SELFIEGATE.HU

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

2025. október 22.

Borka Tamás ev.

1046 Budapest, Káposztásmegyeri út 16/a FSZT. 3.

Tartalom

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Bevezetés és Az adatkezelő adatai

Neve: Borka Tamás ev.
Székhelye: 1046 Budapest, Káposztásmegyeri út 16/a. Fszt. 3.
Képviseli: Borka Tamás
Adószáma: 56973686-1-41
Telefonszáma: +36 20 961 9382
Email címe: selfiegate@gmail.com
Honlap: www.selfiegate.hu
Adatvédelmi tisztviselő neve: a GDPR 37. cikk szerint nem alkalmaz.
Adatvédelmi ügyekben eljár: Borka Tamás

A Borka Tamás EV. a (továbbiakban, mint Társaság vagy Adatkezelő) mint Adatkezelő, magára nézve kötelezőnek ismeri el jelen jogi szabályzat tartalmát. Kötelezettséget vállal arra, hogy tevékenységével kapcsolatos minden adatkezelés megfelel a jelen szabályzatban és a hatályos nemzeti} jogszabályokban, valamint az Európai Unió aktusaiban meghatározott elvárásoknak.

Az Adatkezelő elkötelezett ügyfelei és partnerei személyes adatainak védelmében és kiemelten fontosnak tartja ügyfelei és munkatársai információs önrendelkezési jogainak} tiszteletben tartását. Az adatkezelő a személyes adatokat bizalmasan kezeli és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.

Az Adatkezelő kijelenti, hogy a személyes adatok kezelése során az alábbi szabályokat mindenképpen betartja:

- A személyes adatok kezelését jogszerű és átlátható módon kell végezni, biztosítva a személyeknek a rájuk vonatkozó személyes adatok kezelésének tisztességességét és a kezelés átláthatóságát.
- A személyes adatkezelésnek konkrét célja kell, hogy legyen, és ezt már az adatok gyűjtésének időpontjában közölnünk kell az érintettel.
- Az Adatkezelő soha nem gyűjt személyes adatokat célhoz kötöttség nélkül.
- Az Adatkezelő. kizárólag olyan személyes adatokat gyűjthet és kezelhet, amelyek a cél eléréséhez szükségesek.
- Az Adatkezelő működése során biztosítania kell, hogy a személyes adatok pontosak és naprakészek legyenek, szem előtt tartva, hogy a pontatlan személyes adatokat kijavítsák.
- Biztosítania kell továbbá, hogy a személyes adatokat kizárólag az adatkezelés céljainak eléréséhez szükséges ideig tárolják.
- A személyes adatok kezelését az adatkezelőnek olyan módon kell elvégeznie, hogy a technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, ideértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.

Az Adatkezelő a fen} célok eléréséhez szükséges alábbi tevékenységek elvégzését írásbeli dokumentumokkal támasztja alá:

- – már az üzleti tervekben figyelembe vette az adatvédelem szabályait (beépített és alapértelmezett adatvédelem)
- – a GDPR szabályainak megfelelően tevékenykedő adatfeldolgozót bízott meg,

- – az adatkezelési nyilvántartásai naprakészek,
- – megtett minden szükséges adatbiztonsági intézkedést,
- – az incidenseket megelőző intézkedéseket megtette, és az adatsértéseket azonnal kezelni tudná (van rá technológia és eljárási rend is),
- – adatvédelmi tisztviselőt nem nevezett ki.

Az Adatkezelő. tevékenységének adatkezelése önkéntes hozzájáruláson, illetve törvényi felhatalmazáson alapul.

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETÉNEK – (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról,
- a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: Rendelet)
- az információs önrendelkezési jogról és az információszabadságról szóló 2018. évi XIII. törvény (a továbbiakban: Rendeletv.) rendelkezéseinek
- 2013. évi V. törvény – a Polgári Törvénykönyvről (Ptk.)
- 2000. évi C. törvény – a számvitelről (Számv. tv.)
- 2007. évi CXXXVI. törvény– a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról (Polgári törvénykönyv.)
- 2017. évi CL törvény – az adózás rendjéről (Adótv.)
- 1995. évi CXIX. törvény – a név és lakcímadatokról
- 1774/2002. évi Eu Rendelet
- 71/2003. (VI.27.) FVM rendelet
- 1995. évi LIII. törvény a környezetvédelemről
- 210/2009. (IX.29) Kormányrendelet a kereskedelmi tevékenységről
- 2001. évi CVIII. törvény – az elektronikus kereskedelemről
- 45/2004. (II. 26.) Kormányrendelet az elektronikus kereskedelemről
- 2008. évi XLVIII törvény– a reklámtevékenységről és a kereskedelmi közlésről

2. A Szabályzat célja

A Szabályzat célja azon belső szabályok megállapítása és intézkedések megalapozása, amelyek biztosítják, hogy a Társaság adatkezelő tevékenysége megfeleljen a Rendelet, és az Infotv, és a vonatkozó ágazati} jogszabályok rendelkezéseinek.

A Szabályzat célja továbbá, hogy a Rendeletnek, és az abban megfogalmazott, a személyes adatok kezelésére vonatkozó elveknek (5. cikk) való megfelelés Társaság általi igazolására szolgáljon.

3. A Szabályzat hatálya

Személyi hatály

Jelen szabályzat személyi hatálya kiterjed a Társasággal munkaviszonyban, vagy munkavégzésre irányuló jogviszonyban álló valamennyi olyan természetes személyre, jogi személyre és jogi személyiséggel nem rendelkező szervezetre, mely a Társasággal kapcsolatos jogviszonyból eredően személyes adatot kezel vagy a személyes adatok kezelésével kapcsolatos szabályokat hoz.

E Szabályzat hatálya csak a természetes személyre vonatkozó személyes adatok Társaság általi kezelésére terjed ki.

Egyéni vállalkozó, egyéni cég, egyszemélyes KFT, őstermelő ügyfeleket, vevőket, szállítókat e szabályzat alkalmazásában természetes személynek kell tekinteni.

A Szabályzat hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre vonatkozik, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat.

Tárgyi hatálya

E szabályzat tárgyi hatálya kiterjed a személyes adatokat is tartalmazó nyilvántartások és a kapcsolódó iratok kezelésével összefüggő teljes adatkezelési és informatikai folyamatra, valamint a kapcsolódó informatikai eszközre és szoftverre, a keletkezett iratokra, tekintet nélkül annak fellelési helyétől. Így különösen:

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- a Társaság tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint az informatikai eszközök műszaki dokumentációira,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer– és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

4. Fogalom meghatározások

E Szabályzat alkalmazásában irányadó fogalom meghatározásokat a Rendelet 4. cikke tartalmazza. Ennek megfelelően emeljük ki a főbb fogalmakat:

- „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;
- „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
- „az adatkezelés korlátozása”: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- „profilalkotás”: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják;
- „álnevesítés”: a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

- „nyilvántartási rendszer”: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális, vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
- „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
- „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
- „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;
- „harmadik fél”: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
- „az érintett hozzájárulása”: az érintett akaratának önkéntes, konkrét és 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;
- „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;
- „felügyeleti hatóság”: egy európai uniós tagállam által a GDPR 51. cikknek megfelelően létrehozott független közhatalmi szerv;
- „érintett”: az a természetes személy, akinek a személyes adatait kezelik.

II. AZ ADATKEZELÉS JOGSZERŰSÉGÉNEK BIZTOSÍTÁSA

A személyes adatok kezelésének megkezdése előtt minden esetben dönteni kell arról, hogy a felhasználni kívánt személyes adatra ténylegesen szükség van-e. Személyes adatok kezelését kizárólag akkor lehet megkezdeni, ha kétséget kizáróan indokolható, hogy az adatkezelés célját más módon vagy kevesebb adat igénybevételével, megvalósítani nem lehetséges.

