A SEMILAB FÉLVEZETŐ FIZIKAI LABORATÓRIUM ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

ADATVÉDELMI SZABÁLYZATA

A Szabályzatot jóváhagyom és annak alkalmazását jelen változat hatálybalépési dátumával elrendelem:

_____

dr. Pavelka Tibor László
vezérigazgató

Hatálybalépés napja: 2021. március 01.

Tartalomjegyzék

A SEMILAB Zrt. (a továbbiakban: „**Adatkezelő**”, „**Társaság**”) tevékenysége során fokozottan ügyel a személyes adatok védelmére, a kötelező jogi rendelkezések betartására, a biztonságos és tisztességes adatkezelésre.

Az Adatkezelő fontosnak tartja a Társasággal bármely módon kapcsolatba kerülő érintett természetes személy (a továbbiakban: „**Érintett**”) adatkezeléshez kapcsolódó jogainak tiszteletben tartását és azok érvényre juttatását. Az Adatkezelő ezért kötelezettséget vállal arra, hogy tevékenységével, szolgáltatásával kapcsolatos adatkezelése megfelel jelen Szabályzatban és a hatályos jogszabályokban meghatározott elvárásoknak.

Az Adatkezelő a fentiekre tekintettel a belső adatkezelési folyamatai jogszerűségének biztosítása, nyilvántartása és az érintettek jogainak biztosítása céljából az alábbi adatvédelmi Szabályzatot (a továbbiakban: „**Adatvédelmi Szabályzat**”, „**Szabályzat**”) alkotja.

Adatkezelő megnevezése:	SEMILAB Félvezető Fizikai Laboratórium Zrt.
Adatkezelő cégjegyzékszáma:	01-10-041351
Adatkezelő adószáma:	10311765-2-44
Adatkezelő székhelye:	1117 Budapest, Prielle Kornélia utca 4/A.
Adatkezelő képviselője:	dr. Pavelka Tibor László, vezérigazgató
Adatkezelő képviselőjének elérhetősége:	gdpr@semilab.hu

Jelen rendelkezéseket a Társaság többi szabályzatának előírásaival összhangban kell értelmezni. Amennyiben a személyes adatok védelmével kapcsolatosan ellentmondás áll fent jelen rendelkezések és a bármely más, jelen szabályzat hatálybalépése előtt hatályba lépett szabályzat előírásai között, úgy abban az esetben jelen rendelkezések az irányadóak.

1. A szabályzat célja

A Társaság jelen Szabályzat megalkotásával és elérhetővé tételével biztosítani kívánja az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: „**GDPR**”) 13-14. cikkeiben meghatározott érintetti tájékoztatáshoz való jog megvalósulását. A Szabályzat célja, hogy alkalmazásával a Társaság megfeleljen az GDPR, és a személyes adatok kezelését érintő magyar jogszabályokban foglalt rendelkezéseknek, így az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: „**Infotv**.”) rendelkezéseinek.

A Szabályzat lefekteti a Társaságnál zajló adatkezelések törvényes kereteit, biztosítja az adatvédelem alkotmányos elveinek és az információs önrendelkezési jognak az érvényesítését, elősegíti az adatbiztonság követelményeinek való megfelelést, továbbá megakadályozza a jogosulatlan adatkezelést, kialakítja az adatvédelem szempontjából fontos feladatokat, felelősségi viszonyokat az adatbiztonságban. A Szabályzat célja továbbá a Társaság által adatkezelői, illetve adatfeldolgozói minőségben kezelt és feldolgozott személyes adatok védelmi rendszerének kiépítése és működtetése.

Jelen Szabályzat célja, hogy az érintettek megfelelő tájékoztatást kaphassanak a Társaság által kezelt, illetve az általa megbízott adatfeldolgozó által feldolgozott adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről, valamint az érintett jogairól.

Fentiekre tekintettel az Adatkezelő a Szabályzat által meghatározott adatvédelmi rendszer és az adatvédelemre vonatkozó adatvédelmi gyakorlat kialakításával a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.

Jelen Szabályzattal a Társaság biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését.

Az Adatkezelő által kezelt és feldolgozott személyes adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, véletlen megsemmisülés és sérülés, valamint az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen. Az elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban kezelt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

A Szabályzat mindenkor hatályos változata elérhető a Társaság székhelyén.

A Szabályzattal és annak értelmezésével összefüggésben felmerülő kérdésekkel, illetve az esetleges problémákkal kapcsolatban bővebb tájékoztatás kérhető az Adatkezelőtől az alábbi elérhetőségen: gdpr@semilab.hu.

2. A szabályzat hatálya

A Szabályzat időbeli hatálya 2021. március 01. napjától visszavonásig tart. Az Adatkezelő kiemelten fontosnak tartja a tevékenységével összefüggésben megvalósuló adatkezelés magyarországi jogszabályi feltételeinek való megfelelést és fenntartja magának a jogot jelen Szabályzat megváltoztatására, azzal, hogy a módosított szabályzatot nyilvánosan – székhelyén – közzéteszi.

Jelen Szabályzat személyi hatálya kiterjed a Társasággal munkaviszonyban álló személyekre, továbbá a Társasággal bármely polgári jogi szerződéses jogviszonyban álló természetes személyre és jogi személyre, akiknek a személyes adatát kezeli a Társaság, vonatkozik továbbá a Szabályzat a Társaság vezető tisztségviselőire is.

A fentieknek megfelelően az Adatkezelővel kötendő szerződésekben – az Adatkezelővel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és egyéb szervezetek és ezek alkalmazottai vonatkozásában – biztosítani kell a jelen Szabályzat rendelkezéseinek érvényesülését, ideértve az adatfeldolgozási, adatbiztonsági, továbbá incidenskezelési rendelkezéseket, illetve szükség esetén és szükség szerint biztosítani kell, hogy az érintett személyek a Szabályzatot (eseti kivonatát) a szükséges mértékben megismerjék.

Jelen Szabályzat alkalmazásában az egyéni vállalkozókat, illetve az adószámos magánszemélyként gazdasági tevékenységet végző személyeket természetes személynek kell tekinteni.

A Szabályzat személyi hatálya nem terjed ki azonban a jogi személyeknek, bármely közhiteles nyilvántartás részét képező, illetve abban szerepelő adataira, így a jogi személy nevére és formájára, valamint a jogi személy elérhetőségére vonatkozó adatokra.

A Szabályzat tárgyi hatálya kiterjed az Adatkezelő által kezelt valamennyi – természetes személyhez köthető – személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül, továbbá az Adatkezelő székhelyén, telephelyén folyó, bármely szervezeti egységénél folytatott – kizárólag természetes személyeket érintő – valamennyi számítógépes és manuális adatkezelésre, adattovábbításra, információ átadásra, illetve ezek tárgyát képező adat jelen Szabályzatban meghatározottak szerinti, üzleti titokként kezelésével- védelmével kapcsolatos tevékenységekre, az Adatkezelő által igénybe vett adatfeldolgozók felé irányuló adatáramlásra, és más Adatkezelőkkel való személyes adatokat érintő kommunikációra.

3. Irányadó jogszabályok

A Szabályzatot – különösen – az alábbi jogszabályokkal összhangban kell alkalmazni:

- GDPR
- Infotv.
- a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: „**Szvt.**”);
- a Munka Törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: „**Mt**.”);
- a számvitelről szóló 2000. évi C. törvény (a továbbiakban: „**Sztv**.”);
- az adózás rendjéről szóló 2017. évi CL. törvény (a továbbiakban: „**Art**.”);
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: „**Ptk.**”);
- az üzleti titok védelméről szóló 2018. évi LIV. törvény (a továbbiakban: „**Üttv**.”).

A Szabályzatot – különösen – az alábbi belső szabályozó eszközökkel összhangban kell alkalmazni:

- Információbiztonsági Szabályzat

4. Fogalmak

- ***Érintett*:** bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.
- ***Személyes adat***: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.
- ***Különleges adat:*** A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.
- ***Egészségügyi adat:*** egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

- ***Hozzájárulás:*** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
- ***Adatkezelő:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja.
- ***Adatkezelés:*** az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.
- ***Adatfeldolgozás:*** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.
- ***Adatfeldolgozó:*** az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.
- ***Adattovábbítás*****:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele, nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele.
- ***Harmadik személy:*** olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki, vagy amely nem azonos az érintettel, az Adatkezelővel vagy az adatfeldolgozóval.
- ***Harmadik ország:*** minden olyan állam, amely nem EGT-állam.
- ***Címzett:*** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak.
- ***EGT-tagállam***: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez.
- ***Adatvédelmi incidens:*** a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
- ***Tiltakozás***: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri.
- ***Adattörlés***: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges.
- ***Adatmegjelölés***: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.
- ***Adatmegsemmisítés***: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése.

- ***Üzleti titok***: a gazdasági tevékenységhez kapcsolódó, titkos - egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető -, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.

Amennyiben a mindenkori hatályos adatvédelmi jogszabály (jelen szabályzat megalkotásakor a GDPR) fogalommagyarázatai eltérnek jelen Szabályzat fogalommagyarázataitól, akkor a jogszabály által meghatározott fogalmak az irányadóak.

5. A szabályzat kötelező felülvizsgálata

Jelen Szabályzatot a Társaság vezérigazgatója jogosult jóváhagyni.

A GDPR által támasztott elvárás, hogy a Társaság annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, törlési vagy rendszeres felülvizsgálati határidőket állapítson meg.

Jelen Szabályzatot a fenti elvárásnak megfelelően kötelezően felülvizsgálandó:

- a hatályossá válását követő minden évben,
- jogszabályi változásokat, illetve jelentős szervezeti változásokat követően, illetve
- amennyiben az adatkezelések változása indokolja, vagy új adatkezelés kerül bevezetésre.

A szabályzat felülvizsgálatáért a Társaság Adatvédelmi managere felelős.

6. A Társaság adatkezelésének elvei, szabályai

Mivel az információs önrendelkezés minden természetes személy Alaptörvényben rögzített alapjoga, így a Társaság az egyes adatkezelései, illetve az adatkezelésre vonatkozó eljárásai tekintetében kiemelten fontosnak tartja, hogy azok csak és kizárólag a hatályos jogszabályok rendelkezéseinek megfelelően, továbbá az alábbi alapelvek szem előtt tartásával végezze, illetve gyakorlatát ezeknek megfelelően alakítsa ki:

- ***Jogszerűség, tisztességesség és átláthatóság*** elvére tekintettel a Társaság a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon, jog gyakorlása vagy kötelezettség teljesítése érdekében végzi. A Társaság által kezelt személyes adatok magáncélra való felhasználását a Társaság szigorúan tiltja;

- ***Célhoz kötöttség*** elvére tekintettel a Társaság a személyes adatok gyűjtését, kezelését csak meghatározott, egyértelmű és jogszerű célból, a cél eléréséhez szükséges minimális mértékben és ideig végzi, és azokat nem kezeli az ezekkel a célokkal össze nem egyeztethető módon. Ennek megfelelően a Társaság kizárólag a gyűjtés idején közölt célokra vagy a törvénnyel összhangban egyéb megfelelő célokra használja fel az érintettek személyes adatait.

A Társaság különös figyelmet fordít arra, hogy adatkezelése mindenkor megfeleljen a célhoz kötöttség alapelvének, és amennyiben az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatok törlésre kerüljenek. Ha a továbbiakban már nincs szükség a személyes adatra, azokat a Társaság biztonságos módon és dokumentáltan megsemmisíti. A törlési jegyzőkönyveket 10 évig őrzi a Társaság.

- ***Adatminőség (adattakarékosság és pontosság)*** elvére tekintettel a Társaság az általa végzett adatkezelés során, csak az adatkezelés céljai szempontjából megfelelő, releváns és szükséges mennyiségű személyes adatot kezel, illetve gyűjt. A Társaság továbbá észszerű intézkedéseket tesz annak biztosítása érdekében, hogy a személyes adatok pontosak, teljes körűek és naprakészek legyenek, valamint, hogy az adatkezelés szempontjából szükségtelen személyes adatok törlésre kerüljenek.

- ***Korlátozott tárolhatóság*** elvének megfelelően a Társaság az érintettek azonosítását lehetővé tevő személyes adatokat csak az adatkezelés céljainak eléréséhez szükséges ideig kezeli. Az adatkezelési cél megváltozását vagy megszűnését követően a Társaság gondoskodik az adatok törléséről. A személyes adatokat a Társaság ennél hosszabb ideig csak abban az esetben tárolja, tárolhatja amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor. A személyes adatokat tartalmazó adathordozók selejtezésekor különös gondossággal jár el.

- ***Integritás és bizalmas jelleg*** elvére tekintettel a Társaság biztosítja a személyes adatok zárt, teljes körű, folytonos és kockázatokkal arányos védelmét, szervezési és technikai intézkedéseket tesz különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelem kialakítása érdekében. Az adatok jogosulatlan felhasználás vagy közzététel elleni védelme érdekében a Társaság adatbiztonsági ellenőrzéseket alkalmaz a saját tevékenységei során.

  A Társaság által megtervezett és megvalósított információbiztonsági intézkedések biztosítják a személyes adatok bizalmas jellegét, integritását és rendelkezésre állását. Ezeket az intézkedéseket a Társaság Információbiztonsági Szabályzata tartalmazza.

- ***Elszámoltathatóság*** elvére tekintettel a Társaság az adatkezelési folyamatait úgy tervezi és hajtja végre, adatkezelési rendszerét úgy alakítja ki, hogy az adatkezelés bármely pillanatában képes legyen a jelen pontba foglalt elveknek való megfelelést igazolni, így különösen, hogy mikor, milyen formában történt a személyes adat felvétele és milyen tájékoztatást kapott az érintett a személyes adat felvételekor.

A Társaság a GDPR 13. és 14. cikke szerint megfelelően tájékoztatja az érintetteket.

A Társaság adatkezelői minőségében köteles biztosítani, hogy az érintett a Társaság által kezelt adataihoz - ha a törvény kivételt nem tesz - hozzáférjen, gyakorolhassa a tájékoztatáskéréshez, hozzáféréshez, a helyesbítéshez, a korlátozáshoz, a törléshez, az adathordozhatósághoz, illetve a tiltakozási jogát.

