a **HI-LEX Hungary Kft**

2651 Rétság, Ipari park 3.

cégjegyzékszám: Cg. 12-09-005303

BELSŐ ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZATA

A dokumentum kelte	Jóváhagyta
2018. május 25.	

I. RÉSZ

ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja, hatálya

1.1 A jelen szabályzat („Szabályzat) a HI-LEX HUNGARY Kft., mint adatkezelő (a továbbiakban: „Adatkezelő") által alkalmazandó adatkezelési és adatvédelmi szabályokat, intézkedéseket tartalmazza.

1.2 A Szabályzat célja, hogy az Adatkezelő a vonatkozó jogszabályok, különösen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, a Munka Törvénykönyvéről szóló 2012. évi I. törvény, a kutatás és közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény, az Európai Parlament és a Tanács 2016/679 Rendelete, az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény, a számvitelről szóló 2000. évi C. törvény rendelkezéseivel összhangban szabályozza a birtokában lévő személyes adatok kezelésére, feldolgozására és védelmére vonatkozó általános kérdéseket.

1.3 A Szabályzat személyi hatálya kiterjed az Adatkezelő valamennyi munkavállalójára, megbízottjára, valamint az Adatkezelővel szerződéses, vagy az adatvédelmi tájékoztatóban feltüntetett módon kapcsolatba került természetes és jogi személyekre, üzleti partnerekre, jogi személyiséggel nem rendelkező szervezetekre, az Adatkezelő kezelésében lévő személyes adatokra vonatkozóan a velük kötött szerződés alapján.

A Szabályzat tárgyi hatálya a természetes személyeknek az Adatkezelő által kezelt személyes adatainak adatkezelésére és adatbiztonságára terjed ki.

2. Meghatározások

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 adaton 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 az Adatkezelő utasításai alapján.

Adathordozó: az adat fizikai megjelenési formája, tárolási helye, ideértve az iratokat is.

Adatkezelő: a HI-LEX HUNGARY Kft. (2651 Rétság, Ipari park 3.)

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton 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, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

Adatvédelmi incidens: személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés.

Érintett: bármely meghatározott (azonosított vagy azonosítható) természetes személy. A jelen Szabályzat rendelkezéseiben az Érintett egyaránt lehet Üzleti partner, Munkavállaló, Munkatárs.

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, amely vagy aki nem azonos az Érintettel, az Adatkezelővel vagy az Adatfeldolgozóval.

Hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság.

Honlap: az Adatkezelő által üzemeltetett, www.hi-lex.co.hu URL alatt elérhető internetes oldal, amelyeken keresztül az Adatkezelő Személyes adatokat (publikus forrás IP címet) gyűjt.

Hozzájárulás: az Érintett akaratának önkéntes és határozott akaratkinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez.

Infotv.: az információs önrendelkezési jogról és az információszabadságról szóló hatályos törvény, amely jelenleg a 2011. évi CXII. törvény.

Külső szolgáltató: az Adatkezelő által – akár közvetlenül, akár közvetetten – igénybe vett harmadik fél szolgáltató partnerek, amelyek számára a szolgáltatásaik biztosítása érdekében Személyes adatok továbbításra kerülnek vagy kerülhetnek. Külső szolgáltatónak minősülnek továbbá azon szolgáltatók is, amelyek nem állnak az Adatkezelővel együttműködésben, azonban hozzáférhetnek az Adatkezelő által kezelt személyes adatokhoz, illetve annak felhatalmazása alapján adatfeldolgozást végezhetnek.

Mt.: a Munka Törvénykönyvéről szóló hatályos jogszabály, ami jelenleg a 2012. évi I. törvény.

Munkavállaló: az Adatkezelővel munkaviszonyban álló természetes személy.

Munkatárs: az Adatkezelővel a munkaviszonyon kívüli egyéb munkavégzésre irányuló jogviszonyban álló természetes személy.

Munkáltató: az Adatkezelő.

Ptk.: a Polgári Törvénykönyvről szóló hatályos jogszabály, ami jelenleg a 2013. évi V. törvény.

Rendelet: az Európai Parlament és a Tanács 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról

Szabályzat: a jelen adatvédelmi és adatkezelési, továbbá adat- és informatikai biztonsági szabályzat.

Személyes adat: bármilyen adat vagy információ, amely alapján egy természetes személy Felhasználó – közvetett vagy közvetlen módon – azonosíthatóvá válik.

Üzleti partner: az Adatkezelővel vevői, vagy beszállítói kapcsolatban lévő, vagy ilyen jellegű jogviszony létesítése kapcsán kapcsolatba lépő személyek;

3. Adatkezelési alapelvek

3.1 *Az Adatkezelés jogalapja*

Személyes adat az Adatkezelő által akkor kezelhető, ha

- az Érintett hozzájárulását adta Személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

- az Adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az Érintett az egyik fél, vagy az a szerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges;
- az Adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
- az Adatkezelés az Érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
- az Adatkezelés 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 adatok védelmét teszik szükségessé;
- az Adatkezelés közérdekű feladat végrehajtásához szükséges.

3.2 *Jogszerűség, tisztességes eljárás és átláthatóság*

Az Adatkezelő a Személyes adatokat jogszerűen és tisztességesen, az Érintett számára átlátható módon kezelheti.

3.3 Célhoz kötöttség

3.3.1 Személyes adatot kezelni csak meghatározott, egyértelmű és jogszerű célból lehet (az adatkezelés célhoz kötöttségének elve).

Az Adatkezelésnek minden szakaszában meg kell felelnie a kitűzött célnak. Nem minősül az eredeti céllal össze nem egyeztethetőnek a statisztikai célból történő további Adatkezelés.

3.3.2 Az Adatkezelő köteles gondoskodni arról, hogy az általa kezelt Személyes adatokhoz csak olyan személyek férhessenek hozzá, akik vagy amelyek adatkezelése, adatfeldolgozása vonatkozásában a célhoz kötöttség elve megvalósultnak tekinthető.

3.3.3 A célhoz kötöttség elve megvalósulásának vizsgálata minden esetben az adatkezelési műveletet végző vagy végeztető szervezeti egység vezetőjének feladata és felelőssége. Amennyiben az Adatkezelés célhoz kötöttsége kétséges, a szervezeti egység vezetője köteles a kérdésben vizsgálatot lefolytatni.

3.4 *Adattakarékosság*

3.4.1 Az Adatkezelő biztosítja, hogy az általa kezelt Személyes adatok körének az adatkezelés céljai szempontjából megfelelő, releváns, és a szükséges mértékű Személyes adatokra korlátozódik melyek segítik az Adatkezelő és az Érintett gördülékeny együttműködését.

3.5 *Pontosság*

3.5.1 Az Adatkezelő biztosítja, hogy az általa kezelt Személyes adatok pontosak és szükség esetén naprakész. Az Adatkezelő minden észszerű intézkedést megtesz annak érdekében, hogy az Adatkezelés céljai szempontjából pontatlan Személyes adatokat haladéktalanul töröljék vagy helyesbítsék.

3.6. Korlátozott tárolhatóság

3.6.1 Az Adatkezelő biztosítja, hogy az adatkezelést kizárólag a szükséges ideig végzi, majd az adatokat törli, illetve az adathordozót megsemmisíti.

3.7 *Adatbiztonság*

3.7.1 Az Adatkezelő az Adatkezelés során mindvégig köteles gondoskodni a kezelt Személyes adatok ésszerűen elvárható legmagasabb szintű biztonságáról.

3.7.2 Az általa kezelt Személyes adatok biztonsága érdekében az Adatkezelő:

- az Adatkezelés időtartama alatt megteszi a Személyes adatok biztonságos tárolása, az időtartam lejártával az adatállomány törlése, fizikai megsemmisítése érdekében az általa szükségesnek tartott intézkedéseket;
- óvja az általa kezelt Személyes adatokat a jogosulatlan hozzáférés és az adatok illetéktelen megváltoztatása ellen;
- gondoskodik arról, hogy a Szabályzat rendelkezéseit az adatkezelési tevékenységet végző Munkavállalói, Munkatársai, illetve az általa az Adatkezelésbe bevont teljesítési segédek, Adatfeldolgozók, külső szolgáltatók megismerjék és betartsák, és ehhez kapcsolódóan folyamatosan ellenőrzi a Szabályzat betartását.

3.7.3 Az előző pontban foglaltakon túlmenően, a Személyes adatok automatizált feldolgozása során az Adatkezelő további intézkedésekkel biztosítja

- a jogosulatlan adatbevitel megakadályozását;
- az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli eszköz vagy szoftver segítségével történő használatának megakadályozását;
- annak ellenőrizhetőségét és megállapíthatóságát, hogy a Személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;
- annak ellenőrizhetőségét és megállapíthatóságát, hogy mely Személyes adatokat, mikor és ki vitte be, illetve ki módosította az automatikus adatfeldolgozó rendszerekbe;
- a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
- azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

3.7.4 Az általa kezelt Személyes adatok biztonsága érdekében az Adatkezelő a Munkavállalók által használt, illetve a céges IT eszközökön tárolt (szerveren) egyéb adatokról Munkáltató fontos gazdasági (IT-biztonsági) érdekeire tekintettel időszakonként IT technikai mentést készít, amely során minden olyan adat, amelyet azokban/azokon szerepel/ szerepelt, e mentés részét képezi. Az itt hivatkozott Adatkezelés jogalapja az Adatkezelő lényeges és jogos érdeke.

3.8 *Kiskorú személyek Személyes adatai*

A 16. életévét be nem töltött Érintett Személyes adatai csak a felette szülői felügyeletet gyakorló nagykorú személy hozzájárulása esetén kezelhetők. A szülői felügyeletet gyakorló személy (jellemzően Munkavállaló) által, ilyen típusú adat Adatkezelő részére történő rendelkezésre bocsátása hozzájárulásnak minősül, illetve az adat rendelkezésre bocsátója szavatol azért, hogy mint szülői felügyeleti jogot gyakorló személy, jogosult az adat megadására, és így az adatkezelési nyilatkozat megadására.

3.9 *Tájékoztatás*

3.9.1 Az Érintettet az Adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az Adatkezelés céljáról és jogalapjáról, az Adatkezelő és az Adatfeldolgozó személyéről, az Adatkezelés időtartamáról, továbbá arról, hogy kik ismerhetik meg az Érintettel kapcsolatosan kezelt Személyes adatokat. A tájékoztatásnak ki kell terjednie az Érintett Adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Ennek érdekében az Adatkezelő az adatkezeléssel kapcsolatosan oktatást és tájékoztatást ad minden Munkavállalójának, Munkatársának, az adatkezelési tájékoztatót elérhetővé teszi minden Érintett részére Honlapján, valamint, kérelem esetén külön tájékoztatást ad a kérelmező részére.