A Társaság köteles az érintettek személyes adatait jogszerűen, tisztességesen, átlátható módon kezelni. Senkit nem érhet hátrány abból eredően, hogy a Társaságnál, illetve a jelen Szabályzatban meghatározott egyéb hatóságnál eljárást, jogorvoslatot kezdeményezett vagy bejelentést tett, illetve, hogy a hozzájáruláson alapuló adatkezelés esetén a hozzájárulását nem adta meg, illetve azt később visszavonta.

Az érintettek személyes adatainak gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet. A Társaság köteles tevékenységi köreinek megtervezésekor elkerülni, illetve később megszüntetni minden olyan adatkezelést, amely az adott személyes adatra vonatkozó céllal össze nem egyeztethető módon történik. A Társaság csak a szükséges mértékben jogosult személyes adatot kezelni és köteles minden olyan személyes adatot törölni, amelynek tekintetében az adatkezelés célja megszűnt, illetve az adatkezelés célja nem igazolható.

A Társaság magánszemélyek személyes adatait az alábbi jogalapokon kezelheti:

1. Hozzájárulás

Az érintett-amennyiben a hozzájárulás önkéntessége bizonyítható- hozzájárulást adhat személyes adatainak kezeléséhez. Az érintett a hozzájárulását önkéntes alapon adja és jogosult azt bármikor indoklás nélkül, ugyanolyan egyszerű módon, ahogy a hozzájárulását megadta, visszavonni. A visszavonás nem érinti az azt megelőzően végrehajtott adatkezelés jogszerűségét

A hozzájárulás az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilatkoztatása. Az önkéntesség fogalmilag, valódi választási lehetőséget biztosít az érintettnek. Így nem értelmezhető a hozzájárulás megadásának megtagadása együtt jár valamely szolgáltatásból történő kizárással, tehát negatív következménye van. A hozzájáruláson alapuló adatkezelés nem értelmezhető olyan helyzetben sem, amikor a két fél között hatalmi egyensúlyhiány van.

Kifejezett a hozzájárulás szükséges speciális, az érintettre jelentős adatvédelmi kockázattal járó esetekben.

Az elszámoltathatóság elve értelmében az adatkezelőt igazolási kötelezettség terheli, így az Adatkezelőnek igazolnia kell, hogy az érintett személyes adatai kezeléséhez hozzájárult.

A hozzájárulás bármikor visszavonható és erről az érintettet a hozzájárulása megadása előtt tájékoztatni kell.

Az Adatkezelő. hozzájáruláson alapuló adatkezelés esetén, csak akkor kezel személyes adatokat, ha a hozzájárulás önkéntes alapon, tájékoztatáson alapul, konkrét célt szolgál, az adatkezelés minden okát világosan meghatározva, explicit és pozitív művelet eredménye.

A hozzájárulás előtt az érintettek minden esetben, egyértelmű és egyszerű nyelvezetű, jól látható, visszavonható és a hozzájárulás visszavonásának lehetőségét elmagyarázó írásbeli tájékoztatót kapnak és írnak alá. A tájékoztatás mindig tömör, érthető és könnyen hozzáférhető formában, világos nyelven és mindenki számára közérthetően megfogalmazva kerül megadásra.

A tájékoztatónak az alábbi pontokat kötelezően tartalmaznia kell:

- az adatkezelő, és az adatvédelmi tisztviselő elérhetősége;
- meg kell jelölni milyen célból, gyűjtjük az adatokat;
- meg kell jelölni az adatok kategóriáit;
- meg kell jelölni az adatkezelés jogalapját;
- ha más adatkezelő is megkaphatja az adatokat, ezt is közölni kell;
- továbbítjuk–e az EU–n kívülre az adatokat;
- tájékoztatást kap az érintett arról, hogy megkaphatja a gyűjtött adatokat, mert ehhez hozzáférési joga van;
- tájékoztatni kell az adatvédelmi jogairól;
- tájékoztatni kell, hogy joga van panaszt benyújtani az adatvédelmi hatósághoz;
- tájékoztatni kell, hogy bármikor joga van visszavonni a hozzájárulását;
- tájékoztatni kell az automatizált adatkezelésen alapuló döntéshozatal létezéséről, annak logikájáról és annak következményeiről;
- végül tájékoztatni a hozzájárulás megtagadásának következményeiről.

A tájékoztatásnak díjmentesnek kell lennie.

2. Szerződés előkészítése és teljesítése:

Ez a jogalap alkalmazható olyan szerződés (pl. szolgáltatás nyújtására irányuló szerződés, munkaszerződés, tanulmányi szerződés, adásvételi szerződés stb.) teljesítéséhez szükséges adatkezelések esetén, amelyben az érintett az egyik fél, vagy ha az adatkezelés a szerződés megkötését megelőzően az érintett személy kérésére történő lépések megtételéhez szükséges. Az adatkezelés megfelelő alapja, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség.

Szűken kell értelmezni, vagyis a szerződés megkötését megelőző, a szerződéskötéshez vezető adatkezelés esetén a szerződés teljesülése után már nem megfelelő jogalap az adatkezelésre. (GDPR 6. cikk (1) b) pont;

3. Jogi kötelezettség teljesítése

Az uniós vagy nemzetközi} jog által megkívánt adatkezelés. Az adatkezelés jogalapja lehet egy uniós vagy nemzetközi} jogban foglalt kötelezettségnek a teljesítése. A kötelezettségnek kötelező érvényű jogszabályon kell alapulnia, ebben az esetben az adatkezelés célját is az uniós vagy nemzetközi jogszabályban kell meghatározni. GDPR 6. cikk (1) bekezdés c) pont;

4. Létfontosságú érdek

A létfontosságú érdek, mint adatkezelési jogalap akkor alkalmazható, ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekének védelme miatt szükséges. A létfontosságú érdek, mint jogalap korlátozottan alkalmazható, kizárólag komoly veszélyhelyzet fennállása esetén. (GDPR 6. cikk (1) d) pont;

5. Közérdek és közhatalmi jogosítvány alapján

A közérdekű adatkezelés jogalapként akkor alkalmazható, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Ide tartozik, amikor az Adatkezelőtől adatszolgáltatást kérnek közfeladat teljesítése érdekében és a személyes adat adatszolgáltatásának nem a hatóság megkeresésén és nem jogszabályon alapul. (GDPR
6. cikk (1) bekezdés e) pont;

6. Jogos érdek

A Társaság vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges adatkezelések. A Társaság vagy harmadik fél jogos érdekét az adott adatkezelési célra vonatkozó Adatkezelési Tájékoztatóban is rögzíti. Jogos érdeken alapuló adatkezelés csak abban az esetben történhet, ha a Társaság érdekmérlegelési tesztet készít. A tesztben rögzíti és megvizsgálja, hogy a Társaság jogos érdeke arányosan korlátozza-e az érintett személyes adatok védelméhez való jogait, a magánszféráját, illetve az is, hogy miként biztosítható az egyensúly a Társaság és az érintett érdekei között. GDPR 6. cikk (1) bekezdés f) pont.

Az érdekmérlegelési teszt során figyelembe veendő kérdések és a teszttartalma:

1. Az adatkezelés céljának pontos meghatározása, milyen adatkategóriák, mennyi ideig tartó kezelését igényli a jogos érdek.
2. Az adatkezelő jogos érdekének a lehető legpontosabb meghatározása.
3. A cél elérése érdekében feltétlenül szükséges a személyes adatok kezelése? Vannak–e alternatív megoldások, amelyek alkalmazásával a személyes adatok kezelése nélkül, vagy kevesebb személyes adattal is megvalósítható a tervezett cél?
4. Annak meghatározása, hogy melyek lehetnek az érintett érdekei az adott adatkezelés vonatkozásában, amelyeket felhozhatna az adatkezeléssel szemben?