A Társaság által adatfeldolgozói minőségében kezelt személyes adatok tekintetében az érintett jogainak biztosítása a Társaságot az adatkezeléssel megbízó adatkezelő kötelezettsége.

A személyes adatok kezelésében közreműködő munkatársak, illetve minden esetlegesen a Társasággal egyéb szerződéses viszonyban álló személyek (alvállalkozók, megbízottak, stb.), akik a Társaság által valamely formában kezelt személyes adatokat megismerik, kötelesek a személyes adatok védelmére vonatkozó jogszabályok és jelen Szabályzat rendelkezéseit megismerni és maradéktalanul betartani. Az adatvédelmi szabályok megsértői — a vonatkozó jogszabályok rendelkezéseinek megfelelően — fegyelmi, szabálysértési, polgári jogi és büntetőjogi felelősséggel tartoznak.

Ha a Szabályzat hatálya alatt álló személy tudomást szerez arról, hogy a Társaság által kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

7. A Társaság adatvédelmi rendszere

7.1. Vezérigazgató

A Társaság vezérigazgatója a Társaság sajátosságainak figyelembevételével meghatározza az adatvédelem szervezetét, az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat- és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt, illetve az adatkezelési cél eléréséhez szükséges erőforrásokat biztosítja.

A Szabályzat végrehajtásáért, illetve az abban foglaltak betartásáért saját területükön az egyes szervezeti egységek/területek vezetői a felelősek, akik a Társaság vezérigazgatója felé tartoznak elszámolással.

A vezérigazgató az adatvédelemmel kapcsolatosan:

a) felelős az érintettek GDPR-ban meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
b) felelős a Társaság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
c) felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért;
d) kijelöli az adatvédelmi kérdések tárgyában hatáskörrel rendelkező személyt, valamint kinevezi az Adatvédelmi managert;
e) döntést hoz az Adatvédelmi manager által előkészített adatvédelemmel kapcsolatos kérdésekben;
f) kiadja a Társaság adatvédelemmel kapcsolatos belső szabályait;
g) rendszeresen ellenőrzi az adatvédelmi folyamatokat a Társaságnál az Adatvédelmi managerrel együttműködve;
h) aktívan részt vesz az Adatvédelmi incidenskezelési eljárásban és minden támogatást megad annak érdekében, hogy az esetlegesen bekövetkezett adatvédelmi incidens kivizsgálása a GDPR-nak megfelelően megtörténjen.

7.2. Adatvédelmi manager

A Társaság adatvédelmi rendszerének felügyeletét a vezérigazgató az általa kinevezett vagy megbízott Adatvédelmi manager útján látja el.

Az Adatvédelmi manager jogállása és feladatköre nem azonos a GDPR 38. és 39. cikkében meghatározott Adatvédelmi tisztviselő jogállásával, még akkor sem, ha – egészben vagy részben – azokat a feladatokat elvégzi.

Az Adatvédelmi manager a személyes adatok védelme területén szerzett ismeretei és gyakorlati tapasztalatai, valamint az adatvédelmi feladatok ellátására való alkalmasság alapján jelölhető ki.

A Társaság biztosítja, hogy az Adatvédelmi manager a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.

A Társaság támogatja az Adatvédelmi manager feladatainak ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi manager szakértői szintű ismereteinek fenntartásához szükségesek.

Az Adatvédelmi manager közvetlenül a Társaság vezérigazgatójának tartozik felelősséggel.

Amennyiben az Adatvédelmi manager más feladatokat is ellát, a Társaság a vezetőséggel együtt biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

Az Adatvédelmi manager hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza, legalább az alábbi feltételekkel:

- az adatvédelemmel kapcsolatos nyilvántartások vezetése;
- tájékoztat és szakmai tanácsot ad a Társaság, illetve adatkezelést végző alkalmazottai részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;
- az érintetti jogok gyakorlására irányuló kérelmek kezelése, segítségnyújtás az érintettek számára az adatkezeléssel, vagy jogaikkal kapcsolatban felmerült kérdésük kapcsán;
- az adatvédelmi incidensek kezelése;
- ellenőrzi a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is és jelen Szabályzat rendelkezéseinek betartását;
- a Társaság munkavállalóinak adatvédelmi tudatosságának biztosítása és növelése érdekében, a megfelelő szintű adatvédelmi oktatás megtartásáról gondoskodik, akár külső szolgáltató közreműködésével;
- adatvédelmi hatásvizsgálatok lefolytatása esetlegesen az érintett szakterületi képviselő igénybevételével;
- figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen Szabályzat módosítását;
- segíti a Társaság felügyeleti hatósággal való együttműködését.

Valamennyi munkavállaló kötelezettsége annak bejelentése, ha a Szabályzat megkerüléséről vagy megsértéséről szerez tudomást vagy ennek gyanúja merül fel. A bejelentés megtehető az Adatvédelmi manager megkeresésével is.

A Társaság mindenkori Adatvédelmi managerének nevét és elérhetőségét jelen Szabályzat 1. sz. melléklete tartalmazza. Amennyiben az Adatvédelmi manager személye, esetleg elérhetősége módosul, úgy a Társaság haladéktalanul intézkedik a változás átvezetéséről az 1. sz. mellékletben, a változás átvezetése nem tekintendő a jelen Szabályzat módosításának.

7.3. Adatkezelési folyamatgazda

A Társaság az adatkezelési nyilvántartásában minden azonos céllal rendelkező adatkezeléshez egy adatkezelési folyamatgazdát jelöl ki.

Az Adatkezelési folyamatgazda az általa felügyelt adatkezelés során felelős:

- a kezelt adatokhoz történő hozzáférések engedélyezéséért, a hozzáférések visszavonásáért és a hozzáférések rendszeres, minimum évente egy alkalommal történő felülvizsgálatáért;
- az egyes lépések meghatározásáért, ezek dokumentálásáért;
- jelen Szabályzat vagy a GDPR elvárásainak változása esetén a folyamaton belül a szükséges változtatások végrehajtásáért és dokumentálásáért, és
- a feltárt adatkezelési gyengeségek jelentéséért az Adatkezelési manager részére írásban.

7.4. Adatkezelésre feljogosított személyek

A Társaság szervezeti egységeinél adatkezelést végző alkalmazottak és a Társaság megbízásából az adatkezelésben résztvevő személyek (például: adatfeldolgozók), illetve alkalmazottaik, kötelesek a megismert személyes adatokat korlátlan ideig titokban tartani és megőrizni, valamint megfelelő titoktartási kötelezettségvállalást tenni.

Fontos, hogy a Társaság munkavállalói a munkaviszonyuk kezdetekor titoktartási kötelezettségvállalást tesznek az illetékes HR munkatárs közreműködése által. Amennyiben valamely munkavállaló a munkaviszonyának létesítésekor nem vállalt titoktartási kötelezettséget, úgy jelen Szabályzat hatályba lépését követő 30 napon belül köteles jelentkezni a HR osztálynál a titoktartási kötelezettségvállalás pótlása érdekében.

8. Adatkezelés tervezése

Személyes adatok kezelésével járó új tevékenységek bevezetésekor az alábbi feladatokat kell elvégeznie a Társaság vezérigazgatójának és az Adatvédelmi managernek együttműködve:

a) meg kell határozni:
    1. a kezelendő személyes adatok körét;
    2. az adatok kezelésének célját;
    3. az adatkezelés jogalapját;
    4. az adatkezelés időtartamát;
b) fel kell mérni, hogy az adatok milyen informatikai rendszerben lesznek kezelve, az adatok milyen informatikai rendszerben jelennek meg;
c) meg kell határozni, hogy előre láthatóan az adatokhoz kinek szükséges hozzáférnie az Társaságon belül, illetve kívül;
d) be kell mutatni, hogy az adatokat szükséges-e továbbítani más személy számára;
e) be kell mutatni, hogy az adatkezeléshez igénybe kell-e venni adatfeldolgozót, amennyiben igen, az adatfeldolgozó feladata mi lesz, várhatóan ki lesz az adatfeldolgozó;
f) meg kell határozni, szükséges-e adatvédelmi hatásvizsgálat lefolytatása;
g) meg kell határozni az adatkezelés megkezdésének tervezett időpontját, az adatok felvételének módját és pontos helyét (pl.: erre szolgáló internetes felület vagy papír alapú adatfelvétel).

9. Az adatkezelés jogszerűsége

A Társaság a személyes adatok kezelését csak akkor végzi, amennyiben a GDPR 6. cikk (1) bekezdésében meghatározott jogalapok közül legalább az egyik alkalmazásának lehetősége fennáll az adatkezelés tekintetében, illetve a különleges adatok esetén amennyiben az adatkezelésnek a GDPR 9. cikk (2) és (3) bekezdéseiben foglalt feltétele(i) teljesülnek.

A GDPR 6. cikke alapján **személyes adatok** kezelése tehát legalább az alábbi jogalapok egyikének megléte esetén kezelhető:

- 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 közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához 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, különösen, ha az érintett gyermek.

Különleges személyes adatokat a Társaság – figyelembe véve a GDPR 9. cikkében foglalt rendelkezéseket – abban az esetben kezel, ha annak fennállnak a GDPR 9. cikk (2) és (3) bekezdésében meghatározott feltételei, így különösen:

- az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez;
- az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges;
- az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
- az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;

- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges és ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki (szakmai) titoktartási kötelezettség hatálya alatt áll.

A Társaság a személyes adatok különleges kategóriáit csak a legszükségesebb, elkerülhetetlen esetekben kezeli.

A **16. életévét be nem töltött gyermek** személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte. A Társaság – figyelembe véve az elérhető technológiát – észszerű erőfeszítéseket tesz, hogy ilyen esetekben ellenőrizze, hogy a hozzájárulást a gyermek feletti szülői felügyeleti jog gyakorlója adta meg, illetve engedélyezte.

A Társaság tevékenysége során főszabály szerint az alábbi jogalapokra tekintettel kezeli a személyes adatokat:

9.1. Hozzájárulás jogalap alkalmazása

A GDPR 6. cikk (1) bekezdésének a) pontja, valamint a GDPR 9. cikk (2) bekezdés a) pontja alapján kezelheti a Társaság az érintett (különleges) személyes adatait, ha az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.

Az érintetti hozzájáruláson alapuló adatkezelést megelőzően a Társaság köteles az érintettet tájékoztatni az adatkezelésre vonatkozó – a GDPR. 13. valamint 14. cikkében meghatározott – releváns tényekről, ennek hiányában ugyanis az érintetti hozzájárulás nem tekinthető megadottnak, hiszen ezen információk hiányában érdemi döntést nem tud hozni az adatai tekintetében.

A hozzájárulás érvényességének feltétele továbbá az önkéntesség, ezért

- az „érintett hozzájárulása jogalap" a Társaság munkavállalói esetében főszabály szerint nem alkalmazható (a jogi függőség miatt az önkéntesség nem biztosítható); és
- annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, hogy a szerződés teljesítésének feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

A hozzájárulási nyilatkozatnak – függetlenül annak megjelenési formájától – teljesítenie kell a következő feltételeket:

- legyen egyértelmű;
- más ügyektől elkülöníthető;
- érhető, világos, egyszerű nyelvezetű.

Az érintettet az adatkezeléshez való hozzájárulását bármikor visszavonhatja, erről a jogáról, illetve a visszavonás módjáról a hozzájárulási nyilatkozatban vagy az ezzel egyidőben átadott adatkezelési tájékoztatóban kell tájékoztatni. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

9.2. Szerződéses jogalap alkalmazása

A GDPR 6. cikk (1) bekezdés b) pontjára tekintettel a Társaság megfelelő jogalappal rendelkezik az adatkezelésre vonatkozóan, amennyiben 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. Szerződéskötésre irányuló közvetlen cselekmények esetében (ajánlatkérés, ajánlatadás, szerződéses feltételek egyeztetése) szintén ez a jogalap alkalmazandó.

9.3. Jogi kötelezettség jogalap alkalmazása

Tipikus jogszabályi kötelezettségek teljesítése esetén a Társaság a GDPR 6. cikk (1) bekezdés c) pontja alapján kezeli az érintetti személyes adatokat. Ilyen jogi kötelezettséget írnak elő a Társaság számára – különösen – az Sztv., az Art., az Mt. rendelkezései. A jogi kötelezettségre hivatkozva csak azokat a személyes adat kategóriákat szabad tárolni, amelyeket az adott jogszabály előír, azokat viszont kötelező.

Az Infotv. 5. § (5) bekezdése értelmében, ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg, az adatkezelő az adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e. Ezen felülvizsgálat körülményeit és eredményét a Társaság, mint adatkezelő dokumentálja, e dokumentációt a felülvizsgálat elvégzését követő tíz évig megőrzi és azt a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: „NAIH", „Hatóság") kérésére a Hatóság rendelkezésére bocsátja.

9.4. Létfontosságú érdek jogalap alkalmazása

GDPR 6. cikk (1) bekezdés d) pontja szerinti jogalapra tekintettel kezelhető az érintett személyes adata, ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges. A Társaság főszabály szerint nem alapítja az adatkezelését a létfontosságú érdekre, mint jogalapra.

9.5. Jogos érdek jogalap alkalmazása

A GDPR 6. cikk (1) bekezdés f) pontjában foglaltakra tekintettel jogosult a Társaság a jogos érdekei alapján kezelni a személyes adatokat, ha az adatkezelés a Társaság vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges. Kivételt képez ez alól, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Az adatkezelés jogszerűségének vizsgálatához a Társaság **érdekmérlegelési tesztet** készít, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

Az **érdekmérlegelési teszt során** a Társaság azonosítja jogos érdekét az adatkezeléshez, valamint a súlyozás ellenpontját képező érintetti érdeket és az érintett alapjogot. A Társaság a mérlegelés során figyelembe veszi – különösen – a kezelt, illetve kezelendő adat természetét és szenzitív jellegét, nyilvánosságának mértékét, az esetlegesen bekövetkező szabálysértés súlyosságát, stb.

