volta esetén a panasz nem, vagy nem megfelelően kezelhető.

A Panaszkezelési szabályzat Társaságunk panaszokkal kapcsolatos adatkezelését rögzíti és ismerteti, az Érintettek jogait bemutatja, az irodákban és a web-lapon nyilvánosan hozzáférhető.

Társaságunk a nyilvános Adatkezelési tájékoztatóban és a Panaszkezelési Szabályzatában rögzítette és ismerteti az Érintettek jogait, azok esetleges törvényi korlátozásával együtt, röviden:

- Tájékoztatáshoz való jog
- Helyesbítéshez való jog
- Adatkezeléshez adott hozzájárulás visszavonása; törléshez, ’elfeledtetéshez’ való jog
- Tiltakozáshoz való jog
- Adatkezelés korlátozásához való joga
- Adathordozhatóság joga

Ugyancsak itt adjuk meg a jogszerű jogorvoslati lehetőségeket is, Adatvédelmi megbízottunk elérhetőségét, felügyeleti szerv elérhetőségét, bírósági eljárások lehetőségét.

7. A megvalósítás kockázatai

Társaságunk menedzsmentje folyamatosan készül az üzletmenet-folytonosság fenntartására, ennek érdekében a kritikus üzleti folyamatok sérülése esetén tervezhető lépésekre, egy esetleges leállás utáni visszaállítására is, lehetőleg a legkisebb kieséssel.

Tisztában vagyunk azzal, hogy Társaságunk sikere nemcsak dolgozóink munkájától, szolgáltatásaink minőségétől függ, hanem legalább olyan fontos a zavarmentes működés, a

folyamatos pénzügyi biztonság, a szolgáltatások nyújtásának folyamatossága, s végül, de nem utolsó sorban az informatikai biztonság megteremtése, biztosítása is.
A megvalósítás kockázatai között figyelembe kell vennünk a mindenkori gazdasági környezetet, amelyre nincs ráhatásunk.
A belső erőforrásokból, (fluktuáció, képzettség, elkötelezettség, lojalitás, stb.) fakadó kockázatokat Társaságunk vezetése ismeri, ezek nagysága az elmúlt évek tapasztalatai alapján nem nevezhető jelentősnek.
Az alvállalkozók köre is stabilnak és kiterjedtnek mondható, az ebből fakadó kockázatok is viszonylag könnyen kezelhetők.

Külső kockázat:
A megvalósítás kockázatai között figyelembe kell vennünk a mindenkori gazdasági környezetet, amelyre nincs ráhatásunk. A környezeti hatás bekövetkezési valószínűsége nagyon ritka, és a kockázat minimális, a kockázati valószínűség alacsony.
Belső kockázattal párhuzamosan kezeljük az informatikaim kockázatot is, amelynél a külső hatások veszélye nem lebecsülhető, és megfelelő felkészültség mellett sem zárható ki.
Belső kockázat:
A belső erőforrásokból, (fluktuáció, képzettség, elkötelezettség, lojalitás, stb.) fakadó kockázatokat Társaságunk vezetése ismeri, ezek nagysága az elmúlt évek tapasztalatai alapján nem nevezhető jelentősnek.
A humán erőforrásból fakadó kockázatok kezelése Társaságunk működése alatt folyamatos. A képzés, bérrendezés, a megfelelő munkahelyi légkör biztosítása, a munkakörülmények folyamatos és érzékelhető javítása, az odafigyelés pozitív hatásait a létszámunk stabilitása igazolja. További tartaléklehetőségként tekintjük a cégcsoport egészét, mint rugalmas erőforrást, nemcsak humán problémák kezelése során.
Jelentős és tudatos Társaságunknál az alvállalkozói foglalkoztatás, épp az alvállalkozói kapacitások eredményezte humán vagy technikai erőforrás kapacitás rugalmasság végett. Társaságunk számára az alvállalkozók stratégiai partnerek, akikkel való együttműködés, ellenőrzés, a működésükre való odafigyelés, eredményességük megőrzése fontos szempont a működésünk tervezése és megvalósítása során. Ennek következtében az alvállalkozók köre is stabilnak és kiterjedtnek mondható, az ebből fakadó kockázatok is viszonylag könnyen kezelhetők. Több alvállalkozónk korábbi munkavállalónk, vagy vezetőnk gazdasági társasága.
Az informatikai rendszerek működtetési kockázata a működési kockázatok közül az egyik legjelentősebb, Ezzel kiemelten számolni kell, mert Társaságunk működéséhez, ezen belül az adatkezeléshez is már elengedhetetlen az informatikai kiszolgáló rendszerek megfelelő szintje és biztonsága, ezen rendszer egyes elemeinek, vagy teljes egészének kiesése, elvesztése esetén cégünk jelentős közvetlen és közvetett károkat szenvedhetne el, ami nemcsak súlyos anyagi veszteséget okozna, hanem az adatkezelés biztonságát is zavarná.
Társaságunk felkészült arra, hogy egy esetleges cyber-támadás esetén is, amíg a működéséhez szükséges feltételek helyreállítása folyik, biztosítani tudja a szükséges informatikai hátteret.
Ebben jelent segítséget a cégcsoport *gazdasági biztonsága,* továbbá – kiemelten! - a cégcsoport által biztosított *működési környezet biztonsága* is, egyrészt maga a fizikai irodahálózata, egyéb informatikai rendszerek, szerverek igénybevételének lehetősége, továbbá a stratégiai partnerként kezelt alvállalkozók kapacitása által nyújtott működési tartalék.
Társaságunk tudatosan törekszik az informatikai kockázatok csökkentésére, ezek során többlet kapacitások biztosítására.
A teljes informatikai rendszer tesztelése megtörtént „katasztrófa” elemzése során. Az informatikai rendszer visszaállítását, az IT-struktúra visszaállítás utáni tevékenységét elfogadhatóan rövid idő alatt, a szükséges aktuális adatokkal biztosítani tudjuk.

8. Együttműködés

Jelen Adatvédelmi Szabályzatban rögzített előírások, kötelezettség vállalások nem valósulhatnak meg a Társaságunknál dolgozó munkatársak, és a velünk együtt dolgozó alvállalkozók és foglalkoztatottjaik érdemi együttműködése nélkül.
Tiszteltel kérek mindenkit a hatékony, hosszú távú együttműködésre.

Budapest, 2018.08.27.

…….
ügyvezető