E. Annak meghatározása, hogy miért korlátozza arányosan az adatkezelői jogos érdek az érintett jogokat.

7. Az adatkezelés elmaradásának következményei:

– amennyiben a Társaság az érintett személytől gyűjti az adatokat és az érintett a fenti jogalapokon kezelt adatokat nem adja meg, akkor az adatszolgáltatás elmaradásának következménye az adott szerződés előkészítésének vagy teljesítésének elmaradása, lehetetlenülése lehet.

– amennyiben az érintett személy az általa szolgáltatandó adatoknak csak egy részét adja meg, akkor a nem teljes körűen szolgáltatott adatok alapján kell megítélni, hogy az adatszolgáltatás elmaradása okozhatja–e a szerződés létrejöttének vagy teljesítésének elmaradását.

Szerződésen alapuló adatkezelés esetén a lehetetlenülés jogkövetkezményeit a Társaság csak akkor alkalmazhatja, ha igazolja, hogy a szolgáltatott adat nélkül az érintett személy által indítványozott szerződés teljesítésére nem képes.

III. A SZEMÉLYES ADATOK KATEGÓRIÁI

Személyes adat az 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.

1. Különleges adatok

A természetes személyeket megillető alapvető jogok és szabadságok miatt a különleges adatok természetüknél fogva érzékeny és kockázatot jelentő adatok, melyek megkülönböztetett védelmet igényelnek. Amellett, hogy jogalap szerint kell, történjen az adatkezelés, a Társaság az érintett különleges adatait – ideértve elsősorban az egészségügyi adatokat – különösen az alábbi esetekben kezelhető (hozzájárulás jogalap esetén csak a kifejezett hozzájárulás alkalmazandó):

- Kifejezett hozzájárulás: Az érintett személykifejezett hozzájárulást adhat személyes adatai különleges kategóriáinak kezeléséhez
- GDPR 9. cikk (2) bek. b) vagy h) pontja szerinti esetben: Ez az esetkör alkalmazható pl. a foglalkoztatást szabályozó előírásokból fakadó munkáltatói kötelezettség teljesítése és joggyakorlás érdekében történő adatkezelésre, továbbá megelőző egészségügyi vagy munkahelyi egészségügyi célból a munkavállaló munkavégzési képességének felmérése céljából európai uniós vagy nemzeti jogszabály alapján vagy egészségügyi szakemberrel kötött szerződés értelmében. A megelőző egészségügyi vagy munkahelyi egészségügyi célból történő adatkezelés további feltétele, hogy ezen adatok kezelése olyan szakember vagy személy által, vagy olyan szakember felelőssége mellett történik, akit uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott (szakmai) titoktartási kötelezettség hatálya alatt áll.
- GDPR 9. cikk (2) bek. f) pontja szerinti esetben: Ez az esetkör alkalmazható, ha a különleges adat kezelésére jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges célból kerül sor.
- Egyéb, az adott adatkezelési cél szempontjából egyedi adatkezelési esetkörök lehetnek még a különleges adatok tekintetében:

  az Érintett vagy egy másik természetes személy létfontosságú érdeke, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes hozzájárulást adni;

  az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az Érintett kifejezetten nyilvánosságra hozott;

  az adatkezelés jelentős közérdek miatt szükséges uniós jog vagy tagállami jog alapján; az adatkezelés a népegészségügy területét érintő közérdekből szükséges; valamint

illetve a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő adatkezelés.

Fentek alapján a Társaság kizárólag akkor kezelhet különleges adatokat, ha fennáll az alábbi feltételek egyike:

1. megkapta az érintett magánszemély kifejezett hozzájárulását;
2. uniós vagy magyar jog, vagy kollektív megállapodás értelmében a szolgáltatónak kötelessége az adatkezelés elvégzése;
3. az adatkezelés az érintett személy létfontosságú érdekeinek a védelme miatt szükséges, vagy az érintett személy fizikailag vagy jogilag képtelen a hozzájárulás megadására,
4. az adatkezelés olyan személyes adatokra vonatkozik, amelyet az érintett személy kifejezetten nyilvánosságra hozott;

E. az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges;

6. az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy magyar jog alapján;
7. az adatkezelés a következő célokból történik: megelőző egészségügyi vagy munkaegészségügyi cél, munkavállaló munkavégzésének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy magyar jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében;
8. az adatkezelés a népegészségügy területét érintő közérdekből szükséges, uniós vagy magyar jog alapján;
9. az adatkezelő valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet, az adatkezelés pedig az ilyen szerv jelenlegi vagy volt tagjaira, vagy a szervezettel rendszeres kapcsolatban álló személyekre vonatkozik;
10. az adatkezelés archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges uniós vagy magyar jog alapján.

Az Adatkezelő csak akkor kezeli 16 éves aluli gyermek személyes adatait, ha rendelkezik a gyermek törvényes képviselőjének a kifejezett írásbeli hozzájárulásával.

IV. A TÁRSASÁG TÁJÉKOZTATÁSI KÖTELEZETTSÉGE ÉS INTÉZKEDÉSEI

Az érintettek tájékoztatása az adatkezelő kötelezettsége, amely az átláthatóság alapelvének megvalósítását szolgálja. Az érintetteket tájékoztatni kell az adatkezelő elérhetőségéről, az adatkezelés lényeges körülményeiről, az érintett jogairól és a jogérvényesítés lehetőségeiről.

A tájékoztatást abban az esetben is meg kell adni az érintetteknek, ha a személyes adatokat nem tőlük gyűjtötték. A tájékoztatás megadásának határideje a két esetkörben a következők szerint változik:

1. ha a személyes adatokat az érintettől gyűjtik, az adatok gyűjtésekor,
2. ha a személyes adatok más forrásból származnak, az adatok megszerzésétől számított 1 hónapon belül (ha kapcsolattartásra használják az adatokat, az első kapcsolat felvételekor) kell az érintetteket tájékoztatni.

A tájékoztatás garanciális jellegű az érintett jogok gyakorlása szempontjából, ezért az érintettet

1. érthető és átlátható módon
2. főszabály szerint írásban (elektronikus út is ideértendő), az érintett kérésére szóban
3. díjmentesen kell tájékoztatni.

A fentiek alapján a Társaság köteles tömör, átlátható és könnyen hozzáférhető formában, világosan és közérthetően az érintett személyek rendelkezésére bocsátani bizonyos, az adatkezelésre vonatkozó információkat és tájékoztatni az őket megillető jogokról. Továbbá az érintettek kérelmére bizonyos eljárási szabályok betartásával a Társaság intézkedéseket tehet.

A tájékoztatási kötelezettségek alapján a Társaság az alábbiakról köteles értesíteni az érintettet:

1. A Társaságnak és – ha van ilyen – a Társaság képviselőjének a kiléte és elérhetőségei,
2. az adatvédelmi tisztviselő elérhetőségei, ha a Társaságnál adatvédelmi tisztviselőt jelöltek ki,
3. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja,
4. a GDPR 6. cikk (1) bekezdésének f) pontján alapuló adatkezelés esetén, a Társaság vagy harmadik fél jogos érdekei,

E. adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen,

6. adott esetben annak ténye, hogy a Társaság harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá az Európai Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a GDPR 46. cikkben, a GDPR 47. cikkben vagy a GDPR 49. cikk (1) bekezdésének második pontjában említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás,
7. a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai,
8. az érintett azon joga, 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 joga,
9. a GDPR 6. cikk (1) bekezdésének a) pontján vagy a GDPR 9. cikk (2) bekezdésének a) pontján alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét,
10. a felügyeleti hatósághoz címzett panasz benyújtásának joga,
11. az, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul– e, vagy szerződés kötésének előfeltétele–e, az érintett köteles–e megadni az adatokat és milyen következményekkel járhat az adatszolgáltatás elmaradása,
12. a GDPR 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az Érintettre nézve milyen várható következményekkel bír.