Az érdekmérlegelési teszt részeként **szükségességi-arányossági teszt**et folytat le a Társaság, amelynek értelmében a személyes adatok védelme alóli kivételeknek és a védelem korlátozásainak a feltétlenül szükséges mérték határain belül kell maradniuk. A kezelhető adatok jellege és mennyisége nem haladhatja meg a jogszerű érdekek érvényesítése céljából szükséges mértéket. Az arányosság vizsgálata a célok és a megválasztott eszközök közötti kapcsolat értékelését foglalja magában. A választott eszközök a szükségesség mértékét nem haladhatják meg, azonban az eszközöknek is alkalmasnak kell lenniük a meghatározott cél elérésére.

A súlyozás elvégzése alapján a Társaság megállapítja, hogy kezelhető-e a személyes adat.

A teszt eredményéről az érintettek tájékoztatást kapnak, melyből egyértelműen kiderül, hogy mely jogos érdek alapján és miért tekinthető arányos korlátozásnak az, ha a Társaság e jogalapra hivatkozva kezeli a személyes adatot, tehát a Társaság adatkezeléséhez fűződő jogos érdeke miért múlja felül az érintett érdekeit, illetve jogait.

10. Adatvédelmi hatásvizsgálat

A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó esetekben – figyelembe véve a Hatóság honlapján közzétett GDPR 35. cikk (4) bekezdés szerinti kötelező hatásvizsgálati eseteket – a Társaságok kötelesek – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérjék a magas kockázat különös valószínűségét és súlyosságát – **az adatkezelés megkezdése előtt** adatvédelmi hatásvizsgálatot végezni. Ez a hatásvizsgálat magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, valamint a GDPR-nak való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.

10.1. Hatásvizsgálatot megelőző kockázatértékelés

A Társaság az adatvédelmi hatásvizsgálat lefolytatása előtt, minden alkalommal előzetes kockázatértékelést végez, amely alapján a Társaság eldönti, hogy az adatkezelés valószínűsíthetően magas kockázattal jár-e az érintettek jogaira nézve és emiatt szükséges-e adatvédelmi hatásvizsgálat. Az előzetes kockázatértékelés során a Társaság az ***ASZ-05-01 Hatásvizsgálatot megelőző kockázatértékelés*** c. táblázatában foglaltakat is alkalmazza annak eldöntése érdekében, hogy szükséges-e adatvédelmi hatásvizsgálat lefolytatása.

Fontos, hogy adatkezelés esetén a kockázat mértéke sosem lehet nulla, ugyanakkor egyes adatkezelések tekintetében különbséget kell tenni aközött, hogy az adatkezelés alacsony kockázatot hordoz-e vagy éppen magas kockázatot az érintett jogaira és szabadságaira nézve. A Társaság minden esetben beazonosítja az új adatkezelését és annak legfontosabb jellemzőit, majd a táblázatban rögzített kérdések segítségével igyekszik felmérni az esetleges kockázatok mértékét.

Amennyiben az adatkezelés, illetve az ahhoz kapcsolódó tevékenység nevesítésre kerül a NAIH által kiadott és hatályos, kötelező adatvédelmi hatásvizsgálatokat tartalmazó jegyzékben, úgy mindenképp szükséges az adatvédelmi hatásvizsgálat lefolytatása.

Amennyiben a táblázatban rögzített kérdések alapján nem egyértelműen eldönthető, hogy szükséges-e adatvédelmi hatásvizsgálat lefolytatása, úgy az adatvédelmi hatásvizsgálat lefolytatását el kell végezni.

Az előzetes kockázatértékeléseket minden esetben felül kell vizsgálni, amennyiben az adatkezelés, illetve a jogszabályi és/vagy a belső szabályozási környezet változik.

Az előzetes kockázatértékelés elvégzésért az Adatvédelmi manager felel.

10.2. Az adatvédelmi hatásvizsgálat lefolytatása

Amennyiben valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel - valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelés megkezdését megelőzően az Adatkezelő hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti. Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egyetlen egy hatásvizsgálat keretében is elvégezhetők.

10.3. A hatásvizsgálat elemei

a) az adatkezelés leírása

A hatásvizsgálat lefolytatása során részletesen be kell mutatni a vizsgált adatkezelést, kitérve az adatkezelés környezetének vizsgálatára is. Be kell mutatni ezek alapján az alábbiakat:

- személyes adatok körét,
- adatkezelés célját,
- adatkezelés jogalapján
- adatfelvétel módját,
- kik férhetnek hozzá a személyes adatokhoz,
- megőrzési határidőket,
- az adatkezelést támogató informatikai rendszereket,
- el kell készíteni az adatkezelés funkcionális leírását.

b) jogszabályi megfelelőség

A hatásvizsgálat kiterjed arra is, miként felel meg az adatkezelés a GDPR előírásainak, illetve az adatkezelő hogyan biztosítja az érintetti jogok gyakorlásának feltételeit.

c) szükségesség-arányosság vizsgálata

A Társaság elvégzi az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatát. A szükségességi és arányossági vizsgálat során tételesen ellenőrizni szükséges az alábbi intézkedéseket:

-meghatározott, kifejezett és jogos cél(ok) (célhoz kötöttség),
-az adatkezelés jogszerűsége,
-a kezelt adatok megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak (adattakarékosság),
-korlátozott tárolási időtartam.

d) kockázatok meghatározása, elemzése

A hatásvizsgálatban az Adatkezelő elemzi a természetes személyek jogaira és szabadságaira nézve magas kockázatokat, így első lépésként szükséges egy kockázati lista felállítása.

Ennek megfelelően vizsgálja:

- a kockázatok forrását, természetét
- sajátosságait,
- súlyosságát (alacsony- közepes-magas kockázat),
- miként fordulhatnak elő az egyes kockázatok kapcsán a nem kívánt hatások (például adatokhoz való jogosulatlan hozzáférés, adatok véletlen vagy jogellenes megváltoztatása, adatvesztés), mekkora a valószínűsége ennek bekövetkeztének és ez milyen következményekkel jár az érintett magánszférájára nézve.

e) garanciák és intézkedések meghatározása

A hatásvizsgálatban szükséges kitérni továbbá arra, hogy az Adatkezelő milyen intézkedéseket tesz a kockázatok csökkentése, illetve azok megszüntetése érdekében. Részletezni kell továbbá, hogy az intézkedés milyen mértékben csökkenti a kockázatot, ki(k) felelős(ek) az intézkedés végrehajtásáért és az intézkedés mennyire általános megoldása a kockázat csökkentésének, ki(k) felelős(ek) az intézkedések megtételéhez és végrehajtásához szükséges feltételek (tárgyi, technikai, személyi, anyagi) biztosításáért, mennyi időn belül szükséges az adott intézkedés végrehajtása.

A hatásvizsgálat elvégzését követően szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén gondoskodni szükséges a hatásvizsgálat felülvizsgálatáról, mely során a kockázatok értékelését újra el kell végezni.

A hatásvizsgálatot az Adatvédelmi manager folytatja le, akár külső szolgáltató közreműködésével. Fontos, hogy a kockázatok felülvizsgálatát legalább 2 évente el kell végezni, különösen, ha:

a) az adatkezelési folyamat megváltozik;
b) az adatkezelési folyamatban résztvevők személye megváltozik;
c) a szabályozási környezet megváltozik;
d) amennyiben az Adatvédelmi manager, az adatkezelési folyamatgazdák és az információbiztonsági felelős közül bármelyikük is valószínűsíti, hogy az adatkezelési folyamatot érintő változás jelentős befolyással lehet a természetes személyek jogait és szabadságait érintő kockázatokra.

10.4. Előzetes konzultáció

Amennyiben az Adatkezelő által elvégzett hatásvizsgálat lefolytatásának eredményeképp megállapítható, hogy az adatkezelési folyamat valószínűsíthetően magas kockázattal jár, úgy az Adatkezelő az adatkezelési folyamat megkezdését megelőzően köteles konzultációt kezdeményezni a Hatósággal.

A konzultáció kezdeményezése során az Adatkezelő csatolja:

- az elvégzett hatásvizsgálatot,
- az Adatkezelő vezérigazgatójának és Adatvédelmi managernek az elérhetőségét,
- az adatkezelési folyamatban résztvevő adatkezelő(k), adatfeldolgozó(k) feladatköreinek felsorolását,
- az adatkezelés célját, módját és az érintettek jogai, szabadságai biztosításának védelmében hozott intézkedéseket, garanciákat.

11. Adatkezeléssel kapcsolatos nyilvántartások vezetése

A Társaság a jogszerűség, elszámoltathatóság, átláthatóság elvének megfelelően számos a Társaság adatkezelésével kapcsolatos nyilvántartás vezetésére kötelezett. Ezen belső nyilvántartások vezetése történhet papír alapon, illetve elektronikus úton is. A nyilvántartások vezetésének célja, hogy elősegítse a Társaság jogszerű adatkezelését, illetve elősegítse az érintetti jogok gyakorlását.

11.1. Adatkezelési Nyilvántartás

A Társaság, mint adatkezelő a GDPR 30. cikk (1) bekezdése alapján köteles minden az általa végzett adatkezelési tevékenységet nyilvántartásba venni, és a nyilvántartást vezetni (a továbbiakban: „**Adatkezelési Nyilvántartás**"). Az adatkezelési tevékenység azon adatkezelési műveletek, tevékenységek összességét jelenti, amelyek egy meghatározott adatkezelési cél megvalósításához szükségesek.

Az Adatkezelési Nyilvántartásnak az egyes adatkezelési tevékenységek tekintetében legalább az alábbi adatokat szükséges tartalmaznia:

- adatkezelő neve,
- adatkezelő székhelye,
- adatkezelő képviselőjének neve és elérhetősége és címe,
- adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége (amennyiben van ilyen),
- adatkezelő adatvédelmi managerének neve és elérhetősége,
- sorszám,
- adatkezelés megnevezése,
- adatkezelés célja,
- adatkezelés jogalapja (GDPR hivatkozással és jogszabályi kötelezettség teljesítése esetén a konkrét jogszabályhely megjelölésével),
- érintettek kategóriái,
- személyes adatok kategóriái,
- személyes adatok különleges kategóriái,
- adatok forrása,
- címzettek kategóriái,
- adatfeldolgozó neve és képviselője,
- harmadik országba, nemzetközi szervezet részére történő adattovábbítás,
- adattovábbítás garanciái,
- tárolás időtartama, törlési határidők,

- adatbiztonsági intézkedés általános ismertetése (alkalmazott technikai, szervezési intézkedések),
- adatkezelési folyamatgazda,
- érintett szervezeti egység, terület,
- elfogadás-tudomásul vétel bizonyítása,
- jogos érdek esetén érdekmérlegelési teszt elkészítésére sor került-e,
- megjegyzés.

Egy adott adatkezelési tevékenységet az életciklusa alatt több jogalapra is lehet alapítani, ezek mindegyikét fel kell tüntetni az Adatkezelési Nyilvántartásban.

Az Adatkezelési Nyilvántartás tartalmát az átláthatóság és elszámoltathatóság elvének szem előtt tartásával **folyamatosan felül kell vizsgálni** és **naprakészen** kell tartani, így különösen:

- rögzíteni kell az új adatkezelési tevékenységeket, különösen új adatkezelési cél vagy új érintetti kör esetén;
- a már meglévő adatkezelési tevékenység módosulása esetén rögzíteni kell különösen, ha megváltozott az adatkezelés jogalapja, célja az igénybe vett adatfeldolgozó, a címzettek köre, a személyes adatok köre;
- törölni kell a már nem végzett adatkezelési tevékenységeket.

Az Adatkezelési Nyilvántartást a Társaság Adatvédelmi managere köteles vezetni.

A Társaság az Adatkezelési Nyilvántartás alapján figyelemmel kíséri az egyes adatkezelési tevékenységek tekintetében az adatmegőrzésre irányuló jogszerű vagy jogszerűen megállapított időtartamot, melynek elteltét követően törölni köteles a személyes adatot. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon az adatkezelési tevékenységért felelős személy köteles rendszeresen, dokumentált módon felülvizsgálni az általa kezelt személyes adatokat.

A Társaság az adatkezelési nyilvántartását külön elektronikus dokumentumban vezeti és tárolja.

11.2. Adattovábbítási nyilvántartás

A Társaság az adattovábbítás jogszerűségének ellenőrzése, valamint az érintettek tájékoztatásának elősegítése érdekében a GDPR 5. cikkében foglalt alapelvek megvalósítása érdekében adattovábbítási nyilvántartást (a továbbiakban: „**Adattovábbítási nyilvántartás**”) vezet.

Az Adattovábbítási nyilvántartás legalább az alábbi adatokat tartalmazza:

- adatkezelő neve,
- adatkezelő székhelye,
- adatkezelő képviselőjének neve és elérhetősége,
- adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége (amennyiben van ilyen),
- adatkezelő adatvédelmi managerének neve és elérhetősége,
- sorszám,
- adattovábbítás dátuma,
- címzett,
- adattovábbítás jogalapja,
- személyes adatok köre,

- jogszabályban meghatározott adatok,
- adattovábbítás módja (átadás formája),
- elvárt biztonsági intézkedés,
- megjegyzés (státusz).

A Társaság az Adattovábbítási nyilvántartását külön elektronikus dokumentumban vezeti és tárolja, azt az Adatvédelmi manager vezeti.

11.3. Megkeresésekkel kapcsolatos nyilvántartás

A Társaság a GDPR 5. cikkében nevesített átláthatóság és elszámoltathatóság elvének érvényre juttatása érdekében nyilvántartás vezet az érintetti jogok gyakorlásával kapcsolatos megkeresésekről, annak tartamáról, valamint annak teljesítéséről. A Megkeresésekkel kapcsolatos nyilvántartást a Társaság Adatvédelmi managere köteles vezetni. A nyilvántartás tartalmazza az alábbiakat:

- adatkezelő neve,
- adatkezelő székhelye,
- adatkezelő képviselőjének neve és elérhetősége,
- adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége (amennyiben van ilyen),
- adatkezelő adatvédelmi managerének neve és elérhetősége,
- megkeresés azonosítója (év-sorszám),
- megkeresés ideje,
- érintett neve,
- megkeresés tárgya,
- megkeresés tartalma,
- érintett adatkezelések,
- megkereséssel összefüggésben tett intézkedések,
- végrehajtásért felelős,
- megkeresésre adott válasz kiküldésének dátuma,
- megjegyzés.