3.9.2 Az **Érintett kérelmére** az Adatkezelő **tájékoztatást ad** az Érintett általa kezelt, illetőleg az általa megbízott Adatfeldolgozó által feldolgozott Személyes adatairól, azok forrásáról, az Adatkezelés céljáról, jogalapjáról időtartamáról, az Adatfeldolgozó nevéről, címéről (székhelyéről) és az Adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá – az Érintett Személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.

3.9.3 Az Adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban a kérelem beérkezését követő 30 naptári napon belül közérthető formában, az Érintett kérelmére írásban megadni a tájékoztatást.

3.9.4 A tájékoztatás ingyenes, ha az Érintett a folyó évben azonos adatkörre vonatkozó tájékoztatási kérelmet ugyanazon Adatkezelőhöz még nem nyújtott be.

3.9.5 Amennyiben a Személyes adatot az Adatkezelő részére más adatkezelő továbbította, úgy az adattovábbító adatkezelőt – kérelmére – az Adatkezelő tájékoztatja az átvett Személyes adatok felhasználásáról.

3.10 *Adatfeldolgozó igénybe vétele*

Amennyiben az Adatkezelő az Adatkezelés folyamatába külső Adatfeldolgozót von be, az Adatfeldolgozó által folytatott adatkezelésért felelősséggel tartozik. Az Adatkezelő és az Adatfeldolgozó közötti szerződésben rögzíteni kell az Adatkezelő utasítási és ellenőrzési jogosultságait, az Adatfeldolgozó tájékoztatási kötelezettségeit az elszámoltathatóság elvének érvényesítése érdekében.

4. Az Adatkezeléshez kapcsolódó főbb folyamatok

4.1 *Hatásvizsgálati jegyzőkönyv*

4.1.1 Ha az Adatkezelő olyan új adatkezelési tevékenységet kíván bevezetni, ami növeli az adatkezelés kockázatát, különleges adat kezelése valósul meg, vagy automatikus profilaalkotás történik a tervezett adatkezelési tevékenységről hatásvizsgálati jegyzőkönyvet vesz fel.

4.1.2 A hatásvizsgálati jegyzőkönyvben legalább az alábbi információkat kell rögzíteni:

- az Adatkezelő személye
- a tervezett Adatkezelésbe bevont adatfeldolgozók és/vagy külső szolgáltatók
- a tervezett Adatkezelés célja
- a tervezett Adatkezelés jogalapja
- az Érintettek kategóriái
- kezelt Személyes adatok kategóriái
- a kockázati tényező azonosítása, forrása
- a kockázattal érintett Személyes adatok köre
- a kockázat minősítése, várható hatása, bekövetkeztének valószínűsége
- annak vizsgálata, hogy kockázatának súlyosságára tekintettel szükséges-e az adatvédelmi hatósággal egyeztetni
- annak vizsgálata, hogy van-e a tervezett adatkezeléshez kapcsolódóan olyan alternatív megoldás, amelyben a kockázat mérsékelhető vagy kiküszöbölhető
- a kockázat mérséklése érdekében tett intézkedések leírása, ezen intézkedésektől várt eredmények ismertetése

4.1.3 Az Adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a Személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

4.2 *Érdekmérlegelési teszt*

4.2.1 Ha az Adatkezelés jogalapja az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése, akkor az Adatkezeléshez kapcsolódóan az Adatkezelő érdekmérlegelési tesztet készít.

4.2.2 Az érdekmérlegelési teszt legalább az alábbi információkat tartalmazza:

- az Adatkezelés célja;
- az Adatkezeléssel érintett Személyes adatok kategóriái;
- az Adatkezelő vagy harmadik személynek az adatkezeléshez fűződő érdeke;
- az Érintettnek a mérlegelés tárgyát képező érdeke;
- az Érintett és az Adatkezelő közötti kapcsolat jellege;
- az Adatkezelés hatása az érintett mérlegelés tárgyát képező érdekére;
- az Adatkezeléshez kapcsolódó és az Érintett érdekeit negatívan érintő hatások bekövetkezésének kockázata;
- annak vizsgálata, hogy van-e a tervezett Adatkezeléshez kapcsolódóan olyan alternatív megoldás, amelyben a kockázat mérsékelhető vagy kiküszöbölhető.

4.2.3 Az Adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a Személyes adatok kezelésére vonatkozólag az érdekmérlegelési tesztben rögzített megállapítások fennállnak-e még.

4.3 *Adatkezelési nyilvántartás*

4.3.1 Az Adatkezelő az általa kezelt Személyes adatokról nyilvántartást vezet.

4.3.2 Az adatkezelési nyilvántartás az alábbi főbb elemeket tartalmazza:

- Adatkezelés célja;
- Adatkezelés jogalapja;
- Érintettek kategóriái;
- kezelt Személyes adatok kategóriái;
- címzettek köre (külön megjelölve, hogy sor kerül-e Személyes adatok határon átnyúló továbbítására);
- Adatkezelés időtartama, a törlés tervezett időpontja;
- technikai intézkedések leírása;
- az Adatkezelésért felelős kapcsolattartó elérhetősége.

4.3.3 Az Adatkezelő felelős azért, hogy az adatkezelési nyilvántartást folyamatosan frissítse.

4.3.4 Az Adatfeldolgozó az általa az Adatkezelő nevében végzett adatkezelésekről a jelen pont szerinti tartalommal nyilvántartást vezet.

4.4 *A kezelt adatok módosítása*

4.4.1 Ha az Adatkezelés időtartama alatt az Érintett az Adatkezelő által kezelt adatainak változását bejelenti, vagy az adatok megváltozását az Adatkezelő és/vagy az Adatfeldolgozó észleli, az adatokat a változásnak megfelelően haladéktalanul módosítani kell, illetve ki kell egészíteni vagy ezek érdekében eljárni.

4.4.2 A kezelt adatok módosítása esetén a módosításra kerülő korábbi, valamint a módosítást, kiegészítést követő új adatokat egyaránt fel kell tüntetni a nyilvántartásban, oly módon azonban, hogy a nyilvántartásból az adat aktív, illetve inaktív állapota egyértelműen megállapítható legyen.

4.4.3 Ha az adatok módosítására az Érintett megkeresése alapján kerül sor, az Érintett azonosítására az alábbi 4.9 pontban foglaltak irányadók.

4.4.4 Az adatok módosításának indokát és időpontját az Adatkezelő az adatkezelési nyilvántartásban rögzíti.

4.5 *Adattovábbítás*

4.5.1 Adattovábbítás az Adatkezelő szervezetén belül:

4.5.1.1 Az Adatkezelő szervezetén belül Személyes adatok csak a célhoz kötöttség elvének megfelelően továbbíthatók, és csak megfelelő cél esetén biztosítható az adatokhoz hozzáférési jog.

4.5.1.2 Amennyiben az adatok az Adatkezelőn belül, de osztályok, üzletágak, szolgáltató központok között kerülnek továbbításra, az adott adatkezelésért felelős munkatársat tájékoztatni kell a továbbítás tényéről, a továbbított adatkörökről, adatcsoportokról, a továbbítás céljáról és körülményeiről, illetve az adattovábbítás célját megvalósító Adatkezelés helyéről és várható időtartamáról.

4.5.1.3 Amennyiben az adatok továbbítása az egyes Adatkezelők között kerül sor, a továbbítást az Adatkezelő az adatkezelési nyilvántartásban rögzíti.

4.5.1.4 A rendszeres Adattovábbítás esetén az előző pontokban hivatkozott tájékoztatást, illetve a rögzítést elégséges az első adattovábbításkor megtenni, az adattovábbítások gyakoriságával együtt.

4.5.2 Adattovábbítás külföldre:

4.5.2.1 Személyes adatot az Adatkezelő harmadik országban adatkezelést folytató adatkezelő részére akkor továbbíthat, vagy harmadik országban adatfeldolgozást végző adatfeldolgozó részére akkor adhat át, ha:

- ahhoz az Érintett kifejezetten hozzájárult, vagy

- az Adatkezelésnek a jogszabályban előírt feltételei teljesülnek, és a harmadik országban az átadott adatok kezelése, valamint feldolgozása során biztosított a személyes adatok megfelelő szintű védelme.

4.5.2.2 A Személyes adatok megfelelő szintű védelme akkor biztosított, ha

- az Európai Unió kötelező jogi aktusa azt megállapítja, vagy
- a harmadik ország és Magyarország között az Érintettek jogai érvényesítésére, a jogorvoslati jog biztosítására, valamint az adatkezelés, illetve az adatfeldolgozás független ellenőrzésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés van hatályban.

4.5.2.3 Személyes adatok a nemzetközi jogsegélyről, az adóügyi információcseréről, valamint a kettős adóztatás elkerüléséről szóló nemzetközi szerződés végrehajtása érdekében, a nemzetközi szerződésben meghatározott célból, feltételekkel és adatkörben – a személyes adatok védelmére vonatkozó feltételek hiányában is – továbbíthatók harmadik országba.

4.5.2.4 Az Európai Gazdasági Térség részes államába irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

4.5.3 Amennyiben az adatok továbbítására az Érintett megkeresése alapján kerül sor, az Érintett azonosítására az alábbi 4.9 pontban foglaltak irányadók.

4.5.4 Az Adattovábbításról az adatgazda és a Adatkezelő képviselője együtt hoznak határozatot.

4.5.5 A továbbított Személyes adatokról az Adattovábbítás jogszerűségének ellenőrzése, valamint az arról való tájékoztatás lehetőségének érdekében az Adatkezelő adattovábbítási nyilvántartást vezet.

Az adattovábbítási nyilvántartás tartalmazza

- a Személyes adatok továbbításának időpontját,
- az Adattovábbítás jogalapját,
- az Adattovábbítás címzettjét,
- a továbbított Személyes adatok körének meghatározását, valamint,
- a jogszabályban meghatározott egyéb adatokat.

Az adattovábbítási nyilvántartás vezetése az Adatkezelésért felelős szervezeti egység vezetőjének feladata. A nyilvántartás elektronikus formában is vezethető. Az adattovábbítási nyilvántartást az Adatkezelő 5 évig megőrzi.