A Társaság a tájékoztatási kötelezettségét: -

- ügyfelei felé a társaság honlapján és nyilvánosság felé megnyitott üzlet helyiségében elhelyezett Adatkezelési Tájékoztató kihelyezésével teljesíti,
- munkavállalóinak az adatvédelmi szabályzatáról oktatást ad, és munkavállalóit írásban tájékoztatja a személyes adataik kezelésével kapcsolatos eljárásrendjéről.

V. AZ ÉRINTETT SZEMÉLY JOGAI

1. Az átlátható tájékoztatás

Az érintettek tájékoztatása az adatkezelő kötelezettsége, amely az átláthatóság alapelvének megvalósítását szolgálja. Az érintetteket tájékoztatni kell az adatkezelő elérhetőségéről, az adatkezelés lényeges körülményeiről, az érintett jogairól és a jogérvényesítés lehetőségeiről.

A tájékoztatást abban az esetben is meg kell adni az érintetteknek, ha a személyes adatokat nem tőlük gyűjtötték. A tájékoztatás megadásának határideje a két esetkörben a következők szerint változik:

- ha a személyes adatokat az érintettől gyűjtik, az adatok gyűjtésekor,
- ha a személyes adatok más forrásból származnak, az adatok megszerzésétől számított 1 hónapon belül (ha kapcsolattartásra használják az adatokat, az első
- kapcsolat felvételekor) kell az érintetteket tájékoztatni.

A tájékoztatás garanciális jellegű az érintett jogok gyakorlása szempontjából, ezért az érintettet

- érthető és átlátható módon

- főszabály szerint írásban (elektronikus út is ideértendő), az érintett kérésére szóban
- díjmentesen kell tájékoztatni.

A tájékoztatás időpontja:

- munkavállaló – munkába álláskor az Mt. 46. §. szerinti tájékoztató átadásával egyidejűleg
- vezető tisztségviselő– kinevezéssel/megbízással egyidejűleg
- új munkatárs toborzásakor– a hirdetés feladásával egyidejűleg, ezek hiányában az ajánlatátadással egyidejűleg
- ajánlattevő– ajánlati felhívással egyidejűleg
- résztvevő– esemény szervezésével egyidejűleg
- szerződéses partner– szerződéskötéssel egyidejűleg
- ingatlanba belépő vendég–a belépéssel egyidejűleg.

2. Hozzáféréshez való jog

A hozzáféréshez való jog az átláthatóság alapelvének megvalósítását szolgálja. Az érintett kérelmére vissza kell neki igazolni, hogy a személyes adatai kezelése folyamatban van-e, és ha igen, akkor hozzáférést kell biztosítani számára a kezelt személyes adataihoz, valamint hozzáférést kell biztosítani neki az alábbi információkhoz:

- az adatkezelés célja,
- a kezelt személyes adatok kategóriái,
- a címzettek,
- a tárolás tervezett időtartama,
- az érintett jogai,
- a panasz benyújtásának joga (jogorvoslati jog)
- az automatizált döntéshozatal ténye, ideértve a profilalkotást is.

3. Helyesbítéshez való jog

Ez a jog a pontosság alapelvének való megfeleltetést érvényesít. Ha az Adatkezelő. által kezelt adatok nem pontosak az érintett kérhet a rá vonatkozó pontatlan személye adat helyesbítését vagy kiegészítését.

4. Törléshez való jog

Az Adatkezelő. köteles törölni az érintett kérésére a rá vonatkozó személyes adatot, ha

- az adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,
- az érintett visszavonja a hozzájárulását és az adatkezelésnek nincs más jogalapja,
- az érintett a saját helyzetével összefüggő okokból a jogos érdeken, vagy közfeladat teljesítésén alapuló adatkezelés ellen tiltakozik, ideértve a profilalkotást is és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy marketingtevékenység ellen tiltakozik,
- a személyes adatokat jogellenesen kezelték,
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy nemzeti jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

Az Adatkezelő nem köteles törölni az adatokat az érintett kérelmére, ha valamelyik alább felsorolt kivétel alkalmazandó. Nem törölhető az érintettre vonatkozó személyes adatok, ha az adatkezelés szükséges

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,

- az adatkezelőre alkalmazandó uniós vagy nemzeti jog szerinti kötelezettség teljesítése, illetve közérdekből vagy közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából,
- népegészségügy területét érintő közérdek alapján,
- közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést,
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

5. Korlátozáshoz való jog

Az adatok korlátozása esetén az Adatkezelő csak tárolhatja a személyes adatokat, de egyéb módon nem kezelhet őket. Ez alól kivétel az érintett hozzájárulásával történő adatkezelés, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében vagy az unió illetve valamely tagállam fontos közérdekéből történő adatkezelés.

Az érintett kezelt személyes adatai korlátozását az alábbi esetekben kérhet

- ha az érintett vitatja a személyes adatok pontosságát, a korlátozás arra az időtartamra vonatkozik, amíg az adatkezelő ellenőrzi a személyes adatok pontosságát,
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett a saját helyzetével összefüggő okokból a jogos érdeken vagy közfeladat teljesítésén alapuló adatkezelés ellen tiltakozik, ideértve a profilalkotást is, a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek–e az érintett jogos indokaival szemben.

6. Adathordozhatósághoz való jog

Az adathordozhatóság joga a GDPR által bevezetett új jog, ami az adatok szabad áramlását biztosítja az Európai Unión belül. Az érintett akkor élhet-e jogával, ha

- az adatkezelés hozzájáruláson alapul vagy szerződés teljesítése érdekében és
- automatizált módon történik.

Az adathordozhatóság nem egy általános jog, csak a fen} esetben élhet vele az érintett. Amennyiben az érintett él-e jogával, jogosult arra, hogy

- a rá vonatkozó személyes adatokat géppel olvasható formátumban megkapja, vagy
- kérheti, hogy az adatkezelő közvetlenül továbbítsa az érintettre vonatkozó személyes adatokat egy másik adatkezelő részére.

7. Tiltakozáshoz való jog

Az érintett akkor élhet e jogával, ha az adatkezelés jogos érdeken vagy közérdekű adatkezelésen alapul és az érintett saját helyzetével kapcsolatos okból változik az adatkezelés során bármikor. Következménye főszabály szerint az, hogy az adatkezelő a személyes adatokat nem kezelhet tovább.

Kivétel, ha az adatkezelő bizonyítja, hogy

- az adatkezelést kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy
- jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak, az Adatkezelő ezekben az esetekben jogosult a személyes adatokat tovább kezelni.

Speciálisan alakul a tiltakozáshoz való jog direkt marketing tevékenység esetén. Ebben az esetben, ha az érintett tiltakozik az adatok kezelése ellen, ideértve a profilalkotást is, az adatkezelő nem kezelhet tovább a személyes adatokat (ebből a célból).

8. Jogorvoslathoz való jog

Az érintett jogosult a felügyelet hatóságnál panasz benyújtására (panasztételhez való jog), illetve bírósági jogorvoslatra.

A Felügyeleti hatóság Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatósága (NAIH) (cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c., telefon: +36 (1) 391-1400, honlap:), akihez az érintett jogosult panaszt benyújtani, amennyiben úgy ítéli meg, hogy a rá vonatkozó személyes adatok kezelése megsérti a GDPR-t.