A Társaság a Megkeresésekkel kapcsolatos nyilvántartását külön elektronikus dokumentumban vezeti és tárolja.

11.4. Adatvédelmi incidens nyilvántartása

Az Adatvédelmi incidensek nyilvántartására vonatkozóan a 17.3. pont tartalmaz rendelkezéseket.

11.5. Adatmegszüntetési nyilvántartás

A Társaság a GDPR 5. cikkében nevesített átláthatóság és elszámoltathatóság elvének érvényre juttatása érdekében nyilvántartást vezet azon személyekről, akik a törlési jogukkal élve kezdeményezték, hogy a Társaság törölje az általa kezelt, az érintettre vonatkozó adatokat.

Az adatkezelési és adatmegszüntetési nyilvántartást a Társaság Adatvédelmi managere köteles vezetni.

A nyilvántartás legalább az alábbiakat tartalmazza:

- adatkezelő neve,
- adatkezelő székhelye,
- adatkezelő képviselőjének neve és elérhetősége,
- adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége (amennyiben van ilyen),
- adatkezelő adatvédelmi managerének neve és elérhetősége,
- sorszám,
- kérelem időpontja,
- érintett neve és esetleges azonosítója,
- kérelme tartalma,
- intézkedés megnevezése,
- megjegyzés.

A Társaság az Adatkezelési és adatmegszüntetési nyilvántartását külön elektronikus dokumentumban vezeti és tárolja.

11.6. Adatfeldolgozói nyilvántartás

A Társaság köteles nyilvántartást vezetni arról a tevékenységéről is, melyet valamely adatkezelő nevében adatfeldolgozói minőségben végez. Az adatfeldolgozói nyilvántartásra vonatkozó rendelkezéseket jelen Szabályzat 13. pontja tartalmazza.

12. A Társaság, mint adatkezelő az adatfeldolgozás során

A GDPR 4. cikke alapján, amennyiben az adatkezelésre vonatkozó körülményeket a Társaság határozza meg, így különösen az adatkezelés eszközeit, kezelésének céljait önállóan határozza meg, úgy a Társaság minősül az adott adatkezelés szempontjából adatkezelőnek, ezáltal felelős az adatkezelésre vonatkozó, a GDPR-ban és más hazai ágazati jogszabályokban foglaltak betartásáért.

A Társaság – a fentiekre is tekintettel köteles – olyan adatfeldolgozókat igénybe venni, akik, vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR-ban foglalt követelményeinek való megfelelésre és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

A Társaság, mint adatkezelő – illetve amennyiben adatfeldolgozói minőségében további adatfeldolgozókat vesz igénybe – olyan adatfeldolgozókat vesz igénybe, amelyek megfelelnek a GDPR 32. cikkében foglalt előírásoknak. Az Társaság minden adatfeldolgozójával adatfeldolgozói szerződést köt, amely legalább az alábbi kérdéseket tisztázza:

- az adatkezelés, amelybe az Adatkezelő az adatfeldolgozót bevonta;
- az adatfeldolgozó által ellátott Adatkezelői tevékenység;
- az adatfeldolgozás időtartamát, jellegét és célját;
- az adatfeldolgozásra átadott adatok típusa;
- az adatfeldolgozással érintett érintettek kategóriái;
- az Adatkezelő jogai és kötelezettségei;
- az adatfeldolgozó jogai és kötelezettségei.

Az Adatkezelő csak olyan adatfeldolgozóval köt szerződést adatfeldolgozói feladatra, amely szerződésben vállalja, hogy:

- a személyes adatokat kizárólag az Adatkezelő írásbeli utasításai alapján kezeli;
- az általa személyes adatok feldolgozásában résztvevő személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- biztosítja a GDPR 32. cikk szerinti adatbiztonsági szabályokat;
- Adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vesz igénybe;
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az Adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintettek jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;
- adatvédelmi incidens esetén az incidens tudomására jutása pillanatában azonnal értesíti az Adatkezelőt és együttműködik az adatvédelmi incidens kezelésében;
- az adatfeldolgozási szolgáltatás nyújtásának befejezését követően az Adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az Adatkezelőnek, valamint a személyes adatokról készült másolatokat ezzel egyidőben megsemmisíti vagy törli;
- lehetővé teszi és elősegíti, hogy az Adatkezelő ellenőrizhesse az adatvédelmi szabályok megvalósulását;
- vezeti a GDPR 30. cikk (2) bekezdése szerinti adatfeldolgozói nyilvántartást.

A Társaság és az adatfeldolgozó között létrejövő szerződésnek részét kell, hogy képezze azon rendelkezés, hogy az adatvédelmi és adatbiztonsági jogszabályi előírásokat és jelen Szabályzatban foglalt rendelkezéseit tudomásul veszi, azokat a tevékenysége során betartja, illetve azt is, hogy ennek ellenőrzésére a Társaság jogosult.

A Társaság annak érdekében, hogy az adatfeldolgozóival a GDPR rendelkezéseinek megfelelő adatfeldolgozói szerződéseket köthesse, megalkotta az adatfeldolgozói szerződés-mintáját, amelynek elnevezése a következő: ASZ-31_Adatfeldolgozói_mintaszerzodes_Semilab_adatfeldolgozo_final.

A Társaság kiemelt figyelmet fordít arra, hogy az érintettek személyes adatait az arra jogosult kör ismerhesse meg, valamint ezen személyek a szükséges titoktartási kötelezettségvállalást megtegyék az adatokhoz történő hozzáférést megelőzően.

Az adatfeldolgozói szerződés alkalmazásáért az adott szervezeti egység vezetői felelősek. Amennyiben az alkalmazással összefüggésben kérdésük merül fel, a Társaság Adatvédelmi manageréhez fordulhatnak annak érdekében, hogy a GDPR rendelkezéseinek megfelelően járjanak el az adatkezelések során.

Amennyiben a Hatóság általános szerződési feltételeket határoz meg az adatfeldolgozói szerződésre vonatkozóan, a mintát annak megfelelően módosítani szükséges.

13. A Társaság, mint adatfeldolgozó az adatfeldolgozás során

Amennyiben a Társaság tevékenységének ellátása során más jogi személy, társaság helyett, annak megbízása alapján végez bármilyen adatkezelési műveletet, úgy a Társaság a megbízott művelet(ek) tekintetében a GDPR 4. cikk 8. pontja szerinti adatfeldolgozónak minősül, illetve az Infotv. 3.§ 17. pontja szerinti adatfeldolgozást végez.

Az adatfeldolgozás tényére tekintettel a Társaság gondoskodik az adatfeldolgozói szerződések, valamint a titoktartási nyilatkozatok megkötéséről.

A Társaságot megbízó adatkezelő (a továbbiakban: „**Megbízó**") jogosult és köteles írásbeli utasítást adni a Társaságnak az adatfeldolgozással kapcsolatban. Az utasítás jogszerűségéért a Megbízó felel, a Társaság köteles azonban felhívni a Megbízó figyelmét, ha az utasítás jogszerűtlen, szakszerűtlen.

A Társaság kizárólag a Megbízó írásbeli utasításai alapján láthatja el adatfeldolgozói tevékenységét, az adatkezelést érintő érdemi döntést nem hozhat, az adatkezelés céljának meghatározására vagy az adatok eltérő célból történő felhasználására a Társaság nem jogosult.

Amennyiben a Társaság túlterjeszkedik az adatfeldolgozói szerződésben meghatározott jogain, az adott túlterjeszkedéssel érintett adatok tekintetében önálló adatkezelővé válik, és a Megbízónak, az érintettnek vagy harmadik személynek okozott kárért a károkozás általános szabályai szerint köteles helytállni.

A Társaság az érintett személyek felé adatkezelési kérdésekben önállóan, a saját nevében nem járhat el, nyilatkozatot nem tehet, a Megbízó jogosítványait nem gyakorolhatja.

A Társaság felelőssége az adatfeldolgozási tevékenységéért úgy alakul, hogy amennyiben tevékenységének ellátása során a Megbízóval kötött adatfeldolgozói szerződés előírásainak betartásával jár el, úgy a Társaság adatfeldolgozói tevékenységéért a Megbízó úgy felel, mintha maga járt volna el.

A Társaság továbbá tevékenységi körén belül felelős az adatfeldolgozói szerződés teljesítésével összefüggésben birtokába került személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért, nyilvánosságra hozataláért vagy bármely egyéb, a személyes adatokon jogosulatlanul végzett műveletért. Felelős továbbá az adatfeldolgozói tevékenység keretében végzett valamennyi művelet szakszerű, szakértőtől elvárható végrehajtásáért.

A Társaság felelős mindazon kárért, amely az adatfeldolgozási tevékenységével összefüggésben vagy annak eredményeként az ellenőrzési körében – így különösen alkalmazottai, esetlegesen igénybe vett további adatfeldolgozói magatartása folytán, az általa működtetett informatikai rendszer kialakításának, működtetésének zavara következtében – felmerülő körülmény folytán következett be és annak bekövetkezési lehetősége a számára, mint szakértő számára előre látható volt, és mint szakértőtől elvárható volt, hogy a körülményt elkerülje, vagy a kárt elhárítsa.

A Társaság köteles továbbá írásbeli (ideértve az elektronikus formátumot is) nyilvántartást vezetni a Megbízó nevében végzett adatkezelési tevékenységekről. A GDPR. 30. cikk (2) bekezdésének értelmében a nyilvántartás legalább a következő információkat tartalmazza:

- adatfeldolgozó neve és elérhetősége,
- adatfeldolgozó képviselőjének neve és elérhetősége,
- adatfeldolgozó adatvédelmi tisztviselőjének neve és elérhetősége (amennyiben van ilyen),
- adatfeldolgozó adatvédelmi managerének neve és elérhetősége,
- adatkezelő neve és elérhetősége,
- sorszám,
- adatkezelő képviselőjének neve és elérhetősége, amennyiben van ilyen,
- adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége, amennyiben van ilyen,
- adatkezelési tevékenység minden kategóriájának rögzítése érdekében:
    - adatkezelés megnevezése,
    - adatkezelés célja,
    - adatkezelés jogalapja,
    - érintettek kategóriái,
    - a személyes adatok kategóriái,
    - adattörlésre előirányzott határidő,
    - címzettek kategóriái,
- harmadik országba, nemzetközi szervezet részére adattovábbítás történik-e, ha igen, hova,
- alkalmazott technikai, szervezési intézkedések.

A Társaság az Adatfeldolgozói nyilvántartását külön elektronikus dokumentumban vezeti és tárolja.

Az Adatfeldolgozói nyilvántartást a Társaság Adatvédelmi managere köteles vezetni. Az adatfeldolgozó igénybevételéhez nem kell az érintett(ek) előzetes beleegyezése, de szükséges a tájékoztatásuk.

Amennyiben a fentiektől eltérően az eset összes körülményét figyelembe véve nem adatfeldolgozásnak, hanem közös adatkezelésnek minősül az érintett jogviszony, akkor a Társaság és a további adatkezelők a közöttük létrejött megállapodásban kötelesek meghatározni a GDPR-ban foglalt kötelezettségek teljesítéséért fennálló felelősségük megoszlását, különösen az érintettek jogainak gyakorlásával és tájékoztatásával kapcsolatban. A megállapodásban meg kell jelölni, hogy melyikük tartja az kapcsolatot az érintettel. A megállapodás lényegéről az érintetteket tájékoztatni kell. Biztosítani kell az érintett jogait abban az esetben is, ha azokat a megállapodás feltételeitől függetlenül kívánja gyakorolni.

14. Közös adatkezelés

Ha az adatkezelés összes körülményét figyelembe véve az adatkezelés céljait és eszközeit több adatkezelő közösen határozza meg, azok közös adatkezelőknek minősülnek. Közös adatkezelés esetén az adatkezelők átlátható módon kötelesek meghatározni a GDPR szerinti kötelezettségeik teljesítéséért fennálló felelősségük megoszlását, a közöttük fennálló viszonyt, a kötelezettségeik teljesítésének módját (pl. érintettek tájékoztatáshoz való joga). A megállapodásban az érintettek számára kapcsolattartót kell kijelölni, a megállapodás „lényegét" pedig az érintettek tudomására kell hozni. Biztosítani kell az érintett jogait abban az esetben is, ha azokat a megállapodás feltételeitől függetlenül kívánja gyakorolni.

15. Személyes adatok átadása cégcsoporton belül

A Társaság az alábbi társaságokkal együttesen összevont (konszolidált) éves beszámolót készít és egy cégcsoportot alkot:

- **Flexpert Műszaki Tanácsadó Kft.** (székhely: 1117 Budapest, Prielle Kornélia utca 4/A., cégjegyzékszám: 01-09-682927);
- **MultiFlex Ingatlanhasznosító Kft.** (székhely: 1117 Budapest, Prielle Kornélia utca 4/A., cégjegyzékszám: 01-09-727633);
- **Space Solutions Ingatlanhasznosító Kft.** (székhely: 1117 Budapest, Prielle Kornélia utca 4/B., cégjegyzékszám: 01-09-339821)
- **Semilab Germany Gmbh** (székhely: Geysostraße 13, 38106 Braunschweig, Germany, nyilvántartási szám: HRB205581);
- **Semilab Denmark ApS** (székhely: Marielundvej 46D, st., 2730 Herlev, Dánia, nyilvántartási szám: 37138177);
- **Semilab USA LLC** (székhely: 12415 Telecom Dr, Tampa, Florida, 33637, Egyesült Államok, nyilvántartási szám: 27-0347663);
- **Semilab Japan KK** (székhely: YS Shin Yokohama Bldg. 6F 2-15-10, Shin Yokohama, Kohoku-ku, 222-0033 Yokohama, Japan, nyilvántartási szám: 0123-01-001915);
- **Semilab Korea Co., Ltd.** (székhely: 4F-412, 830, Dongtansunhwan-daero Dongtan SK V1 center, Hwaseong, Gyeonggi, 18468, nyilvántartási szám: 135811- 0173236);
- **Semilab Taiwan** (székhely: 5F-5, No. 32, Kaote II Rd., Zhubei City, Hsinchu County, Taiwan, adószám: 54524601);
- **Semilab (S.E.A) Pte Ltd.** (székhely: 7030 Ang Mo Kio Avenue 5, #08-08, Northstar @ Amk, Singapore 569880, nyilvántartási szám: 200813868N);
- **Semilab Trade (Shanghai) Co., Ltd.** (székhely: Room 234, 2F, Building 2, No. 15, Yingnan Road, China (Shanghai) Pilot Free Trade Zone, adószám: 310115400251708);
- **Semilab Wuxi Technology Co. Ltd.** (székhely: 19-5, Xing Chuang Four Road, XinWu District, Wuxi (214028), P.R China, nyilvántartási szám: 91320214MA1WF3PC5D).