Az adattovábbítási nyilvántartás az adatkezelések nyilvántartásával összevontan is vezethető.

4.6 *Személyes adatok kezelésének korlátozása*

4.6.1 Az Érintett kérheti, hogy Személyes adatainak kezelését az Adatkezelő *korlátozza*,

- ha vitatja a kezelt Személyes adatok pontosságát;
- ha az Adatkezelés jogellenes, de ellenzi a kezelt Személyes adatok törlését;
- ha az Adatkezelés célja megvalósult, de az érintett igényli a kezelt Személyes adatainak Adatkezelő általi kezelését jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez.

4.6.2 A korlátozás hatálya alá eső Személyes adatok a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Európai Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

4.6.3 A Személyes adatok korlátozásának tényét, indokát és időtartamát az adatkezelési nyilvántartásban rögzíteni kell.

4.6.4 Az Érintett azonosítására az alábbi 4.9 pontban rögzítettek irányadók.

4.7 *Személyes adatok törlése*

4.7.1 A Személyes adatot törölni kell, ha

a) kezelése jogellenes;

b) az Érintett kéri a Rendelet 17. cikk (1) bek. b) pont szerint;

c) az hiányos vagy téves – és ez az állapot jogszerűen nem orvosolható –, feltéve, hogy a törlést törvény nem zárja ki;

d) az Adatkezelés célja megszűnt, vagy a Személyes adatok tárolásának törvényben meghatározott határideje lejárt;

e) azt a bíróság vagy a Hatóság elrendelte.

4.7.2 Az Adatkezelő megjelöli az általa kezelt Személyes adatot, ha az érintett vitatja annak helyességét vagy pontosságát, de a vitatott Személyes adat helytelensége vagy pontatlansága nem állapítható meg egyértelműen.

A helyesbítésről, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban a Személyes adatot Adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az Adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

Ha az Adatkezelő az érintett helyesbítés, vagy törlés iránti kérelmét nem teljesíti, a kérelem kézhezvételét követő 30 naptári napon belül írásban vagy az érintett hozzájárulásával elektronikus úton közli a helyesbítés, zárolás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait. A helyesbítés, törlés iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Hatósághoz fordulás lehetőségéről.

A törlésig az Adatkezelő az Érintett szerződésben szereplő adatait papír- és elektronikus formában is nyilvántarthatja.

4.7.3 Az Érintett tiltakozhat Személyes adatának kezelése ellen, ha

- a Személyes adat kezelése (továbbítása) kizárólag az Adatkezelő jogi kötelezettsége teljesítéséhez vagy az Adatkezelő, az adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
- a Személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, vagy tudományos kutatás céljára történik;
- a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.

Az Adatkezelő a tiltakozást köteles a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 naptári napon belül megvizsgálni, annak megalapozottsága kérdésében döntést hozni, és döntéséről az Érintettet írásban tájékoztatni.

Ha az Adatkezelő az Érintett tiltakozásának megalapozottságát megállapítja, az Adatkezelést – beleértve a további adatfelvételt és adattovábbítást is – megszünteti, és a Személyes adatokat zárolja, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíti mindazokat, akik részére a tiltakozással érintett Személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében. Ha az Adatkezelő egyetértett a tiltakozással, vagy a bíróság a tiltakozás jogosságát megállapította, a kezelt Személyes adat az adatátvevő részére nem továbbítható.

Ha az Érintett az Adatkezelőnek a tiltakozás megalapozottsága tárgyában hozott döntésével nem ért egyet, illetve, ha az Adatkezelő a határidőt elmulasztja, az Érintett – a döntés közlésétől, illetve a határidő utolsó napjától számított 30 naptári napon belül – a bírósághoz fordulhat.

Ha a Személyes adatokat átvevő adatkezelő a jogának érvényesítéséhez szükséges adatokat az Érintett tiltakozása miatt nem kapja meg, az adatokhoz való hozzájutás érdekében bírósághoz fordulhat az Adatkezelővel szemben. Az Adatkezelő ilyen esetben az Érintettet is perbe hívhatja.

Ha az Adatkezelő a tiltakozás megalapozottságáról szóló értesítést elmulasztja, az adatátvevő felvilágosítást kérhet az adatátadás meghiúsulásával kapcsolatos körülményekről az Adatkezelőtől, amely felvilágosítást az Adatkezelő az adatátvevő erre irányuló kérelmének kézbesítését követő 8 napon belül köteles megadni. Felvilágosítás kérése esetén az adatátvevő a felvilágosítás megadásától, de legkésőbb az arra nyitva álló határidőtől számított 15 napon belül az Adatkezelővel szemben bírósághoz fordulhat. Az Adatkezelő ilyen esetben az Érintettet is perbe hívhatja.

4.7.4 Az Adatkezelő az Érintett Személyes adatát nem törölheti, ha az Adatkezelést jogszabály írja elő. (Így pl. ha a szerződéses jogviszonyban számla kibocsátására kerül sor, a számlán szereplő adatok a számviteli- és adójogszabályokban meghatározott határidőkig tarthatók nyilván.)

4.7.5 Az Adatkezelő a Személyes adatok törléséről az Adatkezelő által használt központi feladat- és nyilvántartáskezelő rendszerben nyilvántartást vezet.

4.7.6 A jelen pontban hivatkozott jogok gyakorlása során az Érintett azonosítására az alábbi 4.9 pontban rögzítettek megfelelően irányadók.

4.8 *Adatszolgáltatások*

4.8.1 Hatósági adatszolgáltatás

4.8.1.1 A hivatalos szervektől – bíróság, közigazgatási szerv, nyomozó hatóság – érkezett, Személyes adatok szolgáltatására vonatozó megkereséseknek az Adatkezelő a megkeresésben megadott határidőig, ennek hiányában a megkeresés kézhezvételétől számított 30 naptári napon belül köteles eleget tenni.

4.8.1.2 A megkeresések határidőben történő teljesítéséért a megkeresett szervezeti egység vezetője felelős.

4.8.1.3 A büntetőeljárás kapcsán érkezett megkeresést – a bírósági megkeresések kivételével – csak abban az esetben lehet teljesíteni, ha a megkereső szerv pontosan megjelölte a szolgáltatandó adatkört, valamint az adatkezelés célját.

4.8.2 Adatszolgáltatás az Érintett részére

4.8.2.1 Az Érintett kérésére az Adatkezelő az Érintettről az Érintett hozzájárulása alapján kezelt Személyes adatokat tagolt módon, xml/pdf/csv formátumban részére rendelkezésre bocsátja. Az Érintettet ez a jog akkor is megilleti, ha az Adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az Érintett az egyik fél, vagy az adatkezelés az ilyen szerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges. Az Érintett kérheti, hogy az adatkezelő ezeket az adatokat más, az Érintett által megjelölt harmadik személy adatkezelő részére továbbítsa.

4.8.2.2 Az Érintett azonosítása érdekében az Adatkezelő az alábbi 4.9 pontban rögzítettek szerint jár el.

4.8.2.3 Az Adatkezelő az Érintett kérésének teljesítését megtagadhatja, ha a kért Személyes adatok rendelkezésre bocsátása mások jogait sérti. Erről az Adatkezelő az Érintettet az kérés kézhezvételétől számított 30 naptári napon belül tájékoztatja.

4.8.3. Az Adatkezelő az általa teljesített adatszolgáltatásokról nyilvántartást vezet.

Az adatszolgáltatási nyilvántartás legalább az alábbi adatokat tartalmazza:

- az érintett ismert természetes személy azonosító adatai;
- a szolgáltatott, továbbított adatok körét,
- az adatszolgáltatás, adattovábbítás időpontját,
- az adatszolgáltatás, adattovábbítás címzettjeinek nevét, székhelyét, egyéb azonosító adatait.

Az adatszolgáltatási nyilvántartásból kizárólag az Érintett, vagy meghatalmazottja részére nyújtható tájékoztatás az Érintettre vonatkozó körben.

Az Érintett azonosítása során az adatkezelő az alábbi 4.9 pontban foglaltak szerint jár el. Amennyiben az Érintettet meghatalmazott képviseli, a meghatalmazást teljes bizonyító erejű magánokiratban kell foglalni, és szükséges továbbá, hogy az iratból a meghatalmazotti jogosultság kitűnjön valamint, hogy a meghatalmazott személyét és meghatalmazotti jogosultságát hitelt érdemlően igazolja.

4.9 *Az Érintett azonosítása során követendő eljárás*

4.9.1 Annak érdekében, hogy az Érintett a jelen szabályzat fenti 4.4 – 4.8 pontjaiban hivatkozott egyes jogait gyakorolni tudja, az Adatkezelő első lépésként az Érintettet azonosítja személyesen, az azonosításra alkalmas dokumentumok ellenőrzésével, vagy e-mailes megkeresés esetén e-mail útján. Az e-mailes azonosítás során az Adatkezelő az Érintett általa kezelt e-mail címére rövid értesítést küld, amelyben jelzi, hogy az e-mail címhez kapcsolódó Személyes adatok tekintetében joggyakorlási igényt jelentettek be.

A tájékoztató e-mail szövegének rövidnek és tényszerűnek kell lennie. Pl. *„Az általunk kezelt Személyes adataihoz betekintést kértek az [•] e-mail címről. Az adatbiztonság érdekében kérjük, hogy az igényt erősítse meg! Tájékoztatjuk, hogy az adatkezelő az azonosítása érekében e-mailben további megerősítést kérhet."*

Adatbiztonsági okokból az Adatkezelő kérheti, hogy az Érintett az igényt egy, az Adatkezelő részére korábban már megadott Személyes adatának ismételt megadásával is biztosítsa. Ebben az esetben az Adatkezelő a Felhasználó részére egy újabb e-mail üzenetet küld. Pl. *„Az általunk kezelt Személyes adataihoz betekintést kértek az [•] e-mail címről. Az adatbiztonság érdekében kérjük, hogy az igényt erősítse meg az [irányítószáma] megadásával!"*

4.9.2 A megkeresésben foglaltakat az Adatkezelő kizárólag a megerősítést tartalmazó – adott esetben a második – e-mail beérkezését követően teljesítheti, a jelen Szabályzatban foglaltaknak megfelelően.

4.9.3 Amennyiben a megkeresés az Adatfeldolgozó elérhetőségére érkezik, úgy az Adatfeldolgozó a megkeresést köteles haladéktalanul továbbítani az Adatkezelő részére. Közös Adatkezelés estén az adatkezelők a megkeresésről haladéktalanul, írásban (e-mailen) értesítik egymást.