Az érintett a felügyeleti hatóság döntése ellen a felügyeleti hatóság székhelye szerin} tagállam bírósága előtt élhet bírósági jogorvoslati jogával mind az érintette, mind pedig az adatkezelő/adatfeldolgozó és megtámadhatja a döntést.

Az érintett jogosult közvetlenül a bírósághoz fordulni, amennyiben megítélése szerint a személyes adatainak, a Rendeletnek nem megfelelő kezelése következtében megsértették a Rendelt szerin} jogait. Az Infotv. rendelkezése szerint a hatáskörrel rendelkező bíróság az érintett lakhelye vagy tartózkodási helye szerin} törvényszék.

VI. Az adatkezelő részletszabályai az érintett jogainak érvényesítésére

1. Előzetes tájékozódáshoz való jog

Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
- az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
- a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- a Rendelet 6. cikk (1) bekezdésének f) pontján (jogos érdek érvényesítés) alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekei;
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- adott esetben annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a Rendelet 46. cikkben, a 47. cikkben vagy a 49. cikk
  (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az azok másolatának megszerzésére szolgáló módokra vagy az azok elérhetőségére való hivatkozás.

Az adatkezelő a személyes adatok megszerzésének időpontjában, annak érdekében, hogy a tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
- az érintett azon jogáról, 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;
- c) a Rendelet 6. cikk (1) bekezdésének a) pontján (az érintett hozzájárulása) vagy a 9. cikk (2) bekezdésének a) pontján (az érintett hozzájárulása) alapuló adatkezelés esetén a hozzájárulás

bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

- d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- e) 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;
- f) a Rendelet 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg:

Ha a személyes adatokat nem az érintettől szerezték meg, az adatkezelő az érintett rendelkezésére bocsátja a következő információkat:

- az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei;
- az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;
- a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- az érintett személyes adatok kategóriái;
- a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;
- adott esetben annak ténye, hogy az adatkezelő valamely harmadik országbeli címzett vagy valamely nemzetközi szervezet részére kívánja továbbítani a személyes adatokat, továbbá a Bizottság megfelelőségi határozatának léte vagy annak hiánya, vagy a Rendelet 46. cikkben, a 47. cikkben vagy a 49. cikk (1) bekezdésének második albekezdésében említett adattovábbítás esetén a megfelelő és alkalmas garanciák megjelölése, valamint az ezek másolatának megszerzésére szolgáló módokra vagy az elérhetőségükre való hivatkozás.

Az adatkezelő az érintett rendelkezésére bocsátja az érintettre nézve tisztességes és átlátható adatkezelés biztosításához szükséges következő kiegészítő információkat:

1. a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
2. ha az adatkezelés a Rendelet 6. cikk (1) bekezdésének f) pontján (jogos érdek) alapul, az adatkezelő vagy harmadik fél jogos érdekeiről;
3. az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat a személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való joga;
4. d) a Rendelet 6. cikk (1) bekezdésének a) pontján (az érintett hozzájárulása) vagy a 9. cikk (2) bekezdésének a) pontján (az érintett hozzájárulása) alapuló adatkezelés esetén a hozzájárulás bármely időpontban való visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;

E. a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;

6. a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak–e; és
7. a Rendelet 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Az adatkezelő a tájékoztatást az alábbiak szerint adja meg:

1. a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított ésszerű határidőn, de legkésőbb egy hónapon belül;
2. ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy
3. ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.

Ha az adatkezelő a személyes adatokon a megszerzésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

Az 1-5. pontot nem kell alkalmazni, ha és amilyen mértékben:

1. az érintett már rendelkezik az információkkal;
2. a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, a Rendelet 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett adatkezelés esetében, vagy amennyiben az e cikk (1) bekezdésében említett kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;
3. az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy
4. a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia.

2. Az érintett hozzáférési joga

Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

1. az adatkezelés céljai;
2. az érintett személyes adatok kategóriái;
3. azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket, illetve a nemzetközi szervezeteket;
4. adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

E. az érintett azon joga, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen;

6. a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;
7. ha az adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
8. a Rendelet 22. cikk (1) és (4) bekezdésében említett automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel bír, és az érintettre nézve milyen várható következményekkel jár.

Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a Rendelet 46. cikk szerin} megfelelő garanciákról.

Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az Adatkezelő az adminisztratív költségeken alapuló, észszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait.

3. A törléshez való jog („az elfeledtetéshez való jog”)

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha az alábbi indokok valamelyike fennáll:

1. a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
2. az érintett visszavonja a Rendelet 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja értelmében az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
3. az érintett a Rendelet 21. cikk (1) bekezdése alapján tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy az érintett a 21. cikk (2) bekezdése alapján tiltakozik az adatkezelés ellen;
4. a személyes adatokat jogellenesen kezelték;

E. a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

6. a személyes adatok gyűjtésére a Rendelet 8. cikk (1) bekezdésében említett, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az előbbi 1. pont értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az ésszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő Adatkezelőket, hogy az érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

Az 1. és 2. pont nem alkalmazandó, amennyiben az adatkezelés szükséges:

1. a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;
2. a személyes adatok kezelését előíró, az Adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
3. a Rendelet 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;
4. a Rendelet 89. cikk (1) bekezdésével összhangban a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben az 1. pontban említett jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést; vagy

E. jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

4. Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

1. az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;
2. az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
3. az Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
4. az érintett a Rendelet 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek–e az érintett jogos indokaival szemben.

Ha az adatkezelés az 1. pont alapján korlátozás alá esik, az ilyen személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes vagy jogi személy jogainak védelme érdekében, vagy az Unió, illetve valamely tagállam fontos közérdekéből lehet kezelni.

Az Adatkezelő az érintettet, akinek a kérésére az 1. pont alapján korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

5. Az adathordozhatósághoz való jog

1. Az érintett jogosult arra, hogy a rá vonatkozó, általa egy 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, ha:
   1. az adatkezelés a Rendelet 6. cikk (1) bekezdésének a) pontja vagy a 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul; és
   2. az adatkezelés automatizált módon történik.

Az adatok hordozhatóságához való jog 1. pont szerin} gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok Adatkezelők között közvetlen továbbítását.

E jog gyakorlása nem sértheti a Rendelet 17. cikkét. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

Az 1. pontban említett jog nem érintheti hátrányosan mások jogait és szabadságait.

6. A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a Rendelet 6. cikk (1) bekezdésének

1. e) pontján (az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges) vagy
2. f) pontján (az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges) alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is.

Ebben az esetben az Adatkezelő a személyes adatokat nem kezelheti tovább, 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.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik.

A – gyakorlatban leginkább direkt marketingként hivatkozott – közvetlen üzletszerzés érdekében történő adatkezelésről a GDPR is elismeri, hogy az ehhez kapcsolódó adatkezelések esetében a jogos érdek fennállását lehet vélelmezni.

Az Érintett a Társaság által folytatott direkt marketing tevékenységek esetén tehát szintén jogosult tiltakozni személyes adatainak ebből célból történő kezelése ellen, az egyéb jogos érdeken alapuló adatkezeléssel ellentétben azonban a tiltakozás nyomán a Társaságnak nem áll módjában mérlegelni, hogy az Érintett tiltakozása esetén mégis folytathatja-e az adatkezelést.

Amennyiben az Érintett a direkt marketing célból történő adatkezelés ellen tiltakozik, úgy a továbbiakban az Érintett adatait a Társaság ebből a célból tovább nem kezelheti.

Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

Az 1. és 2. pontokban említett jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

Az információs társadalommal összefüggő szolgáltatások igénybevételéhez kapcsolódóan és a 2002/58/EK irányelvtől eltérve az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

Ha a személyes adatok kezelésére a Rendelet 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség.

7. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Az 1. pont nem alkalmazandó abban az esetben, ha a döntés:
1. az érintett és az Adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;
2. meghozatalát az Adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
3. az érintett kifejezett hozzájárulásán alapul.

A 2. pontban említett esetekben az Adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az Adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

A 2. pontban említett döntések nem alapulhatnak a személyes adatoknak a Rendelet 9. cikk (1) bekezdésében említett különleges kategóriáin, kivéve, ha a 9. cikk (2) bekezdésének a) vagy g) pontja alkalmazandó, és az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében megfelelő intézkedések megtételére került sor.

8. Korlátozások

Az Adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a Rendelet 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok

és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban:

1. nemzetbiztonság;
2. honvédelem;
3. közbiztonság;
4. bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;
E. az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot;
6. a bírói függetlenség és a bírósági eljárások védelme;
7. a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;
8. az a)–e) és a g) pontban említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység;
9. az érintett védelme vagy mások jogainak és szabadságainak védelme;
10. polgári jogi követelések érvényesítése.

Az 1. pontban említett jogalkotási intézkedések adott esetben részletes rendelkezéseket tartalmaznak legalább:

1. az adatkezelés céljaira vagy az adatkezelés kategóriáira,
2. a személyes adatok kategóriáira,
3. a bevezetett korlátozások hatályára,
4. a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciákra,
E. az Adatkezelő meghatározására vagy az Adatkezelők kategóriáinak meghatározására,
6. az adattárolás időtartamára, valamint az alkalmazandó garanciákra, figyelembe véve az adatkezelés vagy az adatkezelési kategóriák jellegét, hatályát és céljait,
7. az érintettek jogait és szabadságait érintő kockázatokra, és
8. az érintettek arra vonatkozó jogára, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját.

9. Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a Rendelet 33. cikk (3) bekezdésének b), c) és d) pontjában említett információkat és intézkedéseket.

Az érintettet nem kell az 1. pontban említettek szerint tájékoztatni, ha a következő feltételek bármelyike teljesül:

1. az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
2. az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az 1. pontban említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

3. a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha az Adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja a 3. pontban említett feltételek valamelyikének teljesülését.

10. A felügyeleti hatóságnál történő panasztételhez való jog

Az egyéb közigazgatási vagy bírósági jogorvoslatok sérelme nélkül, minden érintett jogosult arra, hogy panaszt tegyen egy felügyeleti hatóságnál – különösen a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerin} tagállamban –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.

Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy a Rendelet 78. cikk alapján az ügyfél jogosult bírósági jogorvoslattal élni.

6.11 A felügyeleti hatósággal szembeni hatékony bírósági jogorvoslathoz való jog

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

Az egyéb közigazgatási vagy nem bírósági útra tartozó jogorvoslatok sérelme nélkül, minden érintett jogosult a hatékony bírósági jogorvoslatra, ha a Rendelet 55. vagy 56. cikk alapján illetékes felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a 77. cikk alapján benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerin} tagállam bírósága előtt kell megindítani.

Ha a felügyeleti hatóság olyan döntése ellen indítanak eljárást, amellyel kapcsolatban az egységességi mechanizmus keretében a Testület előzőleg véleményt bocsátott ki vagy döntést hozott, a felügyeleti hatóság köteles ezt a véleményt vagy döntést a bíróságnak megküldeni.

6.12. Az adatkezelővel vagy az adatfeldolgozóval szembeni hatékony bírósági jogorvoslathoz való jog

A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a felügyeleti hatóságnál történő panasztételhez való, Rendelet 77. cikk szerin} jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak, e rendeletnek nem megfelelő kezelése következtében megsértették az e rendelet szerin} jogait.

Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerin} tagállam bírósága előtt kell megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerin} tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

VII. ELJÁRÁSI SZABÁLYOK az érintett vonatkozásában

A Társaság indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintetett a GDPR 15–22. cikk szerinti kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

A határidő meghosszabbításáról a Társaság a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmét, a tájékoztatást elektronikus úton kerül megadásra, kivéve, ha az érintett azt másként kéri.

Ha 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, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeletei hatóságnál és élhet bírósági jogorvoslati jogával.

A Társaság a kért információkat és tájékoztatást díjmentesen biztosítja. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt– túlzó, a Társaság, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre ésszerű mértékű díjat számolhat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.

A Társaság minden olyan címzettet tájékoztat az általa végzett valamennyi helyesbítésről, törlésről, vagy adatkezelési–korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére a Társaság tájékoztatja e címzettekről.

A Társaság az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért a Társaság az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. H az érintett elektronikus úton nyújtotta be a kérelmét, az információk elektronikus formátumban kerülnek rendelkezésre bocsátásra megsértése kivéve, ha az érintett másként kéri.

Az érintett a kérelmét bármely ügyfélszolgálati munkakörben foglalkoztatott munkatársnál be nyújthatja, de elbírálása az ügyvezető feladatkörébe tartozik.

A kérelem benyújtása írásban történhet elektronikus levél útján vagy papír alapon. Ha az Érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az Érintett azt másként kéri.

Az Érintett köteles a kérelemben megjelölni, hogy a mely személyes adat vonatkozásában kéri a Társaság intézkedését.

A Társaság az írásban benyújtott kérelem kézhezvételétől számított 1 (egy) hónapon belül köteles a kérelmet elbírálni. Szükség esetén, figyelembe véve a kérelem összetettségét, illetve a folyamatban lévő kérelmek számát, a Társaság a kérelem elbírálásának határidejét további 2 (kettő) hónappal meghosszabbíthatja. A meghosszabbítás tényéről, illetve a késedelem okairól az Érintettet a kérelem kézhezvételétől számított 1 (egy) hónapon belül tájékoztatni kell.

Amennyiben az Érintett kérelme megalapozott, a Társaság a kért intézkedést az eljárási határidőn belül végrehajtja, és a végrehajtás megtörténtével kapcsolatosan írásbeli tájékoztatást ad az Érintett részére.

Ha a Társaság az Érintett kérelmét elutasítja, köteles erről írásbeli határozatot hozni és arról késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 1 (egy) hónapon belül az Érintettet tájékoztatni.

Határozatában köteles megjelölni a döntés alapjául szolgáló tényállást, döntésének indoklását a megfelelő jogszabályok, illetve eseti döntések bemutatásával, továbbá köteles az Érintettet arról tájékoztatni, hogy a Társaság döntésével szemben panaszt nyújthat be valamely felügyeleti hatóságnál és élhet bírósági jogorvoslati jogával.

A Társaság a GDPR 13–14. cikke szerinti információkat, a GDPR 15–22. cikke szerinti érintetti jogokkal kapcsolatos tájékoztatást, továbbá a GDPR 34. cikke esetén az adatvédelmi incidenssel kapcsolatos tájékoztatást, illetve a kérelmezett intézkedéseket díjmentesen biztosítja. Amennyiben azonban az Érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a Társaság, figyelemmel a kért információ, vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre

1. észszerű összegű díjat számíthat fel, vagy
2. megtagadhatja a kérelem alapján történő intézkedést.

Az érintett költségek megtérítésére kizárólag abban az esetben kötelezhető, amennyiben a Társaság az Érintettet a kérelme beérkezését követő 15 napon belül írásban tájékoztatta arról a körülményről, hogy kérelme megalapozatlan vagy túlzó jellegű, és ezzel egyidejűleg tájékoztatta az adminisztratív költség mértékéről, de az Érintett mindezen körülmények ellenére az igényét írásban fenntartotta. Az igény fenntartásának minősül, ha az érintett a Társaság tájékoztatása ellenére nem vonja vissza kérelmét 5 munkanapon belül vagy az ügyintézési határidő végéig.