A cégcsoporton belül az egyes társaságok az összevont (konszolidált) éves beszámoló készítéséhez kapcsolódóan, valamint működésük és szervezetük összehangolása érdekében a GDPR 6. cikk (1) bekezdés f) pont szerinti jogos érdekükből továbbíthatnak adatokat a cégcsoport további tagjai számára, azzal, hogy minden esetben érdekmérlegelési tesztet készítenek és az egyes esetekben az adott társaság a másik társaság részére adatfeldolgozást fog végezni, melyhez kapcsolódóan a szükséges adatfeldolgozói szerződést minden esetben megkötik a felek. Ily módon ezen társaságok bizonyos szervezeti egységei kapcsolódhatnak egymáshoz, közöttük adatáramlás mehet végbe az összevont (konszolidált) éves beszámolósó elkészítéséhez kapcsolódóan. A Társaság cégcsoporton belüli személyes adatok átadásával kapcsolatos részletesebb szabályozása külön dokumentumban került lefektetésre.

16. Adatbiztonsági szabályok

A Társaság az adatkezelés során mindvégig gondoskodik a kezelt személyes adatok ésszerűen elvárható legmagasabb szintű biztonságáról. A Társaság az adatkezelési műveleteit oly módon végzi, hogy megfelelő technikai és szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (integritás és bizalmi jelleg). A Társaság továbbá a személyes adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás,

továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

A Társaság a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

Gondoskodik az adatok biztonságáról, megteszi továbbá azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek a GDPR, valamint az egyéb személyes adatvédelmi szabályok érvényre juttatásához szükségesek.

A Társaság az adatkezelés időtartama alatt az adatok biztonságos tárolása, az időtartam lejártával az adatállomány végleges és visszaállíthatatlan törlése, fizikai megsemmisítése érdekében megteszi a szükséges intézkedéseket.

A Társaság így az alábbi intézkedéseket teszi az adatok biztonságának biztosítása érdekében.

16.1. Papíralapon kezelt személyes adatok tekintetében

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

- Az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá. A Társaság nyilvántartást vezet az adatokat megismerő személyekről.
- A személyes adatokat tartalmazó papír alapú dokumentumokat a Társaság jól zárható, száraz helyiségben, szekrényben tárolja, azokhoz csak meghatározott személyek férnek hozzá, csak ezen meghatározott személyek rendelkeznek hozzáférési joggal és kulccsal azokhoz.
- Amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza a Társaság.
- A papír alapú adathordozókat iratmegsemmisítő segítségével, vagy külső, iratmegsemmisítésre szakosodott vállalkozó igénybevételével kell a személyes adatoktól megfosztani.

16.2. Elektronikusan tárolt személyes adatok

Az informatikai eszközök biztonságára, az elektronikusan tárolt dokumentumokra, adatokra vonatkozó részletes előírásokat a Társaság Információbiztonsági Szabályzata tartalmazza.

17. Adatvédelmi incidensek kezelésének rendje

Az adatbiztonság sérülése, illetve a Társaság által kezelt személyes adatok véletlen vagy jogellenes megsemmisülése, elvesztése, módosulása, jogosulatlan továbbítása vagy nyilvánosságra hozatala, továbbá az azokhoz való jogosulatlan hozzáférés (a továbbiakban: **„Adatvédelmi incidens”**) bekövetkezését, vagy bekövetkezésének gyanúja fennállása esetén a Társaság, illetve a Társaság által kezelt személyes adatokat bármely jogviszony alapján megismerő személy köteles az e pontban foglaltak szerint eljárni.

Az Adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését, vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Az Adatvédelmi incidens eljárásrend érvényben tartásáért, fejlesztéséért és aktualizálásáért felelős az Adatvédelmi manager felel.

A Társaság ezért a tudomására jutott adatvédelmi incidenst az alábbi előírások szerint kezeli:

17.1. Az Adatvédelmi incidens észlelése és jelentése

Adatvédelmi incidensekkel és potenciális veszélyforrásokkal a Társaság valamennyi munkavállalója, szerződött partnere, ügyfele, illetve az informatikai rendszereit fejlesztő, működtető és üzemeltető munkavállalója szembesülhet, illetve észlelhet incidensre utaló jeleket.

Az incidensek korai felismerése érdekében a Társaság információbiztonsági rendszereket és eljárásokat működtet, melynek segítségével észlelésre kerülnek információbiztonsági és/vagy adatvédelmi események, amelyek adott esetben incidensnek minősülhetnek.

Általában az incidensek bekövetkezése előtt vagy bekövetkezése során különleges emberi viselkedés és/vagy az informatikai rendszer helytelen, szokatlan működése lép fel. Az esemény későbbi nyomonkövethetősége érdekében fontos, hogy szakmai kompetencia hiányában az incidenst észlelő ne avatkozzon be, saját hatáskörben ne kezdje meg az esemény kivizsgálását. (Kivételt képez ez alól a vagyoni kárelhárítás, illetve az emberi élet védelmében tett intézkedések.)

Incidens észlelésekor minden lényeges részletet azonnal fel kell jegyezni, a számítógép képernyőről másolatot kell készíteni (amennyiben releváns).

Az Adatkezelő annak érdekében, hogy az esetleges incidensek kivizsgálása hatékonyan megtörténhessen, az Adatvédelmi incidensre utaló körülmények, adatok bejelentéséhez kapcsolódó formanyomtatványt alkalmaz. Amennyiben a Társaság valamely munkavállalója olyan körülményt észlel, tapasztal, amely alapján elképzelhető, hogy adatvédelmi incidens történt vagy adatvédelmi incidens van folyamatban a Társaságnál, haladéktalanul, de legfeljebb 4 munkaórán belül köteles az Adatvédelmi incidensre utaló körülmények, adatok bejelentéséhez kapcsolódó formanyomtatványt kitölteni és szükséges a kitöltött dokumentumot megküldenie a Társaság Adatvédelmi managerének. Az Adatvédelmi incidensre utaló körülmények, adatok bejelentéséhez kapcsolódó formanyomtatvány jelen Szabályzat 2. sz. mellékletét képezi.

Bejelentés esetén szükséges arra is figyelemmel lennie mind a bejelentőnek, mind az Adatvédelmi managernek, hogy az incidens érinti-e a Társaság informatikai rendszerét, vagy szerződött partnereinek informatikai rendszerét, illetve fennáll-e az esélye az érintettek szélesebb körének személyes adatainak szivárgására, jogosulatlan személyek általi hozzáférésére. Amennyiben igen, szükséges a Társaság Információbiztonsági felelősének az értesítése is.

Amennyiben az adatvédelmi incidenst észlelő vagy jelentő személy nem írásban, hanem szóban tesz bejelentést az Adatvédelmi managernek, az Adatvédelmi manager köteles erről jegyzőkönyvet felvenni, amelynek tartalmaznia kell legalább az Adatvédelmi incidensre utaló körülmények, adatok bejelentéséhez kapcsolódó Formanyomtatványban foglalt információkat.

A Társaság az Adatvédelmi manager közreműködésével köteles haladéktalanul értesíteni a Társaság mindazon szerződött partnerét, akiknek adatfeldolgozást végez, amennyiben az incidens a szerződött fél információs rendszerét érinti, és az értesítés elmaradásával további sorozatos incidens bekövetkeztének esélye áll fenn.

Amennyiben az incidens a Társaság informatikai rendszerét is érinti, a Társaság vezetősége köteles értesíteni a rendszer üzemeltetésért felelős személyt, aki köteles az incidens kivizsgálásában segítséget nyújtani az Adatvédelmi managernek.

Adatvédelmi incidens esetén az Adatvédelmi manager jogosult minden iratba betekinteni, illetve minden helyiségbe belépni, amely az adatvédelmi incidens elhárításához szükséges.

17.2. Adatvédelmi incidens kivizsgálása, értékelése

A bejelentést követően az Adatvédelmi manager haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését – informatikai rendszert érintő incidens esetén az IT részleggel együttműködve –, továbbá megteszi mindazon szükséges elsődleges lépéseket, melyek alkalmasak arra, hogy az adatvédelmi incidens által okozott károk mértékét csökkentsék, vagy további adatvédelmi incidensek létrejöttét megakadályozzák.

Az Adatvédelmi manager információt gyűjt az incidensről. Az Adatvédelmi manager munkájába bevonhatja az adatvédelmi incidenssel érintett szervezeti egységek vezetőit és a szervezeti egységek munkavállalóit, akik kötelesek együttműködni az Adatvédelmi managerrel.

A kivizsgálás során az alábbi információkat (amennyiben azok a jelentésből nem derülnek ki) szükséges felderíteni a lehetőségekhez mérten:

- az adatvédelmi incidens bekövetkezésének időpontja és helye,
- az adatvédelmi incidens által érintett adatok köre,
- az adatvédelmi incidenssel érintett személyek köre és száma.

A bejelentő az adatszolgáltatást haladéktalanul, de legkésőbb 4 munkaórán belül teljesíti.

Ezen adatokból az Adatvédelmi manager összegzést készít az Adatvédelmi incidens várható hatásairól és összefoglalja a következményeinek enyhítése érdekében meghozandó intézkedéseket. A vizsgálatot legkésőbb az Adatvédelmi managerhez érkezéstől számított három munkanapon belül be kell fejezni.

Az Adatvédelmi manager vizsgálatának tartalmaznia kell, hogy az Adatvédelmi incidens magas kockázattal jár-e az érintettek jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e az érintettek tájékoztatása az incidensről. Amennyiben nem szükséges az érintettek tájékoztatása, a vizsgálatnak tartalmazni kell ennek indokait is.

Amennyiben az Adatvédelmi manager összegzéséből megállapítható, hogy Adatvédelmi incidens történt és valószínűsíthetően kockázattal járt az érintettekre nézve, összehívja az Adatvédelmi tanácsot, amely az Adatvédelmi managerből, a Társaság Információbiztonsági felelőséből, illetve a Társasággal állandó megbízási jogviszonyban álló ügyvédi iroda kijelölt képviselőjéből áll. Az Adatvédelmi tanács egyeztetésére sor kerülhet akár telefonon keresztül, akár személyesen a Társaság székhelyén, akár egyéb infokommunikációs eszközök igénybevétele által (például: Skype, stb.). Az Adatvédelmi tanács áttekinti az Adatvédelmi manager által elkészített összegzést, megvizsgálja az incidens körülményeit és újraértékeli annak kockázatait, majd egyhangú döntést hoz az incidens kezelése tekintetében, majd annak eredményét az Adatvédelmi manager írásban rögzíti.

Az Adatkezelő az Adatvédelmi incidenst különösen az alábbi szempontok szerint értékeli:

- az incidens típusa (bizalmassági, integritási vagy elérhetőségi);
- a személyes adatok jellege (személyes adat / különleges kategória);
- a személyes adatok száma;
- az érintett személyek száma;
- az érintett természetes személyek kategóriái;
- az érintett természetes személyek azonosíthatósága;
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- az érintett adatkezelés jogalapja.

Az elemzés során kiemelt figyelmet kell fordítani az incidenshez kapcsolódó bizonyítékok szakszerű gyűjtésére és megőrzésére.

Különösen az alábbi feltételek fennállása esetén minősíthető kockázatosnak az adatvédelmi incidens:

- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok;
- az incidensben érintett személyes adatok száma meghaladja az 50 darabot;
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek;
- az incidensben érintett természetes személyek száma meghaladja az 50 főt;
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre;
- a személyes adatok alkalmasak az érintett természetes személyazonosságának ellopására vagy a személyazonosságával való visszaélésre;
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi vagy reputációs veszteséget okozzanak az érintettjüknek.

Az adatvédelmi incidens akkor minősíthető valószínűsíthetően alacsony kockázatúnak, ha a fentiekben felsorolt feltételek közül legfeljebb egy áll fenn és az Adatkezelő képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezte óta nem sérült.

Az Adatkezelő akkor minősíti az adatvédelmi incidenst valószínűsíthetően magas kockázatúnak, ha fentiekben felsorolt feltételek közül legalább kettő fennáll, vagy legalább egy fennáll és az Adatkezelő nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezte óta nem sérült.

Amennyiben bebizonyosodik, hogy a bejelentés téves volt, a megtett biztonsági intézkedések (pl.: titkosítás) következtében az érintettek személyes adatai nincsenek veszélyben, az incidens vizsgálata a Adatvédelmi manager döntését követően lezárható. Az incidenst ebben az esetben is szükséges felvezetni a Társaság tárgyévre vonatkozó adatvédelmi incidens nyilvántartásába.

Amennyiben az adatvédelmi incidens (magas) kockázattal jár a természetes személyek jogaira nézve, úgy az erről szóló döntés meghozatala után az Adatvédelmi tanács tájékoztatja a Társaság vezérigazgatóját ezen tényről és intézkedik az érintettek megfelelő tájékoztatásáról a 17.6. pont alapján, valamint az incidens Hatóság részére történő megfelelő bejelentéséről a 17.5. pont szerint.