4.9.4 A megkeresést legkésőbb a megkeresés beérkezésétől számított 30 naptári napon belül teljesíteni kell. A megkeresés tényét, időpontját, valamint a teljesítés időpontját az Adatkezelő az adatkezelési nyilvántartásban rögzíti.

4.10 *Eljárás adatvédelmi incidens esetén*

4.10.1 Az Adatkezelő valamennyi munkatársa köteles a tudomására jutott adatvédelmi incidens vagy az Adatkezelő eszközeivel, adathordozóival vagy hálózataival kapcsolatos visszaélés tényét a közvetlen felettesének vagy a munkáltatói jogkör gyakorlójának (alvállalkozó esetén a szerződéses kapcsolattartójának) haladéktalanul jelezni.

Adatvédelmi incidens, valamint az informatikai biztonsággal kapcsolatos visszaélés, továbbá az informatikai biztonság sérelme esetén a fent megjelölt munkavállalók (felettes vezető, kapcsolattartó stb) a cég képviseletére jogosult vezető tisztségviselőjét (ügyvezető) haladéktalanul tájékoztatni.

Az Adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az Adatkezelőnek.

4.10.2 Az adatvédelmi incidensről az Adatkezelésért felelős egység vezetője jegyzőkönyvet vesz fel, amely tartalmazza

- az adatvédelmi incidens időpontját;
- az adatvédelmi incidens jellegét;
- az adatvédelmi incidens által érintett adatok körét, hozzávetőleges számát;
- az érintettek kategóriáit, hozzávetőleges számát;
- az adatvédelmi incidens valószínűsíthető következményeit;
- az adatvédelmi incidens orvoslására tett intézkedéseket.

4.10.3 Az adatvédelmi incidenst az Adatkezelő képviselője legkésőbb a tudomásra jutástól számított 72 órán belül köteles a Hatóság felé bejelenteni. A bejelentésben meg kell adni az Adatkezelő kapcsolattartóját is.

4.10.4 Az Adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

4.10.5 Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az Érintett jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül tájékoztatja az Érintettet az adatvédelmi incidensről.

Nem szükséges az Érintettet tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében az adatvédelmi incidenst megelőzően alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a Személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az Érintett jogaira és szabadságaira jelentett, az említett magas kockázat valószínűsíthetően nem következik be;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az Érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az Érintettek hasonlóan hatékony tájékoztatását.

4.11 *Dokumentumok tárolása*

A jelen 4. pontban hivatkozott dokumentumok minden esetben legalább egy példányban készülnek.

A dokumentumokat az Adatkezelő adott adatkezelésért felelős adatgazdája tárolja.

5. Belső adatvédelmi tisztségviselő

5.1 A Rendelet 37. cikke rögzíti azokat az eseteket, amely esetekben az Adatkezelőnek belső adatvédelmi tisztségviselőt kell kijelölnie.

5.2 Áttekintve az Adatkezelő által folytatott adatkezelési tevékenységeket, megállapítást nyert, hogy az Adatkezelő nem tartozik a Rendelet 37. cikke által nevesített kategóriák közé.

5.3 A fentiek alapján az Adatkezelőnél belső adatvédelmi felelős kijelölésére a hivatkozott rendelkezés alapján az Adatkezelő nem köteles.

5.4 Az Adatkezelők által folytatott adatkezelési tevékenység jogszerűségéért az Adatkezelő ügyvezetéséért felelős személyek felelősek. Rajtuk kívül az egyes adatkezelési tevékenységek esetén a jelen Szabályzat rendelkezéseinek betartása és betartatása az adott adatkezelés esetében eljáró adatgazda és/vagy Munkatárs körébe tartozik.

6. Belső adatvédelmi felelős

6.1 Az Infotv. alapján az Adatkezelő által kijelölt belső adatvédelmi felelős, amennyiben van ilyen, az alábbi feladatokat látja el:

- közreműködik, illetőleg segítséget nyújt az Adatkezeléssel összefüggő döntések meghozatalában, valamint az Érintettek jogainak biztosításában,
- irányítja az adatvédelmi ellenőrzéseket, vizsgálatokat,
- ellenőrzi a Szabályzatban foglaltak betartását,

- tájékoztatja az Adatkezelő más szervezeti egységeit a Szabályzat és a kapcsolódó külön szabályzatok gyakorlati alkalmazásáról, segítségét nyújt a gyakorlati tapasztalatok összegzésében,
- figyelemmel kíséri az adatvédelmi jogszabályok változását, szükség esetén javaslatot tesz a Szabályzat módosítására,
- figyelemmel kíséri az Érintetteknek nyújtott tájékoztatás rendszerét,
- vezeti a Szabályzat szerinti nyilvántartásokat,
- kivizsgálja a Személyes adatok kezelésével (feldolgozásával, továbbításával) kapcsolatban hozzá érkezett bejelentéseket és panaszokat,
- fogadóórát köteles tartani, ahol előzetes bejelentéseket követően lehet a belső adatvédelmi felelőssel egyéni konzultációt folytatni,
- jogosulatlan Adatkezelés észlelése esetén annak megszüntetésére hívja fel az Adatkezelőt vagy az Adatfeldolgozót,
- megszervezi a Szabályzat alkalmazásával kapcsolatos adatvédelmi oktatást és az adatvédelmi tárgyú tájékoztató kiadványok kibocsátását,
- évente tájékoztatja az adatvédelmi biztost azokról az elutasított kérelmekről, amelyekben az Érintettek saját Személyes adataik kezeléséről érdeklődtek,
- együttműködik az Adatkezelő szervezeteivel a felmerülő adatvédelmi tárgyú kérdések megoldásában.

6.2 Tekintettel arra, hogy az Adatkezelő nem folytat az Infotv. 24. § (1) bekezdés alá tartozó tevékenységet, az Adatkezelőnél külön belső adatvédelmi felelős kijelölésére jelenleg nem kerül sor. A belső adatvédelmi felelős feladatkörébe tartozó feladatok a személyzeti vezető, és a pénzügyi vezető megosztva látja el.

7. Vegyes rendelkezések

7.1 A jelen Szabályzat rendelkezéseiről az Adatkezelő tájékoztatja a Munkavállalóit és Munkatársait.

A Szabályzat hatályos szövege elektronikus formában elérhető az Adatkezelő központi hálózatán.

A Szabályzatban foglalt rendelkezéseiről az Adatkezelő a Munkavállalói és Munkatársai részére oktatásokat szervez, amelyen valamennyi Munkavállaló és Munkatárs köteles részt venni.

7.2 Az Adatkezelőnek az arra feljogosított szerve bármikor jogosult a jelen Szabályzat rendelkezéseit egyoldalúan módosítani.

A Szabályzat bármilyen módosítása a verziószám változásával jár, melyet a Szabályzat címoldalán fel kell vezetni.

7.3 A Szabályzat, illetve mellékleteinek felülvizsgálatára az alábbiak szerint kerül sor:

a) évente egy alkalommal, a belső felülvizsgálatok során,

b) rendkívüli, a megváltozott körülmények hatására a felülvizsgálatot el kell végezni az alábbi események bármelyikének bekövetkezésekor:

- az Adatkezelő Szervezeti és Működési Szabályzata módosítása;
- az információbiztonságot is érintő jogszabály-változás, amennyiben annak hatálya az Adatkezelőre is kiterjed;
- az információkezelést és –feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás;
- az Adatkezelő tulajdonában vagy használatában lévő elektronikus információs rendszerekben, illetve azok fizikai környezetében beálló lényeges változás.

c) minden olyan esetben, amikor a Szabályzatban leírtakhoz képest egyéb jelentős változás történik.

7.4 A mindenkori felülvizsgálat végrehajtása az ügyvezető feladat- és felelősségi körébe tartozik.

7.5 A Szabályzat módosításról az Adatkezelő mint Munkáltató a szervezetében szokásos módon – akár a munkahelyi email címekre történő megküldéssel – értesíti a Munkavállalókat és a Munkatársakat.

II. RÉSZ

Az Adatkezelő egyedi adatkezelési tevékenységei

1. Adatkezelési célok

Az Adatkezelő által folytatott adatkezelési tevékenységek céljai az alábbiak lehetnek.

1.1 A Munkavállalók Személyes adatainak kezelése esetében a Munkáltató által folytatott Adatkezelés célja lehet:

a) a munkaviszonyból származó kötelezettségek teljesítése;

b) bérszámfejtési vagy a munkaviszonnyal összefüggő, jogszabály által meghatározott egyéb feladatok ellátása;
c) statisztikák, elemzések készítése;
d) a Munkavállalók kezdeményezése esetén egyedi juttatások biztosítása;
e) Munkavállaló, vagy egy másik természetes személy érdekeinek védelme;
f) Munkáltató vagy egy harmadik fél jogos érdekeinek érvényesítése.

1.3 Az Adatkezelővel szerződéses kapcsolatban álló Üzleti partnerek által megadott Személyes adatok kezelése során az Adatkezelés célja lehet:

a) az Adatkezelő szerződéses kötelezettségeinek teljesítése;

b) a szerződő partner kötelezettségei teljesítésének ellenőrzése;
c) az Adatkezelő jogos érdekeinek érvényesítése.

2. Az Adatkezelések jogalapja

2.1 A Munkavállalók Személyes adatainak kezelésekor az Adatkezelés jogalapja lehet:

a) az Adatkezelőt terhelő jogszabályi kötelezettség teljesítése;

b) az Adatkezelő szerződésben rögzített kötelezettségének teljesítése;
c) Munkavállaló, vagy egy másik természetes személy érdekeinek védelme;
d) Munkáltató vagy egy harmadik fél jogos érdekeinek érvényesítése;
e) a Munkavállaló önkéntes hozzájárulása.

2.3 Az Adatkezelővel szerződéses kapcsolatban álló Üzleti partner által megadott Személyes adatok kezelésének jogalapja lehet:

a) az Adatkezelő szerződésben rögzített kötelezettségének teljesítése;

b) az Érintett önkéntes hozzájárulása.

2.4. A Rendelet 6. cikk b) pontja alapján az Érintett által a Munkáltatóval állás betöltése és/vagy a munkaszerződés előkészítése érdekében közölt Személyes adatai kezelése a munkaszerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges Adatkezelésnek minősül, tehát Munkáltató ezen Személyes adatokat a munkaviszony Érintettel történő létesítésének elmaradásáig, de legfeljebb három hónapig az Érintett külön hozzájárulása nélkül jogosult kezelni.