A költségek viselésére kötelezett érintett a költséget vagy külön köteles megfizetni a Társaság által kibocsátott fizetési felszólítás kézhezvételétől számított 8 napon belül.

Abban az esetben, amennyiben a Társaságnak a kérelem előterjesztőjének kilétével kapcsolatban megalapozott kétsége támad, a Társaság az érintett személyazonosságának megerősítéséhez szükséges további információk rendelkezésre bocsátását igényelheti.

Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.

Ha 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, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.

Társaságunk, mint Társaság a Rendelet 13. és 14. cikk szerinti információkat és az érintett jogairól szóló tájékoztatást (Rendelt 15–22. és 34. cikk) és intézkedést díjmentesen biztosítja. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, a Társaság, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre:

1. 3.350,– Ft összegű díjat számíthat fel, vagy
2. megtagadhatja a kérelem alapján történő intézkedést.

A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása a Társaságot terheli.

Ha Társaságunknak, mint Társaságnak megalapozott kétségei vannak a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, az érintett személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

A Társaság az ügyfélmegkeresések tényéről, időpontjáról, tartalmáról, elbírálásáról és a következményeiről nyilvántartást vezet, melynek megőrzéséről 5 évig gondoskodik. A Társaság adatvédelmi tevékenységének további javítása érdekében az ügyfélmegkereséseket és az esetleges hatósági megkereséseket elemzi, levonja a megfelelő következményeket, és ennek eredményéről évente – a személyes adatok kivételével – a Társaság dolgozóinak feljegyzést készít.

VIII. A TÁRSASÁG ADATKEZELÉSEI ÉS ADATTOVÁBBÍTÁSAI

A személyes adatok kezelése általánosságban (jogalaptól függetlenül) akkor jogszerű, ha a Társaság az adatkezelés megkezdése előtt:

- meghatározza az adatkezelés céljait és az egyes célokhoz szükséges minimális személyes adatot, és
- minden egyes céllal kapcsolatban meghatározza, hogy a GDPR 6. cikkében felsorolt jogalapok közül melyikre hivatkozással kezeli a személyes adatokat az egyes célokból, és
- megfelelő adatvédelmi tájékoztatót készít és tesz elérhetővé az érintettek számára figyelemmel a választott jogalapok esetleges többlet feltételeire, és
- meghatározza, hogy az adatokhoz ki és milyen módon férhet hozzá, védve a személyes adatokat a jogosulatlan hozzáférés ellen, és
- a fenti lépéseket megfelelően dokumentálja, hogy utólagosan bizonyítható legyen (elszámoltathatóság).

8.1. Adatkezelés az érintett hozzájárulása alapján

A hozzájáruláson alapuló adatkezelés esetén az érintett hozzájárulását személyes adatai kezeléséhez adatkérő lapon vagy online felületen hozzájárulás kérő lapon kell kérni.

Hozzájárulásnak minősül az is, ha az érintett a Társaság internetes honlapjának megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak.

A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni.

Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik – így az értékesítési, szolgáltatási szerződés megkötése- a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti a Rendeletet, kötelező erővel nem bír.

A Társaság nem kötheti szerződés megkötését, teljesítését olyan személyes adatok kezeléséhez való hozzájárulás megadásához, amelyek nem szükségesek a szerződés teljesítéséhez.

A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Ha a személyes adat felvételére az érintett hozzájárulásával került sor, a Társaság a felvett adatokat törvény eltérő rendelkezésének hiányában a rá vonatkozó jogi kötelezettség teljesítése céljából további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

A Társaság az Adatkezelési Tájékoztatóját a honlapján a láblécben elérhetővé teszi az érintettek számára.

Az Adatkezelési Tájékoztató célja, hogy az érintetteket nyilvánosan is elérhető formában az adatkezelés megkezdése előtt és annak folyamán is egyértelműen és részletesen tájékoztassa az adataik kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait a Társaság az Infotv. 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat.

A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Ezen adatkezelési tájékoztatót a legfontosabb adatkezelési lépések mindegyikénél külön linkkel jelölve megismerhetővé kell tenni (például egy regisztráció esetében a regisztráció előtt, a regisztráció folyamatánál stb.). E tájékoztató elérhetőségéről az érintetteket tájékoztatni kell.

A jogi kötelezettség teljesítése jogcímén alapuló adatkezelés az érintett hozzájárulásától független, mivel az adatkezelést törvény határozta meg.

Az érintettel az adatkezelés megkezdése előtt ez esetben közölni kell, hogy az adatkezelés kötelező, továbbá az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen:

1. az adatkezelés céljáról és jogalapjáról,
2. az adatkezelésre és az adatfeldolgozásra jogosult személyéről,
3. az adatkezelés időtartamáról,
4. arról, ha az érintett személyes adatait a Társaság a rá vonatkozó jogi kötelezettség alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat.

A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatkezelés esetén a tájékoztatás megtörténhet az előbbi információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

A Társaság kizárólag akkor kezelhet különleges adatokat, ha fennáll az alábbi feltételek egyike:

1. megkapta az érintett magánszemély kifejezett hozzájárulását;
2. uniós vagy magyar jog, vagy kollektív megállapodás értelmében a Társaságnak kötelessége az adatkezelés elvégzése;
3. az adatkezelés az érintett személy létfontosságú érdekeinek a védelme miatt szükséges, vagy az érintett személy fizikailag vagy jogilag képtelen a hozzájárulás megadására,
4. az adatkezelés olyan személyes adatokra vonatkozik, amelyet az érintett személy kifejezetten nyilvánosságra hozott;

E. az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges;

6. az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy magyar jog alapján;
7. az adatkezelés a következő célokból történik: megelőző egészségügyi vagy munkaegészségügyi cél, munkavállaló munkavégzésének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy magyar jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében;
8. az adatkezelés a népegészségügy területét érintő közérdekből szükséges, uniós vagy magyar jog alapján;
9. a Társaság valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet, az adatkezelés pedig az ilyen szerv jelenlegi vagy volt tagjaira, vagy a szervezettel rendszeres kapcsolatban álló személyekre vonatkozik;

10. az adatkezelés archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges uniós vagy magyar jog alapján.

A Társaság csak akkor kezeli egy gyermek személyes adatait, ha rendelkezik a gyermek törvényes képviselőjének a kifejezett írásbeli hozzájárulásával.

8.1.1. Adatkezelés a Társaság közösségi oldalán

A Társaság termékei, szolgáltatásai megismertetése, népszerűsítése céljából Facebook oldalt tart fenn.

A Társaság Facebook oldalon felett kérdés nem minősül hivatalosan benyújtott panasznak.

A Társaság Facebook oldalán a látogatók által közzétett személyes adatokat a Társaság nem kezeli. A

látogatókra a Facebook Adatvédelmi- és Szolgáltatási Feltételei irányadók.

Jogellenes, vagy sértő tartalom publikálása esetén a Társaság előzetes értesítés nélkül kizárhatja az érintettet a tagok közül, vagy törölheti hozzászólását.

A Társaság nem felel a Facebook felhasználók által közzétett jogszabályt sértő adattartalmakért, hozzászólásokért. A Társaság nem felel semmilyen, a Facebook működéséből adódó hibáért, üzemzavarért vagy a rendszer működésének megváltoztatásából fakadó problémáért.

A Társaság Facebook oldalán az oldallal kapcsolatos Adatvédelmi Tájékoztatót helyez el.