17.3. Az adatvédelmi incidens nyilvántartása

Az adatvédelmi incidensekre vonatkozó nyilvántartást az Adatkezelő Adatvédelmi managere vezeti külön dokumentumban, elektronikusan. A nyilvántartás tartalmazza:

- adatkezelő neve,
- adatkezelő székhelye,
- adatkezelő képviselőjének neve és elérhetősége,
- adatkezelő adatvédelmi tisztviselőjének neve és elérhetősége (amennyiben van ilyen),
- adatkezelő adatvédelmi managerének neve és elérhetősége,
- incidens azonosító (év-sorszám),
- incidens bejelentésének dátuma,
- incidens bejelentője,
- incidens bekövetkezésének dátuma,
- incidens jellege, az incidenshez kapcsolódó tények és körülmények,
- érintettek száma,
- érintettek köre,
- érintett személyes adatok kategóriái,
- érintett adatrekordok száma,
- érint-e különleges adatot az incidens,
- könnyen/nehezen azonosíthatók az érintett természetes személyek,
- érint-e gyermekeket vagy hátrányos helyzetű/sérült embereket,
- sérült-e a személyes adatok bizalmassága,
- sérült-e a személyes adatok integritása,
- sérült-e a személyes adatok rendelkezésre állása,
- szándékos károkozás történt-e,
- az adatvédelmi incidens hatása (valószínűsíthető következmények),
- incidens kockázati szintje (választható válasz: valószínűsíthetően nem jár kockázattal, valószínűsíthetően magas kockázattal jár, valószínűsíthetően kockázattal jár),
- adatvédelmi incidens orvoslása (intézkedések),
- hatósági bejelentés szükséges igen vagy nem,
- hatósági bejelentés dátuma, módja,
- érintettek tájékoztatása szükséges igen-nem,
- érintettek tájékoztatásának dátuma, módja,
- meghatározott javító intézkedések,

- a javító intézkedések végrehajtásáért felelős személy,
- a javító intézkedések végrehajtásának határideje,
- megjegyzések.

17.4. Helyesbítő-megelőző intézkedések

A károk enyhítését és az incidens lokalizálását követően az Adatvédelmi manager az incidenst kiváltó ok megtalálásával, meghatározásával foglalkozik. A cél, hogy meghatározásra kerüljenek azok a helyesbítő-megelőző intézkedések (legyen akár átmeneti, megkerülő megoldás) amelyek alkalmazásával az érintett természetes személyek jogaira és szabadságaira vonatkozó kockázat jelentősen csökkenthető, az incidens megismétlődésének valószínűsége csökken, és ezáltal biztosított legyen a Társaság által kezelt személyes adatok megfelelő védelme.

A helyesbítő-megelőző intézkedések – az incidenst lehetővé tévő gyengeség természetétől függően – lehetnek több fázisúak, azaz azonnal végrehajtandó intézkedések, illetve később megvalósítandó, nagyobb erőforrás igényű intézkedések.

A kidolgozott és jóváhagyott helyesbítő-megelőző intézkedéseket az Adatvédelmi managernek az Adatvédelmi incidensek nyilvántartásába be kell vezetnie.

A Társaság Vezérigazgatója felelős a helyesbítő intézkedések végrehajtásához szükséges erőforrások biztosításáért. A javasolt helyesbítő-megelőző intézkedések bevezetéséről a Vezérigazgató dönt.

A helyesbítő-megelőző intézkedések kidolgozásakor a meglévő intézkedéseket mind a szervezési, a technikai és az információbiztonsági területeken át kell tekinteni.

A helyesbítő intézkedések végrehajtását követően a módosított, illetve újként bevezetett szervezési, technikai és/vagy információbiztonsági intézkedések megfelelőségét ellenőrizni kell, a változásokat a releváns szabályzásokba át kell vezetni és az érintett munkatársakat tájékoztatni szükséges.

Az Adatvédelmi manager a hasonló incidensek áttekintésével eldönti, hogy szükségesek-e az alábbi intézkedések:

- utólagos elemzést lefolytatása, a mélyebb összefüggések megértése és az incidens jövőbeni előfordulásának megakadályozása céljából,
- továbbképzést/oktatást szervezése az incidensben érintett személynek,
- szabályzat, utasítás vagy információbiztonsági kontroll módosítása, fejlesztése az ismételt előfordulás kockázatának csökkentése érdekében,
- az incidens elhárítását követően az érintett rendszerkörnyezetben monitorozás, nyomon követés elrendelése.

Amennyiben ezek bármelyikére szükség van az Adatvédelmi manager felveszi a szükséges intézkedéseket az adatvédelmi incidensek nyilvántartásába, és gondoskodik azok jelen pont szerinti végrehajtásáról.

Az Adatvédelmi manager további feladata az incidens utólagos nyomon követése és az incidens lezárásáig be nem fejezett javító intézkedések megvalósításának nyomon követése.

17.5. Az adatvédelmi incidens bejelentése a Hatóság részére

Az Adatvédelmi manager az adatvédelmi incidenst a Társaság tudomására jutását követően haladéktalanul, de legkésőbb az incidens Társaság tudomására jutásától számított 72 órán belül bejelenti a Hatóság részére, kivéve, ha az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg határidőben, az Adatvédelmi manager köteles ennek okát igazolni a Hatóság részére.

A Hatósági bejelentésnek tartalmaznia kell:

- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

Az Adatvédelmi manager felelős a Hatósághoz történő bejelentésért a Társaság Adatvédelmi tanácsával történt egyeztetést követően, a Társaság vezérigazgatójának egyidejű tájékoztatása mellett.

A bejelentések kapcsán az **Adatvédelmi Manager:**

- nyilvántartást vezet a bejelentésekről,
- köteles meggyőződni a bejelentések hatósághoz történő megérkezéséről,
- további kommunikációt folytat az bejelentett incidensek hatósági megítéléséről és a teendőkről.

17.6. Az érintettek tájékoztatása adatvédelmi incidensről

Ha az Adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve és az érintettek tájékoztatása szükséges. Az Adatvédelmi manager haladéktalanul értesíti az érintetteket és erről a Társaság Vezérigazgatóját is értesíti. Az érintettek tájékoztatása független a Hatóság felé irányuló tájékoztatási kötelezettségtől.

Az érintettek részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következőket:

- a Társaság Adatvédelmi managerének nevét, elérhetőségét;
- az Adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- a Társaság által az Adatvédelmi incidens javítására tett vagy tervezett intézkedéseket, beleértve adott esetben az Adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az értesítés összeállítását az Adatvédelmi manager végzi és a Társaság Vezérigazgatója hagyja jóvá. Az érintettek felé megvalósult tájékoztatásról a Társaság Adatvédelmi managere nyilvántartást vezet.

Nem kell az érintetteket tájékoztatni:

- Ha a Társaság olyan technikai, szervezési, védelmi intézkedéseket hajtott végre az érintett adatokra vonatkozóan, amelyek megakadályozzák az illetéktelen személyek számára való hozzáférést az adatokhoz vagy megakadályozzák az adatok értelmezhetőségét.
- Ha az adatvédelmi incidens bekövetkezését követően a Társaság olyan intézkedéseket tett, amelyek biztosítják, hogy a feltárt adatkezelési kockázat valószínűsíthetően nem valósul meg.
- Ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé, ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, mely tájékoztatás elektronikus úton is megtörténhet.

Az incidenskezelésbe bevontak körén túl bármilyen kommunikáció csak a Társaság Vezérigazgatója jóváhagyásával lehetséges.

17.7. Rendszeres tréningek

Az Adatvédelmi manager jelen Szabályzat rendelkezéseinek betartása érdekében, gondoskodik az adatvédelmi tudatosság növelése céljából adatvédelmi incidensekkel kapcsolatos oktatásról, mely során a múltban bekövetkezett adatvédelmi incidensek tapasztalatait, vagy a lehetséges adatvédelmi incidensek veszélyeit ismerteti, elemzi, a kockázatok csökkentésével, megelőzésével kapcsolatosan tájékoztatást ad, illetve az ismereteket ellenőrzi.

18. Az érintettek jogainak érvényesítése

Az Adatkezelő fokozott figyelmet fordít arra, hogy a GDPR 12. - 23. cikkeiben meghatározott érintetti jogok érvényesítése megfeleljen a jogszabályi követelmények és az érintettek elvárásinak.

Az érintett tájékoztatást kérhet személyes adatai kezeléséről, valamint jogosult arra, hogy hozzáférjen a GDPR 15. cikkében meghatározott információkhoz, továbbá kérheti személyes adatainak helyesbítését, illetve – a jogszabályokban elrendelt adatkezelések kivételével – törlését vagy kezelésének korlátozását, illetve amennyiben a GDPR 21. cikkében foglalt feltételek teljesülnek, tiltakozhat a személyes adatok kezelése ellen, vagy élhet az adathordozhatóság jogával, illetve hozzájárulás visszavonásának jogával az Adatkezelő székhelyére megküldött levélben, vagy személyesen, továbbá jogosult az Adatkezelő Adatvédelmi manageréhez fordulni a gdpr@semilab.hu e-mail címén, a személyes adatainak kezelése vonatkozásában.

Az érintett tájékoztatást kérhet személyes adatai kezeléséről, jogosult arra, hogy hozzáférjen a GDPR 15. cikkében meghatározott információkhoz, valamint kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – törlését vagy kezelésének korlátozását, illetve tiltakozhat a személyes adatok kezelése ellen a Társaság feltüntetett elérhetőségein.

18.1. A kérelem teljesítésének határideje

Az Adatkezelő köteles az érintett személyes adatának kezelésével összefüggő kérelmére (bármely jog gyakorlása esetén) az érkezésétől számított legkésőbb egy hónapon belül írásban, közérthető formában választ adni. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

A határidő meghosszabbításáról az Adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Az új határidő a kérelem kézhezvételétől számított legfeljebb három hónapon belüli időpont lehet.

A kérelem beérkezését követő három napon belül a Társaság intézkedik arról, hogy az adatkezelés szempontjából illetékes szervezeti egység vezetőjének, valamint az Adatvédelmi managernek megküldésre kerüljön az érintetti kérelem. Az Adatvédelmi manager részére támogatást nyújt az érintetti kérelem tekintetében az illetékes szervezeti egység vezetője a kérelem GDPR-nak megfelelő megválaszolása érdekében.

Amennyiben a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet

- az intézkedés elmaradásának okairól, és
- arról, hogy az érintett panaszt nyújthat be a felügyeleti hatóságnál, valamint élhet bírósági jogorvoslati jogával.

18.2. A kérelem teljesítésének módja

Az Adatkezelő törekszik arra, hogy az érintettnek adott tájékoztatás minden esetben a GDPR által meghatározott szabályok teljesítése mellett is a lehetőségekhez mérten tömör, átlátható, érthető, könnyen hozzáférhető, világos és közérthető legyen.

Az érintetti jogok gyakorlására irányuló kérelem előterjesztése esetén a Társaság Adatvédelmi managere kezeli és teljesíti a kérelmeket, vagy intézkedik a kérelmek teljesítéséről.

Amennyiben az Adatvédelmi manager a kérelem kapcsán adatkezelési incidens gyanúját tárja fel, akkor a jelen Szabályzat 17. pontjának megfelelően kivizsgálja az esetet.

Az érintetti jogok teljesítésénél fontos szempont, hogy a kérelmet benyújtó érintett azonosítása megfelelő legyen. Az Érintettek azonosítását az Érintetti igényt felvevő kolléga végzi el. Kétség esetén késedelem nélkül bevonja az azonosításba az Adatvédelmi managert. Az érintett kérelme megfelelő azonosítószámot kap, amely feltüntetésre kerül a Megkeresésekkel kapcsolatos nyilvántartásban.

Amennyiben az érintett kérdés, kérés vagy panasz okán a Társasághoz fordul, ezeket a bejelentkezéseket és az ezek nyomán született intézkedéseket a Társaság nyilvántartja a Megkeresésekkel kapcsolatos nyilvántartásában.

A Társaság megfelelő módon közölt kérelemnek tekinti, ha az igényt az érintett:

- szóban személyesen személyazonosítást követően a Társaság székhelyén teszi meg, vagy
- írásba foglalt igény esetén azt az Adatkezelő hivatalos címére vagy a gdpr@semilab.hu e-mail címre úgy küldi meg, hogy a kérelme tekintetében ő mint érintett azonosítható legyen.

Az Adatkezelő az érintettnek adott minden tájékoztatást főszabály szerint írásban tesz meg. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri. Amennyiben az érintett kéri a szóbeli tájékoztatást, úgy személyazonossága igazolását követően az Adatkezelő erre felhatalmazott munkavállalója a tájékoztatást szóban is megadhatja.

A nem a fenti megfelelő módok valamelyikén közölt igényt az Adatkezelő nem veszi figyelembe.

18.3. A kérelem teljesítésének díja

Az Adatkezelő a jogok gyakorlásával kapcsolatban tett intézkedéseiről szóló tájékoztatást, illetve a jogok gyakorlásával kapcsolatos intézkedést (például a dokumentumok rendelkezésre bocsátását is) díjmentesen köteles biztosítani az érintett számára. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, az Adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre észszerű összegű díjat számíthat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.

Amennyiben az Érintett egy hónapon belül második alkalommal is kikéri ugyanazon adatokat, melyek ez idő alatt nem változtak, úgy az Adatkezelő az alábbiak szerint adminisztratív költséget számít fel:

- az adminisztratív költség elszámolás alapja a mindenkori minimálbér egy órára vetített mértéje, mint óradíj,
- a tájékoztatáshoz felhasznált munkaórák száma az előbbiekben meghatározott óradíjon alapulva,
- papír alapú tájékoztatási igény esetén a válasz nyomtatási költség önköltség áron és a postázás díja.

18.4. A kérelem elutasításának lehetőségei

A GDPR 12. cikk (4) bekezdésében, valamint a 32. cikkében foglalt (adatbiztonsági) szabályokra tekintettel, az érintettet megillető jogok gyakorlására - az adatkezelésre vonatkozó előzetes általános tájékozódáshoz való jog kivételével - csak a kérelmező megfelelő azonosítása, illetve kérelme tartalmának hitelesítését biztosító követelmények fennállása esetén van lehetőség.