Amennyiben az Érintettel a munkaviszony bármely okból nem jön létre, vagy ha az előző bekezdés szerinti időtartam eltelt, Munkáltató az érintett fenti személyes adatait két évig jogosult tárolni, azzal, hogy ezen Adatkezelés jogalapja az Érintett hozzájárulása. A hozzájáruláson alapuló adatkezelés célja, hogy a Munkáltató az Érintettnek a Munkáltatónál történő potenciális elhelyezkedését lehetővé tévő jövőbeni olyan helyzetben, amikor az Érintett a Munkáltató által létesíteni kívánt munkaviszony vagy munkavégzésre irányuló egyéb jogviszony betöltésére a Munkáltató megítélése szerint alkalmas lehet, a Személyes adatok lehetővé tegyék a Munkáltató ezen álláspontjának kialakítását és az érintett közvetlen megkeresését.

3. Az adatkezelési tevékenységet végző munkakörök és az általuk végzett adatkezelési (rész)folyamatok

3.1. *Adott feladatért, projektért felelős Munkavállaló, Munkatárs*

3.1.1 Adatkezelő erre kijelölt Munkavállalója/Munkatársa esetenként, vagy kijelölt Üzleti partner, vagy ügycsoport esetén folytathat adatkezelési tevékenységet. Ilyen esetekben kezelheti az érintett Üzleti partnerek képviselőinek, kapcsolattartóinak a Személyes adatait.

Az Érintett a Személyes adatokat személyesen, telefonon, a kijelölt Munkavállaló/Munkatárs céges e-mailjére küldött üzenetben adja meg.

A kijelölt Munkavállaló/Munkatárs az Érintett a Személyes adatait a Munkáltató által részére biztosított személyi számítógépen, mobil telefonon, a Munkáltató belső hálózatának felületein, a Munkáltató szerverein vagy a Munkáltató által biztosított, és az e-mail fiókhoz tartozó tárhely szolgáltatásban, az Adatkezelő által üzemeltetett megrendelésállomány-nyilvántartó rendszerben, illetve az ERP szolgáltatást biztosító Külső szolgáltató által elérhetővé tett felületen kezelheti.

3.1.2 A kijelölt Munkavállaló/Munkatárs az Üzleti partnerrel kötött szerződések teljesítése érdekében kezelheti az Üzleti partner kapcsolattartóinak nevét, e-mail címét és telefonszámát, beosztását.

3.2 *Pénzügy számviteli és kontrolling feladatokat ellátó vezető és munkatárs (együtt: pénzügyi számviteli munkatárs)*

3.2.1. A pénzügyi számviteli munkatárs kezelheti az Üzleti partnerek vagy e partnerek által megadott kapcsolattartók Személyes adatait, valamit a Munkavállalók és a Munkatársak Személyes adatait.

A pénzügyi számviteli munkatárs az általa kezelt Személyes adatokat a Munkáltató központi szerverein és céges e-mail fiókjában kezeli, tárolhatja.

A pénzügyi számviteli munkatárs az Adatkezelés során céges asztali gépet, céges laptopot, valamint saját mobiltelefont használ.

3.2.2 A pénzügyi területhez kapcsolódóan az Adatkezelő által kezelt Személyes adatok köre adatkezelési célok szerint

a) az Adatkezelő szolgáltatásait igénybe vevő Érintettek esetén kezelheti a számlázáshoz, pénzügyi teljesítéshez szükséges adatokat, mint az Érintett nevét, anyja nevét, születési adatait (hely, időpont), állandó lakcímét, személyi igazolvány számát, adóazonosító jelét, bankszámlaszámát;
b) a munkaszerződés megkötéséhez és a munkaviszonya nyilvántartásához kapcsolódóan az Adatkezelő kezeli ill. kezelheti a Munkavállaló nevét, anyja nevét, születési adatait (hely, időpont), állandó lakcímét, személyi igazolvány számát, adóazonosító jelét, bankszámlaszámát, TAJ számát, jelenlegi munkaviszonyának kezdetét, bér és egyéb bérjellegű, vagy béren kívüli juttatások, ezek összegének megállapításához kapcsolódó adatokat (pl. prémium értékelés, munkahelyi értékelése), a heti munkaórák számát, munkaidő nyilvántartását (beleértve az igazolt vagy igazolatlan távollétek ideje, indoka, és az azokat megalapozó dokumentáció), az adókedvezmények igénybevételével kapcsolatos adatokat, esetleges kiküldetések helyszínére és időpontjára vonatkozó adatokat, a könyvelés vagy könyvvizsgálat részét képező bizonylatokon, kapcsolódó dokumentumokban megjelenő, a Munkavállalóval szembeni hátrányos jogkövetkezmény kiszabásával, vagy egyéb, a munkaviszonyból fakadó kötelezettségek megszegésével kapcsolatos adatokat, a Munkavállaló állampolgárságára vonatkozó adatot, a Munkavállaló gyermekeinek számát, nevét, születési helyét és idejét, a Munkavállaló egészségügyi adatait;
c) a kontrolling tevékenység során az Adatkezelő kezeli a Munkavállaló és a munkabérét, valamint a Munkatárs nevét és díjazását;
d) könyveléshez kapcsolódóan az Adatkezelő kezeli a Felhasználó számlázási adatai, az üzleti partner kapcsolattartójának nevét és elérhetőségeit (telefonszámát és e-mail címét).

3.3 Személyzeti vezető és munkatárs (együtt: személyzeti munkatárs)

3.3.1. A személyzeti munkatárs kezelheti a Munkavállalók és a Munkatársak Személyes adatait.

A személyzeti munkatárs az általa kezelt Személyes adatokat a Munkáltató központi szerverein és céges e-mail fiókjában kezeli tárolhatja.

A személyzeti munkatárs az Adatkezelés során céges asztali gépet, céges laptopot, valamint saját mobiltelefont használ.

3.3.2 A személyzeti területhez kapcsolódóan az Adatkezelő által kezelt Személyes adatok köre adatkezelési célok szerint

a) az álláshirdetésekre jelentkezők esetében az Adatkezelő kezelheti az Érintett nevét, anyja nevét, születési adatait (hely, időpont), állandó lakcímét, személyi igazolvány számát, adóazonosító jelét, bankszámlaszámát, TAJ számát, az Érintett végzettségére, korábbi munkahelyeire, munkaköreire vonatkozó adatokat, az Érintett állampolgárságára vonatkozó adatot, az Érintett gyermekeinek számát, nevét, születési helyét és idejét valamint a jelentkező által önkéntesen megadott további Személyes adatokat;
b) a munkaszerződés megkötéséhez és a munkaviszonya nyilvántartásához kapcsolódóan az Adatkezelő kezeli ill. kezelheti a Munkavállaló nevét, anyja nevét, születési adatait (hely, időpont), állandó lakcímét, személyi igazolvány számát, adóazonosító jelét, bankszámlaszámát, TAJ számát, jelenlegi munkaviszonyának kezdetét, bér és egyéb bérjellegű, vagy béren kívüli juttatások, ezek összegének megállapításához kapcsolódó adatokat (pl. prémium értékelés, munkahelyi értékelése), a heti munkaórák számát, munkaidő nyilvántartását (beleértve az igazolt vagy igazolatlan távollétek ideje, indoka, és az azokat megalapozó dokumentáció), az adókedvezmények igénybevételével kapcsolatos adatokat, esetleges kiküldetések helyszínére és időpontjára vonatkozó adatokat, a könyvelés vagy könyvvizsgálat részét képező bizonylatokon, kapcsolódó dokumentumokban

megjelenő, a Munkavállalóval szembeni hátrányos jogkövetkezmény kiszabásával, vagy egyéb, a munkaviszonyból fakadó kötelezettségek megszegésével kapcsolatos adatokat, a Munkavállaló állampolgárságára vonatkozó adatot, a Munkavállaló gyermekeinek számát, nevét, születési helyét és idejét, a Munkavállaló egészségügyi adatait;

c) a Munkáltató által a munkavégzés helyén elhelyezett kamerák által készített felvételeken szereplő személyes adatok.

3.4 *IT tevékenységet ellátó Munkatárs, rendszergazda (IT munkatárs)*

3.4.1 Az IT munkatárs kezelheti az Üzleti partnerek által megadott bármely Személyes adatot, valamint a Munkavállalók és a Munkatársak Személyes adatait, beleértve a Munkavállalók / Munkatársak által használt eszközök karbantartásakor számukra elérhetővé tett Személyes adatokat.

Az IT munkatárs az Adatkezeléseket fő szabály szerint a Munkáltató által részére biztosított személyi számítógépen, mobil telefonon, valamint bármely olyan eszközön, amelyre vonatkozólag rendszergazdai feladatait látja el; továbbá a Munkáltató IT rendszerében, vagy a Munkáltató által biztosított, és az e-mail fiókhoz tartozó tárhely szolgáltatásban kezelheti.

Ha az IT munkatárs saját személyi számítógépet és/vagy mobiltelefont használ, úgy köteles ezek használatakor a Munkáltató adatbiztonságra vonatkozó rendelkezéseit betartani.

3.4.2 Az IT területhez kapcsolódóan az Adatkezelő által kezelt Személyes adatok köre adatkezelési célok szerint

a) Amennyiben az Érintett a Honlap felületét látogatja, a Honlapon regisztráció nélkül tartalmat ér el, az Adatkezelő rendszere automatikusan rögzíti a Felhasználó IP címét.

b) Az Adatkezelői informatikai rendszerek működtetése, biztonságának biztosítása során az Adatkezelő automatikusan rögzíti a honlapot böngésző számítógépének azon adatait, amelyek a Honlap látogatása során generálódnak, és amelyeket az Adatkezelő rendszere a technikai folyamatok automatikus eredményeként rögzít. Az automatikusan rögzítésre kerülő adatokat a rendszer automatikusan naplózza és a naplófájlok törlési idejéig (maximum 6 hónap) tárolja.

c) az álláshirdetésekre jelentkezők esetében az Adatkezelő kezelheti az Érintett nevét, anyja nevét, születési adatait (hely, időpont), állandó lakcímét, személyi igazolvány számát, adóazonosító jelét, bankszámlaszámát, TAJ számát, az Érintett végzettségére, korábbi munkahelyeire, munkaköreire vonatkozó adatokat, az Érintett állampolgárságára vonatkozó adatot, az Érintett gyermekeinek számát, nevét, születési helyét és idejét.

d) a Munkáltató által a munkavégzés helyén elhelyezett kamerák által készített felvételeken szereplő személyes adatok.

3.4.3 Adatbázisok frissítése

Az Adatkezelő a honlapot böngésző kliensgépek IP címét legfeljebb 6 hónapig tárolja, ezt követően törli a rendszereiből.

Az Adatkezelő az informatikai rendszerek működtetése, biztonságának biztosítása érdekében automatikusan rögzített adatokat legfeljebb 6 hónapig tárolja, ezt követően törli az éles rendszereiből.

3.5 *Ügyvezető*

3.5.1 Az Ügyvezető a HI-LEX Hungary Kft. tevékenységének operatív irányításáért felelős vezetője.

3.5.2 Az Ügyvezető a saját munkaterületéhez tartozó esetekben kezelheti az egyes munkakörök esetében fentebb felsorolt, a Munkavállalókhoz, Munkatársakhoz, Üzleti partnerekhez Adatfeldolgozókhoz, Külső szolgáltatókhoz vagy más üzleti partnerekhez kapcsolódó valamennyi Személyes adatot.

3.5.3 Az Ügyvezető kezelheti az általa irányított területen dolgozó Munkavállalók Személyes adatait. Ezen belül kezelheti:

a) a Munkavállalók munkaviszonyának nyilvántartásához kapcsolódó Személyes adatokat;

b) a bérszámfejtés és a kontrolling tevékenység kapcsán leírt egyes Személyes adatokat;
c) a Munkavállaló részére biztosított céges IT eszközökön folytatott levelezésekben szereplő személyes adatok;
d) a Munkavállaló rendelkezésre bocsátott céges mobil eszközökből, vagy azokkal kapcsolatban a szolgáltató által küldött, a használat részleteit tartalmazó kimutatás alapján a Munkáltató számára elérhető adatokat;
e) a céges gépjárművekkel kapcsolatban Munkáltató számára elérhető adatokat (üzemanyag számlák, bírságok adatai, esetleges baleseti körülmények, műholdas járműkövetés adatai);
f) a Munkáltató által a munkavégzés helyén elhelyezett kamerák által készített felvételeken szereplő személyes adatok.

3.5.4 Az Ügyvezető a Munkáltató álláshirdetéseire jelentkezők esetében, az Érintett hozzájárulása alapján kezelheti a fenti 3.3.2 pontban hivatkozott adatokat.

3.5.5 Az Ügyvezető az általa kezelt Személyes adatokat a részére biztosított személyi számítógépen, mobil telefonon, a Munkáltató rendszerében, a Munkáltató szerverein vagy a Munkáltató által biztosított, és az e-mail fiókhoz tartozó tárhely szolgáltatásban kezeli.

4. A kamerarendszer

4.1. A kamerarendszer működtetésének célja, jogalapja

a) Az adatkezelő az emberi élet, testi épség, személyi szabadság védelme, jelentős értéket képviselő áruk, eszközök, értéktárgyak vagyonvédelme érdekében elektronikus megfigyelőrendszert (a továbbiakban: kamera) alkalmaz. Kamera kizárólag a következő helyszíneken üzemel: *Iroda bejárat, előtér*
b) A kamerarendszert kizárólag az adatkezelő működteti.
c) A kamerarendszer karbantartására az adatkezelő arra szakképesítéssel rendelkező karbantartó társaságot bíz meg, amely társaság az adatvédelmi szabályok betartását garantálja.
d) Ha az adatkezelő telephelyén jogszerűen senki sem tartózkodhat (így például munkaidőn kívül vagy a munkaszüneti napokon), akkor a telephely teljes területe is megfigyelhető.
e) A kamerák látószöge kizárólag saját tulajdonban vagy használatban lévő területre irányul és kizárólag meghatározott jogszerű célból.
f) Az adatkezelő igazolni tudja, hogy az alkalmazott elektronikus megfigyelőrendszer összeegyeztethető az Infotv. 4. § (1)-(2) bekezdésében szereplő célhoz kötöttség elvvel és érdekmérlegelés teszttel, miszerint személyes adatok kezelése kizárólag meghatározott célból, joggyakorlás és kötelezettség teljesítése érdekében történik.

g) Az adatkezelő elsősorban emberi élet, testi épség, személyi szabadság védelme, jelentős értéket képviselő áruk és eszközök, üzleti-, fizetési, bank- és értékpapírok, értéktárgyak vagyonvédelme érdekében alkalmazza a megfigyelő rendszert.
h) Az adatkezelő figyelemfelhívó jelzést köteles elhelyezni azokon a területeken, ahol kamerákat helyezett el.

4.2. A felvételek tárolása

A rögzített felvételeket az adatkezelő főszabályként 30 munkanapig tárolja, ennél hosszabb ideig történő felvételmegőrzés olyan kivételes eset, amikor a felvételeket a fent említett időtartamnál hosszabb ideig szükséges megőrizni. Ennek okát az adatkezelő igazolni köteles.

i) A rögzített felvételeket az adatkezelő harmadik fél részére csak törvényben meghatározott esetben (pl. rendőrség, munkavédelmi hatóság részére) adja át.
j) A rögzített anyagokat kizárólag szabálysértés vagy bűncselekmény gyanúja, illetve munkahelyi baleset esetében lehet visszanézni.
k) A rögzített anyagokat bíróság vagy más hatóság előtt bizonyítékként fel lehet használni.
l) A digitálisan rögzített felvételeket külső hálózatokon keresztül nem lehet elérni, azokról mentés vagy másolat kizárólag a törvényben meghatározott esetben, pl. bűnügyi eljárás céljára készíthető.
m) A biztonsági kamerák folyamatosan üzemelnek. Azokat kikapcsolni, eltakarni vagy bármely módon a rögzítést akadályozni tilos.

4.3. A felvételek visszanézése

a) A felvételek visszanézésére döntési jogosultsággal rendelkező meghatározott személyi csoport rendelkezik jogosultsággal.
b) A felvételek visszanézésének okát, idejét és visszanézésére jogosult személy nevét jegyzőkönyvben kell rögzíteni.
c) Az adott Üzleti Partner látogatásával kapcsolatosan rögzített felvételek visszanézésénél az érintett Üzleti Partner képviselője, Munkavállaókkal kapcsolatban rögzített felvételek visszanézésénél érintett Munkavállaló jelenlétének jogát biztosítani kell, a képviselő, vagy Munkavállaló esetleges nyilatkozatainak jegyzőkönyvbe rögzítése mellett.
d) Az érintettek tájékoztatást kérhetnek a felvételek kezeléséről.

- A kamerákkal folyamatosan sugárzott képek megtekintésére jogosultak köre:
  - ügyvezető
  - területi vezető
  - személyzeti vezető
  - rendszergazda

A kamerák által készített és tárolásra került felvételek visszanézésére, mentés készítésére, felvételek törlésének felügyeletére jogosultak köre:

- ügyvezető
- személyzeti vezető
- rendszergazda egy felsorolt vezető jelenlétében.

4.4. Az adatbiztonsági intézkedések

e) A képfelvételek megtekintésére és visszanézésére szolgáló monitor úgy kerül elhelyezésre, hogy a képfelvételek sugárzása alatt azokat a jogosultsági körön kívül más személy ne láthassa.
f) A megfigyelést és a tárolt képfelvételek visszanézését kizárólag a jogsértő cselekmények kiszűrése, az azok megszüntetéséhez szükséges intézkedések kezdeményezése céljából lehet végezni.
g) A kamerák által sugárzott képekről a központi felvevő egységen kívül más eszközzel felvételt készíteni nem lehet.
h) A tárolt képfelvételekhez hozzáférés csak biztonságos módon, és akként történhet, hogy az adatkezelő személye azonosítható legyen. A tárolt képfelvételek visszanézését és a képfelvételekről készített mentést dokumentálni kell. A jogosultság indokának megszűnése esetén a tárolt képfelvételekhez a hozzáférést haladéktalanul meg kell szüntetni.
i) A képfelvételek rögzítése egy dedikált célhardveren történik. Az eszköz fizikailag zárt környezetben kerül elhelyezésre, a rendszerbe történő belépés felhasználónév/jelszó alapú hitelesítéshez kötött
j) Jogsértő cselekmény észlelését követően a cselekményről készült felvétel zárolása és a szükséges hatósági eljárás haladéktalan kezdeményezése felől intézkedni kell, egyben tájékoztatni kell a hatóságot, hogy a cselekményről képfelvétel készült.
k) A kamerás megfigyelő rendszer létéről és működéséről a bejáratoknál dolgozók, és egyéb látogatók által használt terekben is tájékoztatást kell adni.

5. Informatikai Biztonsági Szabályzat

Jelen szabályzat elválaszthatatlan mellékletét, részét képezi a HI-LEX Hungary Kft. Informatikai Biztonsági Szabályzata (IBSZ). Jelen szabályzat az IBSZ azon rendelkezéseit tartalmazza, melyek betartása kötelező erővel bír a Munkavállalókra, Munkatársakra vonatkozóan, és amelyek megszegése súlyos szerződésszegésnek minősül, ennek minden jogkövetkezményével.

III. RÉSZ

Felhasználói Szabályzat

Az alábbi szabályok az Informatikai Biztonsági Szabályzat felhasználókra vonatkozó kivonatát tartalmazzák. A kivonatban szereplő előírások minden „HI-LEX felhasználó" számára kötelező érvényűek. Ezek megismerése és betartása az informatikai rendszer használatának előfeltétele. „Felhasználó" alatt a szabályzat a HI-LEX Hungary Kft. informatikai rendszerét használó személyt érti, legyen az Munkavállaló, Munkatárs, egyéb harmadik személy.

1. Általános rendelkezések

1. Mind a Munkavállaló, mind a Munkatárs a Munkáltató érdekében végzett tevékenysége, illetve a Munkáltatóval fennálló jogviszonya során felmerülő, illetve tudomására jutott információkat, valamint Személyes és egyéb adatokat kizárólag a Munkáltató céljainak és érdekeinek megfelelően használhatja.
2. Minden, a Munkáltató működése során keletkező információt, valamint adatot a Munkavállaló és a Munkatárs köteles bizalmasan, a Munkáltatót illető üzleti titokként kezelni. Ennek megfelelően:

2.1. nem jogosult a Munkáltatóval fennálló jogviszonya fennállása alatt, sem ennek megszűnését követően – a Munkáltató kifejezett írásbeli hozzájárulása nélkül – bizalmas információt más tudomására hozni;

2.2. semmilyen körülmények között nem jogosult a bizalmas információt más célra, illetve másféle módon használni, mint amelyet az Munkáltató megállapított.