Nem biztosítható a jogok gyakorlása a kérelmező személyének azonosítását korlátozottan lehetővé tevő módon benyújtott, így különösen:

- a más jogszabályban meghatározott teljes bizonyító erejű magánokiratra vonatkozó rendelkezéseknek nem megfelelő, vagy
- az elektronikus aláírással nem hitelesített, vagy
- elektronikus levél, telefonon, valamint telefax útján érkezett kérelmek esetén.

Amennyiben a személyazonosság igazolása nem történik meg, az Adatkezelő jogosult az érintett kérelmét elutasítani, és köteles tájékoztatni az érintettet jogai gyakorlásának módjáról.

Az Adatkezelő nem fogadja el a személyazonosítás telefonos úton történő egyetlen formáját sem, így az érintett telefonon nem kezdeményezheti jogainak érvényesítését.

18.5. Tájékoztatás és hozzáférés

A GDPR 13. cikkében foglalt kötelezettségnek megfelelően a Társaság köteles – amennyiben a személyes adat az érintettől származik a személyes adatok megszerzésének időpontjában – az adatkezelésre vonatkozó alábbi információkat érintettek rendelkezésére bocsátani:

a) az adatkezelőnek és képviselőjének a kiléte és elérhetőségei;
b) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
d) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
e) a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
f) az érintett azon jogáról szóló tájékoztatás, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
g) hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
h) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
i) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az érintett köteles-e a személyes adatokat megadni, továbbá, hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása.

Ha a személyes adatokat nem az érintettől szerezték meg, az Adatkezelő az érintett rendelkezésére bocsátja a fenti információkat, valamint azokon túlmenően a GDPR 14. cikkének értelmében az alábbi információkat:

a) az érintett személyes adatok kategóriái;
b) a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
c) a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

Ha a személyes adatokat nem az érintettől szerezték meg az Adatkezelő a tájékoztatást:

a) a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül;
b) ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy
c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor köteles megtenni.

Nem kell eleget tenni a fent írt tájékoztatási kötelezettségnek, amennyiben:

- az érintett már rendelkezik az e pontokba foglalt információkkal,
- a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne,
- az adat megszerzését vagy közlését kifejezetten előírja az Adatkezelőre alkalmazandó uniós vagy a hatályos magyar jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről is rendelkezik vagy
- a személyes adatoknak valamely uniós vagy a hatályos magyar jogban előírt szakmai titoktartási kötelezettség alapján bizalmasnak kell maradnia.

Az érintett hozzáférési joga – a GDPR 15. cikkében meghatározottakkal összhangban – az alábbi információk rendelkezésre bocsátására terjed ki:

- adatkezelés céljai;
- érintett személyes adatok kategóriái;
- azon címzettek, akikkel a személyes adatokat közlik vagy közölni fogják;
- személyes adatok tárolásának tervezett időtartama;
- érintett jogai a személyes adatok kezelése körében;
- az adatok forrása, amennyiben nem az érintettől gyűjtötték őket;
- automatizált döntéshozatalra vonatkozó információk.

A Társaság minden esetben törekszik arra, hogy az általa az érintettnek adott tájékoztatás minden esetben a GDPR által meghatározott szabályok teljesítése mellett is a lehetőségekhez mérten tömör, átlátható, érthető, könnyen hozzáférhető, világos és közérthető legyen.

A tájékoztatás és intézkedés megtételéréért a Társaság Adatvédelmi managere a felelős a szervezeti egységek vezetői által szolgáltatott adatok alapján. Az írásbeli tájékoztatók mintáit az Adatvédelmi manager a vezérigazgatóval előzetesen jóváhagyja.

A tájékoztatásra vonatkozó adatok birtokában lévő szervezeti egység vezetője köteles az Adatvédelmi managerrel együttműködni, számára előzetesen írásban minden információt, adatot megadni a tájékoztatás teljesítéséhez.

A személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető kell, hogy legyen, valamint azt világosan és egyszerű nyelvezettel kell megfogalmazni. Ez az elv vonatkozik különösen az érintetteknek az adatkezelő kilétéről és az adatkezelés céljáról való tájékoztatására, valamint az azt célzó további tájékoztatásra, hogy biztosított legyen az érintett személyes adatainak tisztességes és átlátható kezelése, továbbá arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a róluk kezelt adatokról.

18.6. Helyesbítés

A valóságnak nem megfelelő adatot az Adatkezelő – amennyiben a szükséges adatok és az azokat bizonyító közokiratok rendelkezésre állnak – indokolatlan késedelem nélkül helyesbíti és azzal egyidőben írásban tájékoztatja az érintettet a helyesbítés tényéről és időpontjáról.

Arra az időtartamra, amíg az Adatkezelő ellenőrzi a személyes adatok pontosságát, a kérdéses személyes adatok korlátozásra kerülnek a jelen Szabályzat 18.8. pontjának megfelelően.

Az adatok módosítását a kapcsolattartásra kijelölt személy végzi

- a központi kapcsolattartásra szolgáló adatbázisban és
- minden olyan szigetszerű alkalmazásban, ahol a központi adatbázis nem szinkronizálódik automatikusan.

A helyesbítésről és annak várható időtartamáról a kapcsolattartásra kijelölt személy tájékoztatja az érintetteket.

Amennyiben az érintett személyes adatának helyesbítését kéri és nem áll rendelkezésre a személyes adat, amelyre a már kezelt adatot helyesbíteni kell, hiánypótlásra hívja fel az Adatkezelő az érintettet.

Az Adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő tájékoztatja e címzettekről.

Az Adatvédelmi manager rendszeresen ellenőrzi az Érintettek adatmódosítási kérelmeinek pontos végrehajtását.

Amennyiben az Érintett olyan adatot szeretne módosítani, amelyet valamely Európai Uniós vagy magyar jogszabályi előírás alapján az adatkezelő nem módosíthat, a Társaság késedelem nélkül, de maximum egy hónapon belül tájékoztatja az Érintettet, hogy a változtatási igényt nem hajtja végre.

18.7. Törlés

Az Adatkezelő az érintett kérésére indokolatlan késedelem nélkül törli a személyes adatot, amennyiben az adatkezelés hozzájáruláson alapult, az érintett kéri az adatok törlését (visszavonja a hozzájárulását) és nincs más adatkezelési jogalap.

Az Adatkezelő törli továbbá a személyes adatokat, amennyiben:

- már nincs szükség a személyes adatokra;
- az érintett a GDPR 21. cikkének megfelelően tiltakozik a személyes adatai kezelése ellen;
- a személyes adatok kezelése jogellenes;
- jogi kötelezettség teljesítése okán szükséges az adatok törlése.

Az érintett törlési jogának korlátozására csak a GDPR-ban írt alábbi kivételek fennállása esetén kerülhet sor, azaz a fenti indokok fennállása esetén a személyes adatok további megőrzése jogszerűnek tekinthető,

a) ha a véleménynyilvánítás és a tájékozódás szabadságához való jog gyakorlása, vagy
b) ha valamely jogi kötelezettségnek való megfelelés (azaz az Adatkezelési Nyilvántartásban jogi kötelezettség jogalappal rögzített tevékenység esetén az adatkezelés céljának megfelelő időtartam alatt), vagy
c) ha közérdekű archiválás céljából, vagy
d) ha tudományos és történelmi kutatás céljából vagy statisztikai célból, vagy
e) ha jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

A személyes adatot az Adatkezelő olyan módon törli, hogy helyreállítása többé ne legyen lehetséges.

Az Adatkezelő minden olyan címzettet tájékoztat a törlésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő tájékoztatja e címzettekről.

Amennyiben az Érintett olyan adatot szeretne törölni, amely valamely Európai Uniós vagy magyar jogszabályi előírás alapján az adatkezelő nem törölhet, a Társaság késedelem nélkül, de legfeljebb egy hónapon belül tájékoztatja az Érintettet, hogy a törlési igényt nem hajtja végre.

18.8. Korlátozáshoz való jog

Az érintett kérelmezheti az Adatkezelőnél a rá vonatkozóan tárolt személyes adatok megjelölését jövőbeli kezelésük korlátozása céljából.

Az adatkezelés korlátozására abban az esetben kerülhet sor, amennyiben:

- az érintett vitatja az adatok pontosságát, az adatok helyességének megállapításáig terjedő időtartamra az Adatkezelő korlátozza a személyes adatok kezelését;
- az adatkezelés jogellenes és az érintett törlés helyett a felhasználás korlátozását kéri;
- az adatkezelőnek már nincs szüksége az adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez;
- az érintett tiltakozik a személyes adatok kezelése ellen a GDPR 21. cikke szerint, a tiltakozással kapcsolatos mérlegelés elvégzésének erejéig.

Az érintett személyes adata kezelése elleni tiltakozásának elbírálásának időtartamára – de legfeljebb 5 napra – az adatkezelést az Adatkezelő Adatvédelmi managere az illetékes szervezeti egység vezetőjének közreműködésével felfüggeszti, a tiltakozás megalapozottságát megvizsgálja és döntést hoz, amelyről a kérelmezőt tájékoztatja.

Amennyiben a személyes adat kezelését az Adatkezelő korlátozza, az ilyen személyes adatot a korlátozás időtartama során - a tárolás kivételével - csak az érintett hozzájárulásával vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve a valamely tagállam fontos közérdekéből lehet kezelni.

Amennyiben az adatkezelés korlátozását az Adatkezelő feloldja, a korlátozás feloldását megelőzően a korlátozás feloldásának tényéről írásban tájékoztatja azt az érintettet, akinek a kérésére a korlátozás megtörtént, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel.

Az Adatkezelő minden olyan címzettet tájékoztat az adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az Adatkezelő Adatvédelmi managere az illetékes szervezeti egység vezetőjének közreműködésével tájékoztatja e címzettekről.

Ha az adatkezelés korlátozását az érintett kérte, a korlátozás feloldásáról az Adatkezelő Adatvédelmi managere az illetékes szervezeti egység vezetőjének közreműködésével előzetesen tájékoztatja az érintettet.

18.9. Tiltakozás

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a közérdekű feladat végrehajtására vagy jogos érdekre hivatkozó jogalapon alapuló kezelése ellen. Vagyis abban az esetben tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja

- a GDPR 6. cikk. (1) bekezdés e) pontja szerinti közérdek vagy
- a GDPR 6. cikk (1) bekezdés f) pontja szerinti jogos érdek.

Tiltakozási jog gyakorlása esetén az Adatkezelő nem kezelheti tovább a személyes adatokat, kivéve, ha az Adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak. Annak megállapítása kapcsán, hogy az adatkezelést kényszerítő erejű jogos okok indokolják, az Adatkezelő vezérigazgatója dönt az Adatkezelő Adatvédelmi managerével történt egyeztetést követően. Az ezzel kapcsolatos álláspontjáról véleményben tájékoztatja az érintettet.

A megállapításig terjedő időtartamra a személyes adatok a 18.8. pontnak megfelelően korlátozásra kerülnek.

18.10. Adathordozhatóság

Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban **megkapja**, továbbá jogosult arra, hogy ezeket az adatokat egy másik **adatkezelőnek továbbítsa** anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, amennyiben:

- az adatkezelés jogalapja az érintett hozzájárulása vagy az adatkezelésre olyan szerződés teljesítése érdekében volt szükség, amelyben az érintett az egyik fél vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges [GDPR 6. cikk (1) bekezdés a) vagy b) pont, illetve 9. cikk (2) bekezdés a) pont] és
- az adatkezelés automatizált módon történik.

Az érintett kérelmezheti továbbá az Adatkezelőtől, hogy az általa kezelt személyes adatokat egy másik, az érintett által egyértelműen megjelölt Adatkezelőnek továbbítsa.

E pontba foglalt jog nem illeti meg az érintettet, ha az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges, valamint, ha ez a jog hátrányosan érintené mások jogait és szabadságait.

A hordozható adatok átadásáért felelős: Adatvédelmi manager**.**

18.11. A hozzájárulás visszavonásához való jog

Amennyiben az érintett személyes adatai Adatkezelő általi kezelésének jogalapja az érintett hozzájárulása, akkor az adatkezeléshez adott hozzájárulását az érintett bármikor visszavonhatja. Az érintettet a hozzájárulás visszavonásának jogáról, illetve a visszavonás módjáról a hozzájárulási nyilatkozatban vagy az ezzel egyidőben átadott adatkezelési tájékoztatóban kell tájékoztatni. A hozzájárulás visszavonásának olyan egyszerűnek kell lenni, mint amilyen egyszerű volt a hozzájárulás megadása. Az Adatkezelő az érintett által adott hozzájárulás visszavonását követően is kezelheti az érintett személyes adatait jogi kötelezettségének teljesítése vagy jogos érdekei érvényesítése céljából, ha az érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

18.12. Az érintetti jogok gyakorlása az érintett halálát követően

Az érintett halálát követő öt éven belül, az elhalálozott személyt életében megillető jogokat az érintett közeli hozzátartozója, vagy az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal – ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal – meghatalmazott személy, illetve az Infotv. szerint meghatározott személy jogosult érvényesíteni.

19. Felelősség, jogorvoslat, jogérvényesítés

19.1. A társaság felelőssége

A Társaság, mint adatkezelő felelősséggel tartozik az érintettek személyes adatai kezelésének jogszerűségéért.

A Társaság, mint adatfeldolgozó csak abban az esetben tartozik felelősséggel az érintettekkel szemben az adatkezelés által okozott károkért, ha nem tartotta be az adatkezelővel kötött szerződésben, illetve az irányadó jogszabályokban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el, egyebekben az adatfeldolgozó a Társaság által végzett adatfeldolgozói tevékenységért úgy felel, mintha maga járt volna el.

Az érintett, aki a GDPR megsértésének eredményeként vagyoni vagy személyiségi jogi jogsértést szenvedett, az elszenvedett kárért az adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.

A bírósági jogorvoslathoz való jogának érvényesítése érdekében az érintett a Társaság, illetve – az adatfeldolgozó tevékenységi körébe tartozó adatkezelési műveletekkel összefüggésben – az adatfeldolgozó ellen bírósághoz fordulhat, ha megítélése szerint az adatkezelő, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a személyes adatait a személyes adatok kezelésére vonatkozó, jogszabályban vagy az Európai Unió kötelező jogi aktusában meghatározott előírások megsértésével kezeli.

Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet a GDPR-t sértő adatkezelés okozott. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a GDPR-ban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Ha a Társaság az érintett adatainak jogellenes kezelésével vagy az adatbiztonság követelményeinek megszegésével az érintett személyiségi jogát megsérti, az érintett sérelemdíjat követelhet.

Az érintettel szemben a Társaság felel az általa igénybe vett adatfeldolgozó által okozott kárért és a Társaság köteles megfizetni az érintettnek az adatfeldolgozó által okozott személyiségi jogsértés esetén járó sérelemdíjat is. A Társaság mentesül az okozott kárért való felelősség és a sérelemdíj megfizetésének kötelezettsége alól, ha bizonyítja, hogy a kárt vagy az érintett személyiségi jogának sérelmét az adatkezelés körén kívül eső elháríthatatlan ok idézte elő.

Az adatkezelő, illetve az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

Amennyiben az érintett úgy ítéli meg, hogy az adatkezelés a GDPR vagy az Infotv. rendelkezéseibe ütközik, illetve sérelmesnek véli, ahogy a Társaság személyes adatait kezeli, úgy panasszal fordulhat a Társasághoz a megadott elérhetőségein, illetve a gdpr@semilab.hu e-mail címen keresztül az Adatvédelmi managerhez is jogosult fordulni.

Az érintett jogosult az Adatkezelő adatkezelési eljárásával kapcsolatos panasszal közvetlenül a hatósághoz fordulni, bejelentéssel élhet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (cím: 1055 Budapest, Falk Miksa utca 9-11., postacím: 1374 Budapest, Pf. 603., telefonszám: +36 (1) 391-1400, E-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu).

Az érintettnek lehetősége van adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben szabadon eldöntheti, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím) szerinti törvényszéknél (http://birosag.hu/torvenyszekek) nyújtja-e be keresetét. A lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a http://birosag.hu/ugyfelkapcsolati-portal/birosag-kereso oldalon.

19.2. A Társaság munkavállalóinak felelőssége, titoktartási kötelezettség

Az adatkezelést végző személy a tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért. Az adatkezelést végző személy tevékenysége során: kezeli és megőrzi a feladata ellátása során birtokába került adatokat; ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására; gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá; betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat; részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon.

A Társaság munkavállalója munkajogi, polgári jogi és büntetőjogi felelősséggel tartozik a munkája során végzett adatkezelési műveletek jogszerűségéért és a jelen Szabályzatban foglaltak betartásáért.

Felróható magatartásnak, ezáltal vétkes kötelezettségszegésnek minősül amennyiben a munkavállaló nem tartja be a jelen Szabályzatban, illetve a személyes adatok kezelésére vonatkozó jogszabályokban foglalt kötelezettségeit. A munkavállalóval szemben ilyen esetben a munkaszerződésében írt hátrányos jogkövetkezmények alkalmazhatóak.

A munkavállaló a jelen Szabályzatban, valamint a jogszabályokban foglalt személyes adatok kezelésére vonatkozó kötelezettségének megszegésével okozott kárt köteles megtéríteni, ha nem úgy járt el, ahogy az adott helyzetben általában elvárható.

Az Mt. 179.§ (3) bekezdés alapján, a kártérítés mértéke nem haladhatja meg a munkavállaló négyhavi távolléti díjának összegét. Szándékos vagy súlyosan gondatlan károkozás esetén a teljes kárt kell megtéríteni.

Nem kell megtéríteni azt a kárt, amelynek bekövetkezése a károkozás idején nem volt előrelátható, vagy amelyet a munkáltató vétkes magatartása okozott, vagy amely abból származott, hogy a munkáltató kárenyhítési kötelezettségének nem tett eleget.

A Társaság valamennyi munkavállalója a Mt. 8. § (4) bekezdése alapján köteles jelen Szabályzat, továbbá a hatályos jogszabályok szerint a rájuk bízott, illetve tudomásukra jutott személyes adatokat és üzleti titkokat időbeli korlátozás nélkül – tehát a munkaviszony megszűnését követően is – megőrizni. A munkavállalók személyes adatokat kizárólag a munkaköri leírásban meghatározott feladatkörükön belül ismerhetik meg.

A Társaság kiemelt hangsúlyt fektet arra, hogy a harmadik személyekkel kötött szerződésekből eredő titoktartási kötelezettségének teljes mértékben eleget tegyen, e kötelezettséget pedig a munkavállalóival, illetve alvállalkozóival is betartassa.

20. Záró Rendelkezések

Jelen Szabályzat valamely pontjának érvénytelensége a Szabályzat hatályát nem érinti.

Jelen Szabályzat a Társaság valamennyi szervezeti egysége és munkavállalója számára kötelező érvényű. Az Mt. 17.§ (2) bekezdése alapján, a Munkáltatói szabályzatot közöltnek kell tekinteni, ha azt a helyben szokásos és általában ismert módon közzéteszik.

Jelen Szabályzat hatálybalépésének ideje: 2021. március 01.

1. sz. Melléklet - A Társaság mindenkori Adatvédelmi managerének neve és elérhetősége

A Társaság jelenlegi Adatvédelmi managerének neve:	**Varga Adrienn**
A Társaság jelenlegi Adatvédelmi managerének e-mail címe:	**gdpr@semilab.hu**
A Társaság jelenlegi Adatvédelmi managerének telefonszáma:	+3670-502-8464

2. sz. Melléklet – Formanyomtatvány (adatvédelmi incidensre utaló körülmények, adatok bejelentéséhez)

Az adatvédelmi incidens a GDPR 4. cikk 12. pontja alapján, a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Szükséges vizsgálni, hogy adott esetben adatvédelmi incidens történt-e, illetve amennyiben igen, szükséges-e azt bejelenteni az illetékes Felügyeleti Hatósághoz.

Példák lehetnek adatvédelmi incidensre a következő esetek:

- ügyféladatbázisának példányát tartalmazó készülék elveszik, vagy ellopják;
- mobiltelefon, pendrive, laptop elvesztése;
- adathordozók ellopása;
- a személyes adatok állományából létező egyetlen példányt zsarolóvírus titkosítja;
- az adatkezelő titkosította a személyes adatok állományából létező egyetlen példányt, de a titkosításhoz használt kulcs már nincs a birtokában;
- előre nem látható károsodás éri az eszközeinket, pl. tűz- vagy vízkár;
- hacker támadás éri az informatikai rendszert;
- rossz helyre küldjük az e-mailt, amely személyes adatokat tartalmaz;
- átadjuk a jelszavainkat valakinek, aki jogosulatlanul hozzáfér a személyes adatokhoz;
- nyilvánosságra hozunk személyes adatokat, amelyeket nem lett volna szabad;
- megtévesztéssel vagy más úton információt szereznek az adatokról illetéktelenek.

A jelen felsorolás csak példálózó jellegű, ha valamely munkavállaló adatvédelmi incidensre utaló eseményt tapasztal vagy ezzel kapcsolatban bármely más releváns információhoz jut, haladéktalanul köteles értesíteni a Társaság Adatvédelmi managerét.

Az értesítés során az incidens észlelésének/körülményeinek szöveges ismertetésével egyidejűleg az alábbi táblázat (Wordben kitöltve) haladéktalanul megküldeni az illetékes részére.

1. Adatvédelmi incidenst észlelő személy adatai	
Az incidenst észlelő személy neve:	
Az incidenst észlelő személy szervezeti egységének megnevezése és elérhetőségei (telefonszám, e-mail cím):	
2. Időpontok, helyszín,	
Adatvédelmi incidens időpontja, helyszíne	
Adatvédelmi incidens kezdő időpontja	
Adatvédelmi incidens záró időpontja	
Az adatvédelmi incidens továbbra is fennáll	Igen/Nem
Az incidensről való tudomásszerzés	

időpontja		
Az incidens észlelésének módja		
Adatvédelmi incidens körülményeinek leírása		
3. Az adatvédelmi incidensről		
Bizalmas jelleg	Sérült/Nem sérült	
Integritás	Sérült/Nem sérült	
Rendelkezésre állás[1]	Sérült/Nem sérült	
Adatvédelmi incidens jellege (több válasz is elfogadható)		adathalászat
		elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön)
		eszköz elvesztése vagy ellopása
		informatikai rendszer feltörése (hackelés)
		levél elvesztése vagy jogosulatlan felnyitása
		papír alapú dokumentum elvesztése, ellopása, vagy olyan helyen hagyása, amely nem minősül biztonságosnak
		papír alapú dokumentum nem megfelelő módon történő megsemmisítése
		rosszindulatú számítógépes programok pl. Zsarolóprogram
		személyes adatok jogosulatlan megismerése
		személyes adatok jogosulatlan szóbeli közlése
		személyes adatok nagy nyilvánosság előtti jogellenes közzététele
		személyes adatok téves címzett részére történő elküldése
		egyéb
Adatvédelmi incidens részletes leírása:		
Adatvédelmi incidens okai (több válasz is elfogadható)		külső, rosszhiszemű cselekmény
		külső, rosszhiszeműnek nem minősülő cselekmény
		szervezeten belüli, rosszhiszemű cselekmény
		szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény
		egyéb
Adatvédelmi incidens egyéb okainak leírása		
4. Az adatvédelmi incidenssel érintett adatok köre		
4.1 Személyes adatok		
Személyazonossághoz kapcsolódó adatok	Érintett/Nem érintett	
Személyi szám	Érintett/Nem érintett	
Elérhetőségi adatok (e-mail cím, telefonszám)	Érintett/Nem érintett	
Amennyiben elérhetőségi adatok érintettek, azok céges kapcsolattartóhoz vagy magánszemélyhez tartoznak?		

[1] Lásd: 7.1., 7.2., 7.3. pont

Azonosító adatok	Érintett/Nem érintett
Gazdasági, pénzügyi adatok	Érintett/Nem érintett
Képfelvétel	Érintett/Nem érintett
Hangfelvétel	Érintett/Nem érintett
Hivatalos okmányok	Érintett/Nem érintett
Helymeghatározó adatok	Érintett/Nem érintett
Biometrikus adatok	Érintett/Nem érintett
Büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok	Érintett/Nem érintett
4.2 Különleges adatok	
Faji eredetre, nemzetiséghez tartozásra vonatkozó adatok	Érintett/Nem érintett
Politikai véleményre vonatkozó adatok	Érintett/Nem érintett
Vallásos vagy más világnézeti meggyőződésre vonatkozó adatok	Érintett/Nem érintett
Érdek-képviseleti szervezeti tagságra vonatkozó adatok	Érintett/Nem érintett
Szexuális életre vonatkozó adatok	Érintett/Nem érintett
Egészségügyi adatok	Érintett/Nem érintett
Genetikai adatok	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb személyes adatok leírása	
Az adatvédelmi incidenssel érintett személyes adatok becsült száma	
5. Az érintettek	
Alkalmazottak	Érintett/Nem érintett
Felhasználók	Érintett/Nem érintett
Feliratkozók	Érintett/Nem érintett
Diákok	Érintett/Nem érintett
Ügyfelek (jelenlegi és potenciális)	Érintett/Nem érintett
Kiskorúak	Érintett/Nem érintett
Kiszolgáltatott személyek	Érintett/Nem érintett
Hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek	Érintett/Nem érintett
Még nem ismert	Érintett/Nem érintett
Egyéb	Érintett/Nem érintett
Az egyéb leírása	
6. Az incidens ELŐTT és UTÁN alkalmazott intézkedések	
Az adatvédelmi incidens előtt alkalmazott intézkedések leírása	
Amennyiben eszköz érintett az incidens során, abban az esetben	

volt-e az incidenssel érintett eszközön képernyőzár, PIN kód?	
Amennyiben eszköz érintett az incidens során, abban az esetben az incidenssel érintett eszköz tartalmazott- e céges levelezést, magánlevelezést, magán telefonszámokat vagy képeket, egyéb, személyes adatot tartalmazó fájlokat? Ha igen, kérjük típusonként feltüntetni a darabszámot!	
Amennyiben eszköz érintett az incidens során, abban az eszköz tartalmazott-e SD kártyát vagy memóriakártyát?	
Amennyiben eszköz érintett az incidens során, abban az esetben az eszközhöz való hozzáférés letiltásra került-e az incidenst követően?	
Amennyiben eszköz érintett az incidens során, abban az esetben, ha az eszköz letiltásra került, a letiltásra mikor és milyen módon került sor?	
Amennyiben eszköz érintett az incidens során, abban az esetben az incidens óta észleltek-e illetéktelen belépést vagy hozzáférést az eszköz használatával kapcsolatban?	
7.Következmények	
7.1. Bizalmas jelleg sérülése	
Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult	Igen/Nem
Az adat összekapcsolhatóvá vált az érintett egyéb adatával	Igen/Nem
Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges	Igen/Nem
Egyéb	Igen/Nem
Az egyéb bizalmas jelleget érintő következmény leírása	
7.2. Integritás sérülése	
Az adat módosíthatóvá vált annak ellenére, hogy archivált elavult adat volt	Igen/Nem
Az adatot valószínűsíthetően	Igen/Nem

módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták		
Egyéb	Igen/Nem	
Az egyéb integritást érintő következmény leírása		
7.3 Rendelkezésre állás sérülése		
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének elvesztése	Igen/Nem	
Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása	Igen/Nem	
Egyéb	Igen/Nem	
Az egyéb rendelkezésre állást érintő következmény leírása		
7.4 Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények		
Az incidens valószínűsíthető hatásai az érintettekre (több válasz is elfogadható)		álnevesítés engedély nélküli feloldása
		érintett jogainak korlátozása
		hátrányos megkülönböztetés
		jó hírnév sérelme
		pénzügyi veszteség
		szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése
		személyazonosság-lopás
		személyazonossággal való visszaélés
		személyes adatok feletti rendelkezés elvesztése
		egyéb
Az egyéb valószínűsíthető hatások leírása		
A valószínűsíthető következmények súlyossága		elhanyagolható
		korlátozott
		jelentős
		maximális