3. Mind a Munkavállaló, mind a Munkatárs köteles a hardware és szoftver eszközöket, adathordozókat, valamint az informatikai és telekommunikációs hálózat állagát megóvni, a bennük keletkezett hibákat haladéktalanul az Ügyvezető felé jelezni.

4. Mind a Munkavállaló, mind a Munkatárs a hardware és szoftver eszközöket, adathordozókat és az informatikai és telekommunikációs hálózatot kizárólag a Munkáltató céljainak és érdekeinek megfelelően használhatja.

5. Minden Munkavállaló és Munkatárs kötelessége, hogy amennyiben adatvédelmi incidens vagy a Munkáltató eszközeivel, adathordozóival vagy hálózataival kapcsolatos visszaélés jutott a tudomására, ennek tényét a közvetlen felettesének vagy a munkáltatói jogkör gyakorlójának (alvállalkozó esetén a szerződéses kapcsolattartójának), Személyes adatok érintettsége esetén pedig az adatgazdának is haladéktalanul jelezze.

6. Adatvédelmi incidens, valamint az informatikai biztonsággal kapcsolatos visszaélés, továbbá az informatikai biztonság sérelme esetén az észlelő személy a HR Vezetőt, és/vagy a Pénzügyi Vezetőt köteles haladéktalanul tájékoztatni.

7. Az adatok, adathordozók, a hardware és szoftver eszközök biztonságos tárolásáról, illetve az Munkáltató informatikai és telekommunikációs hálózatai biztonságáról mind a Munkavállalónak, mind a Munkatársnak kötelessége gondoskodni. Az erre alkalmas mobil eszközök rögzíthetősége érdekében az Munkáltató biztosítja az erre célra megfelelő zárakat, amelyek Munkavállaló ill. Munkatárs általi használata kötelező. A munkavégzéshez szükséges hardware és szoftver eszközök javíttatása és pótlása a Munkáltatót terheli, de ezek okának, és/vagy a felelősség kérdésének megállapítását az Ügyvezető kezdeményezheti, a kár megtéríttetését indokolt esetben elrendelheti.

8. A hardware és szoftver eszköz fogalomkörébe tartozó számítógépeken, szervereken kizárólag az Munkáltató tulajdonában lévő licencelt szoftver használható; a regisztrált konfigurációtól eltérő, nem rendszeresített szoftverek használata, illetve privát szoftverek telepítése, használata tilos. A Munkavállaló és a Munkatárs ettől csak az Ügyvezető/Pénzügyi Vezető írásbeli jóváhagyásával térhet el. A telepített szoftvereket az Munkáltató szúrópróba szerűen ellenőrzi.

9. A Munkavállaló ill. a Munkatárs birtokában lévő Személyes adatoknak a rendeltetésszerű Adatkezeléstől eltérő lemásolása, továbbá az Munkáltató szoftvereinek lemásolása, az adatoknak, illetve a Munkáltató szoftvereinek magáncélú felhasználása, a szoftverek nem rendeltetési helyükön való telepítése szigorúan tilos, és jogi következményeket von maga után.

2. A Felhasználó feladata és kötelessége:

1. Ismernie kell az IBSZ-ben megfogalmazott, rá vonatkozó előírásokat és be kell tartania azokat.

2. Rendelkeznie kell az általa használt eszközök és programok munkavégzéshez szükséges ismeretével.

3. Részt kell vennie adatvédelmi oktatáson és az ott elhangzottak alapján kell használnia az informatikai rendszert.

4. Tevékenysége befejezésekor a programokból szabályszerűen ki kell lépniük.

5. Be kell tartania a munkavégzés során a „tiszta asztal" szabályt.

6. A HI-LEX Hungary Kft. informatikai eszközeinek használatba vétele előtt elfogadja a cég vonatkozó adatkezelési és adatvédelemre vonatkozó szabályait.

7. A cég informatikai eszközeit nem használja magáncélra.

3. Programozott fenyegetés elleni védelem

1. A vírusfertőzések megelőzése céljából a HI-LEX Hungary Kft. informatikai rendszerében csak engedélyezett szoftverek alkalmazhatók.

2. Informatikai biztonsági oktatások keretében a felhasználókat, adminisztrátorokat és fejlesztőket vírusvédelemmel kapcsolatosan oktatásban, képzésben kell részesíteni.

3. A technikai lehetőségek figyelembevételével el kell érni, hogy a vírusvédelem komplex módon, és ne csak a rendszer végpontjait alkotó kliens számítógépeken működjön, hanem a klienseken és a szervereken egyaránt, operációs rendszertől függetlenül.

4. A vírusvédelmi eszközök minden technikai elemét úgy kell felépíteni, hogy biztosítható legyen a rendszeres, automatizált frissítés.

5. Az a felhasználó, aki az adatait és adathordozóit a vírusellenőrzés vagy a vírusvédelmi intézkedés (vírusirtás) alól bármilyen indokkal kivonja, az abból eredő károkért teljes anyagi és erkölcsi felelősséggel tartozik.

6. A vírusvédelmi eseményeket, amennyiben az automatizált védelmi rendszer ezeket nem tudta semlegesíteni incidensként kell kezelni és minden esetben ki kell vizsgálni. A vizsgálat során meg kell győződni arról, hogy van e olyan megoldás, amely képes lett volna a támadás semlegesítésére és azt lehetőség szerint alkalmazni kell.

7. A kritikus vírusvédelmi eseményeket (frissítési hiba, leállt védelmi szolgáltatás, vírustalálat) be kell vonni az automatizált riasztási rendszerbe.

8. A rendszerek automatizált naprakészen tartásáról az üzemeltetőnek gondoskodni kell.

9. Szoftvert, alkalmazásokat a felhasználók az internetről nem tölthetnek le, a hálózatról nem futtathatnak, külső adathordozón a cég területére nem hozhatnak be és nem telepíthetnek.

10. Telepítést (hardver, szoftver) csak az informatikai üzemeltető végezhet az informatikai üzemeltetésre vonatkozó mindenkor hatályos belső szabályok alapján.

11. A cég informatikai hálózatába levélmellékletként érkezett állományokat ellenőrizni kell, hogy nem tartalmaznak-e rosszindulatú kódot. A vírusvédelmi rendszernek alkalmasnak kell lennie arra, hogy a rosszindulatú kódot hordozó csatolmányt eltávolítsa, karanténba helyezze.

12. A felhasználók részéről a vírusellenőrző szoftver beállításainak módosítása tilos - ha megoldható ezeket a beállításokat jelszóhoz kell kötni.

13. Vírus felbukkanása esetén a szoftver kísérelje meg azt kiirtani, és értesítse az üzemeltetőt, de legalább a felhasználót.

14. Kárt okozó, rendszerek működését befolyásoló esemény vagy vírusfertőzés esetén a felhasználónak azonnal értesítést kell küldeni az üzemeltetőnek és le kell kapcsolnia a számítógépét. A beérkezett értesítés alapján az üzemeltető végzi el a vírusmentesítést.

15. A vírusvédelmi rendszert úgy kell kialakítani, hogy egy központi menedzsment kiszolgálóról lehetőség legyen az üzemeltetés ehhez kapcsolódó alábbi feladatainak elvégzésére:
    15.1. telepítés,
    15.2. eltávolítás, frissítés,
    15.3. policy módosítás,
    15.4. riportolás,riasztások beállítása

16. A rendszer a vírus találatokról a Rendszergazda számára automatizált riasztásokat kell, hogy generáljon.

17. A Rendszergazda napi feladata kell, hogy legyen a vírusvédelem működésének ellenőrzése.

4. Adathordozók kezelése

4.1. Az adathordozók kezelése:

1. A személyes adatokat, üzleti értékeket tartalmazó adathordozókat elkülönítetten, védett környezetben, illetve titkosított formában kell tárolni.

2. Az informatikai adathordozók (mágneses, optikai, stb.) eredeti, biztonsági, vagy archív másolatait az adattároló eszközök gyártója által előírt környezeti feltételeket biztosító tárolóeszközökben (doboz, kazetta, stb.) kell elhelyezni.

3. Abban az esetben, ha az adathordozó megközelíti (élettartam -10%) a gyártó által javasolt felhasználási időtartamot, az adathordozóról másolatot kell készíteni.

4. Az adathordozókon egyértelmű és egységes jelöléssel fel kell tüntetni a tárolt adatokra vonatkozó információt.

5. Külső szervezettől érkezett adathordozókat, csak ellenőrző eljárás, vírusvédelmi ellenőrzés lefolytatása után lehet további használatba venni.

4.2. Cserélhető adathordozók (USB drive) használata:

1. Cserélhető adathordozót csak előzetes titkosítás után szabad használni adattárolásra.

2. Amennyiben erre a technológia lehetőséget ad a titkosítást az operációs rendszerben ki kell kényszeríteni.

3. Titkosítás alá be nem vont adathordozón céges adatot, személyes adatot, illetve üzleti szempontból érzékeny egyéb adatot tilos tárolni.

4. Cserélhető adathordozóról céges adatot más, nem a HI-LEX tulajdonába tartozó számítógépre másolni csak a Pénzügyi Vezető engedélyével szabad.

5. Saját adathordozót csak az ügyvezető / Pénzügyi Vezető engedélyével szabad használni a HI-LEX informatikai rendszerében.

6. A titkosítási szabályokat saját adathordozó esetében sem szabad megkerülni.

7. Amennyiben egy munkakörnél nincs szükség cserélhető adathordozók használatára, ott ennek a lehetőségét le kell tiltani az operációs rendszerben.

4.3. Adathordozók selejtezése:

1. Amennyiben egy adathordozó selejtezésre kerül, az adathordozót vagy meg kell semmisíteni, vagy a teljes tárterületét legalább három alkalommal felül kell írni.

2. A selejtezés megtörténtét nyilvántartásban kell rögzíteni. A nyilvántartásnak tartalmaznia kell a selejtezés dátumát, az azt végző személy nevét és a selejtezés módját, valamint az eszköz további sorsát.

3. A selejtezési dokumentumot a Pénzügyi Vezetőnek is hitelesítenie kell.

5. Hardver eszközök védelme

1. A HI-LEX Hungary Kft-ben csak a vezetőség által engedélyezett hardver eszközök használhatók.

2. A használatban lévő hardver eszközöket nyilvántartásba kell venni. A nyilvántartás vezetése az üzemeltető feladata.

3. A hardver eszközök kikerülését a céges környezetből és/vagy személyes használatba adását dokumentálni kell az üzemeltetőnek.

4. Minden olyan eszköz esetében, amely adattárolásra alkalmas és kikerül az céges környezetből az adattároló tárterületet el kell titkosítani.

5. A hardver eszközök meghibásodását a felhasználónak azonnal jelentenie kell az üzemeltetőnek.

6. A hardver eszközöket garanciális ügyintézése a Rendszergazda feladata.

7. Minden Kritikus fontosságú rendszerelem esetében rendelkezni kell gyártói garanciával. Ennek nyilvántartása a Rendszergazda feladata.

8. Külső szolgáltató által biztosított hardver eszközökre olyan szerződést kell kötni, amely biztosítja az eszközök garanciális hibajavítását.

6. Elektronikus levelezés védelme

1. Az elektronikus levelezés, mint szolgáltatás a HI-LEX Hungary Kft. nem minden munkatársának jár.

2. Az elektronikus levelezést a cég felhőszolgáltatásként veszi igénybe.

3. A cég jogosult a levelező rendszerben továbbított üzenetet a feladó, vagy címzett kiszolgáltatása nélkül a hatóság számára jogszabályi megalapozottság esetén átadni.

4. Különleges és indokolt esetben az Ügyvezető és a Pénzügyi Vezető jogosult az elektronikus leveleket megtekinteni. A betekintésről minden esetben jegyzőkönyvet kell készíteni. A betekintés során minden esetben be kell tartani a fokozatosság elvét, melynek során először csak a levelek fejlécét vizsgálják át és csak indokolt esetben tekintik meg a levél tartalmát.

5. Az egymás levelezésének megtekintése minden más esetben tilos.

6. A felhasználó tudomásul veszi, hogy a központi levelezés során a felhasználó levelezési forgalma naplózásra kerül.

7. Tilos bármilyen céges levelezés, illetve annak résztartalmának továbbítása a Felhasználó magán emailcímére, illetve céges információ továbbítása bármilyen nem a HI-LEX Hungary Kft. birtokában lévő emailcímről.

8. A levelek fogadásakor, megnyitás előtt a Felhasználó próbáljon meggyőződni arról, hogy a levél valós feladótól érkezett.

9. Ismeretlen feladótól érkező levelekhez csatolt fájlok megnyitása tilos. Ilyen esetben a Felhasználó azonnal értesítse a Rendszergazdát.

10. Tilos vírusos levelek, illetve tartalom szándékos küldése.

11. A levelezési rendszeren tilos biztonsági szempontból érzékeny anyagot, üzleti titkot illetéktelen személy részére küldeni.

12. Tilos a levelezési rendszeren keresztül olyan tartalmú levelet küldeni, amely bármilyen más személy, csoport vagy társaság személyes érdekeit sértheti.

13. A felhasználó csak saját nevében küldhet levelet, kivéve, ha erre felelős vezető utasítja.

14. Tilos az elektronikus levelek oly módon történő titkosítása, hogy a visszafejtésre használható kulcs nincsen a Munkáltató birtokában.

15. Tilos a levelező rendszer nem a Munkáltató érdekében végzett tevékenységhez kapcsolódó, nagy terjedelmű vagy nagy mennyiségű levelek, illetve kéretlen kereskedelmi üzenetek küldésére történő használata.

16. Tilos rasszista, szemérmet és jó ízlést sértő, valamint szélsőséges politikai nézeteket képviselő tartalmú levelet küldeni.

17. Tilos másokra nézve sértő, vallási, etnikai, politikai, vagy más jelleg érzékenységet bántó, zaklató tevékenység (pl. pornográf/pedofil anyagok) közzététele.

18. Tilos a levelezőrendszer reklám, hirdetés – ide nem értve a Munkáltató tevékenységéhez kapcsolódó promóciót – céljára, mások munkájának hátráltatására, illetve internetes szolgáltatások veszélyeztetésére történő használata.

19. A felhasználóknak tilos lánclevelet, rémhíreket küldeniük a központi levelező rendszeren keresztül.

20. A levelező kliens minden esetben csak titkosított, hitelesített kapcsolaton keresztül érheti el a szolgáltatót.

21. A levelezési jelszavakat a felhasználók kötelesek bizalmasan kezelni.

7. Adatmentés

1. A munkaállomások nem kerülnek mentésre. Ez okból a munkaállomásokon nem tárolható olyan érzékeny adat, amely nem található meg a mentett környezetben.

2. A fontos adatokat minden esetben a fájlmegosztásokon kell tárolni. Ideiglenesen lemásolhatók off-line munkavégzés céljából, azonban amint lehetséges a módosított állományt vissza kell menteni a megfelelő hálózati megosztásra.

8. Internet elérés szabályozása

8.1. Az internet elérésre vonatkozó felhasználói szabályok:

1. A felhasználó nem tehet közzé az interneten a cégről publikusan nem elérhető információkat.

2. A felhasználók nem használhatják céges emailcímüket olyan oldalakra történő feliratkozásra, mely nem a munkavégzésükhöz kapcsolódik.

3. Alkalmazások és böngészőbe épülő modulok felhasználók általi telepítése nem engedélyezett.

4. Fájlcsere szolgáltatás működtetése céges számítógépen tilos.

5. Dark-web, ártó kódokat tartalmazható, vagy illegális tartalmú oldalak tudatos felkeresése céges számítógépről tilos.

6. Helyi rendszergazdai jogokkal történő internetezés tilos.

7. Csak olyan gépről engedélyezett az internet elérése, mely naprakész vírusvédelemmel rendelkezik.

8. A cég által kezelt személyes adatok, illetve bizalmas információk külső levelező rendszeren keresztüli továbbítása tilos.

8.2. Közösségi média használata:

1. A közösségi média használata nem történhet a munkával kapcsolatos kötelezettségek teljesítésének rovására.

2. A közösségi média felületeken tilos bármilyen olyan tartalom közzététele, amely alkalmas lehet a Munkáltató jó hírnevének, jogos gazdasági érdekének veszélyeztetésére.

3. A közösségi média felületeket tilos mások bárminemű zaklatására, megfenyegetésére, rágalmazására vagy becsmérlésére használni.

4. Tilos különösen megosztani a közösségi média felületeken a Munkáltató által "üzleti titoknak" és/vagy "szigorúan bizalmasnak" minősített információkat, ide értve az Munkáltató belső működésére, folyamataira, infrastruktúrájára, vezetőségére, munkavállalóira vonatkozó információkat is, kivéve azt az esetet, amikor a Munkáltató, vagy a Munkáltató megbízottja a belső kommunikáció támogatására a Munkáltató által meghívott résztvevőkkel működő, nem nyilvános közösségi csatornát üzemeltet.

5. Tilos továbbá a közösségi média felületeken megosztani a munkavégzéséhez kapcsolódóan kezelt Személyes adatokat, beleértve a jelszavakat is.

6. Kizárólag a Munkáltató előzetes hozzájárulásával, és a Munkáltató által meghatározott felületeken és feltételek mellett szabad a Munkáltató székhelyén, telephelyein és irodáiban készült fényképeket, hang- és videó felvételeket és egyéb információkat megosztani.

9. Jelszókezelés

1. A felhasználók részére központilag ki kell kényszeríteni a biztonságos jelszó policy-t.

2. Minden felhasználó jelszavát illetéktelenektől gondosan védeni kell.

3. A felhasználók jelszavát a felhasználón kívül senki sem ismerheti.

4. Amennyiben lehetséges, az egyes rendszerek esetében be kell vezetni a központi címtárba történő hitelesítést és a címtárban tárolt jelszó alkalmazását.

5. A jelszavakra az alábbi céges szabályok érvényesek, minden HI-LEX által használt informatikai rendszer esetében:
   5.1. Jelszóhossz: minimum 10 karakter
   5.2. Bonyolultság: kisbetű, nagybetű, szám
   5.3. Érvényesség minimum: 1 nap
   5.4. Érvényesség maximum: 90 nap
   5.5. Jelszótörténet: 6 jelszó

6. A jelszót soron kívül meg kell változtatni, ha az illetéktelen (más) személy tudomására jutott, illetve juthatott, vagy a felhasználó azt elfelejtette.

7. Olyan rendszereket szabad csak bevezetni, melyek a jelszavakat minden esetben kódoltan tárolják.

8. A technikai felhasználók és az alapértelmezett adminisztrátor fiókok jelszavát nagy bonyolultságúra kell állítani, és zárt, védett helyen (pl: páncélszekrény, borítékban) kell tárolni.

9. Az olyan automatizált programokban, ahol a technikai felhasználók jelszavai rögzítve megjelenhetnek kódolt tárolást kell alkalmazni, illetve a fájlok olvasási hozzáférését korlátozni kell.

10. Felhasználói felelősségek megállapítása

1. A HI-LEX Hungary Kft. felhasználóinak felelőssége, hogy az informatikai rendszer elemeit csak a biztonsági szabályoknak megfelelően használják.

2. Arra az esetre, ha a felhasználó napközben magára hagyja a gépét, zárolást vagy jelszavas képernyővédőt kell alkalmaznia. A képernyő zárolását központi policy alkalmazásával, 10 perces várakozási idővel ki kell kényszeríteni.

3. A munkaidő végén a felhasználóknak a „tiszta asztal" elvet kell alkalmazniuk. Érzékeny adatot tartalmazó dokumentumokat minden esetben elzárva kell tartaniuk.

4. A munkaidő végén a kliensgépeket minden esetben szabályosan le kell állítaniuk.

5. Amennyiben egy felhasználó nem tartja be a céges biztonsági előírásokat és ezért a cég adatvagyona, jóhíre, üzleti folyamatai sérülnek, a felhasználónak felelősséget kell vállalnia az okozott kárért.

6. Ilyen esetben a felelősségek megállapítása az Ügyvezető és az Pénzügyi Vezető együttes jelenlétében kell, hogy történjen.

Jelen Szabályzat a HI-LEX Hungary Kft. 2018. május 25. napjától hatályos szabályzata.

Kihírdetve a 2/2018 számú munkáltatói utasítással.

Kelt: Budapest, 2018. május 25.

.....

HI-LEX Hungary Kft. ügyvezetője