8.1.2. Hírlevél szolgáltatáshoz kapcsolódó adatkezelés

A honlapon vagy az ügyfélszolgálaton a hírlevél szolgáltatásra regisztráló természetes személy az erre vonatkozó négyzet bejelölésével adhatja meg hozzájárulását személyes adatai kezeléséhez. Tilos a négyzet előre bejelölése. A feliratkozás során a honlapon az Adatkezelési tájékoztatót egy linkkel elérhetővé kell tenni, ügyfélszolgálaton az Adatvédelmi Tájékoztató kinyomtatva és összefűzve az ügyfelek rendelkezésére áll. A hírlevéről az érintett a hírlevél „Leiratkozás” alkalmazásának használatával, vagy írásban vagy e-mailben tett nyilatkozattal bármikor leiratkozhat, amely a hozzájárulás visszavonását jelen}. Ilyen esetben a leiratkozó minden adatát haladéktalanul törölni kell. A kezelhető személyes adatok köre: a természetes személy neve (vezetéknév, keresztnév), e-mail címe.

A személyes adatok kezelésének célja:

1. Hírlevél küldése a Társaság termékei, szolgáltatásai tárgyában
2. Reklámanyag küldése

Az adatkezelés jogalapja: az érintett hozzájárulása.

A személyes adatok címzettjei, illetve a címzettek kategóriái: a Társaság ügyfélszolgálattal, marketing tevékenységével kapcsolatos feladatokat ellátó munkavállalói, adatfeldolgozóként a Társaság IT szolgáltatója munkavállalói a tárhely szolgáltatás teljesítése céljából,

A személyes adatok tárolásának időtartama: a hírlevél-szolgáltatás fennállásáig, vagy az érintett hozzájárulása visszavonásáig (törlési kérelméig).

A hozzájárulás megadásáról és a törlési kérelmekről a Társaság nyilvántartást vezet. Ugyancsak nyilvántartást vezet a tiltakozó ügyfélmegkeresésekről a 1995. évi CXIX tv. 21§ (1). értelmében tiltakozó listát (Robinson listát vezet).

8.1.3. Ajándéksorsolás és nyereményjátékok szervezésével kapcsolatos adatkezelés

Ha a társaság ajándéksorsolást (1991. évi XXXIV. törvény 23.§) szervez, hozzájárulása alapján kezelheti az érintett természetes személy nevét, címét, telefonszámát, e-mail címét, online azonosítóját. A játékban való részvétel önkéntes. A személyes adatok kezelésének célja: nyereményjáték nyertesének megállapítása, értesítése, a nyeremény megküldése. Az adatkezelés jogalapja: az érintett hozzájárulása.

A személyes adatok címzettjei, illetve a címzettek kategóriái: az ajándéksorsolást felügyelő közjegyző. A személyes adatok tárolásának időtartama: az ajándéksorolás végelszámolásától számított 5 év.

8.1.4. Direkt marketing célú adatkezelés

Ha külön törvény eltérően nem rendelkezik, reklám természetes személynek, mint reklám címzettjének közvetlen megkeresése módszerével (közvetlen üzletszerzés), így különösen elektronikus levelezés vagy azzal egyenértékű más egyéni kommunikációs eszköz útján - a 2008. évi XLVIII. törvényben meghatározott kivétellel - kizárólag akkor közölhető, ha ahhoz a reklám címzettje előzetesen egyértelműen és kifejezetten hozzájárult.

A Társaság által reklám-címzett megkeresés céljára kezelhető személyes adatok köre: a természetes személy neve, címe, telefonszáma, e-mail címe, online azonosító.

A személyes adatok kezelésének célja a Társaság tevékenységéhez kapcsolódó direkt marketing tevékenység folytatása, azaz reklámkiadványok, hírlevelek, aktuális ajánlatok nyomtatott (postai) vagy elektronikus formában (e-mail) történő rendszeres vagy időszakonként megküldése a regisztrációkor megadott elérhetőségekre.

Az adatkezelés jogalapja: az érintett hozzájárulása.

A személyes adatok címzettjei, illetve a címzettek kategóriái: a Társaság ügyfélszolgálattal kapcsolatos feladatokat ellátó munkavállalói, adatfeldolgozóként a Társaság IT szolgáltatója szerverszolgáltatást végző munkavállalói, postai kézbesítés esetén a Posta munkavállalói.

A személyes adatok tárolásának időtartama: a hozzájárulás visszavonásáig.

A hozzájárulás megadásáról és a törlési kérelmekről a Társaság nyilvántartást vezet. Ugyancsak nyilvántartást vezet a tiltakozó ügyfélmegkeresésekről a 1995. évi CXIX tv. 21§ (1). értelmében tiltakozó listát (Robinson listát vezet).

8.2. Munkaviszonnyal kapcsolatos adatkezelések

8.2.1. Munkaügyi, személyzeti nyilvántartás

A munkavállalóktól kizárólag olyan adatok kérhetők és tarthatók nyilván, valamint olyan munkaköri orvosi alkalmassági vizsgálatok végezhetők, amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez, illetve a szociális-jóléti juttatások biztosításához szükségesek és a munkavállaló személyhez fűződő jogait nem sértik.

A Társaság munkáltatói jogos érdekeinek érvényesítése (Rendelet 6. cikk (1) bekezdése f)) jogcímén munkaviszony létesítése, teljesítése vagy megszűnése céljából kezeli a munkavállaló alábbi adatait:

1. név
2. születési név,
3. születési ideje,
4. anyja neve,
E. lakcíme,
6. állampolgársága,
7. adóazonosító jele,
8. TAJ száma,
9. nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
10. telefonszám,
11. e–mail cím,
12. személyi igazolvány száma,
13. lakcímet igazoló hatósági igazolvány száma,
14. bankszámlaszáma,

1E. online azonosító (ha van)
16. munkába lépésének kezdő és befejező időpontja,
17. munkakör,
18. iskolai végzettségét, szakképzettségét igazoló okmány másolata,
19. fénykép,
20. önéletrajz,
21. munkabérének összege, a bérfizetéssel, egyéb juttatásaival kapcsolatos adatok,
22. a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozást, illetve ennek jogosultságát,
23. a munkavállaló munkájának értékelése,
24. a munkaviszony megszűnésének módja, indokai,
2E. munkakörtől függően erkölcsi bizonyítványa
26. a munkaköri alkalmassági vizsgálatok összegzése,
27. magánnyugdíj pénztári és önkéntes kölcsönös biztosító pénztári tagság esetén a pénztár megnevezése, azonosító száma és a munkavállaló tagsági száma,
28. külföldi munkavállaló esetén útlevélszám; munkavállalási jogosultságot igazoló dokumentumának megnevezését és száma,
29. munkavállalót ért balesetek jegyzőkönyveiben rögzített adatokat;
29. a jóléti szolgáltatás, kereskedelmi szálláshely igénybevételéhez szükséges adatokat;
30. a Társaságnál biztonsági és vagyonvédelmi célból alkalmazott kamera és beléptető rendszer, illetve a helymeghatározó rendszerek által rögzített adatokat.

Betegségre és szakszervezeti} tagságára vonatkozó adatokat a munkáltató csak a Munka Törvénykönyvben meghatározott jog, vagy kötelezettség teljesítése céljából kezel.

A személyes adatok címzettjei: a munkáltató vezetője, munkáltatói jogkör gyakorlója, a Társaság munkaügyi feladatokat ellátó munkavállalói és adatfeldolgozói.

A Társaság tulajdonosai részére csak a vezető állású munkavállalók személyes adatai továbbíthatók.

A személyes adatok tárolásának időtartama: a munkaviszony megszűnését követő 3 év.

Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a Munka törvénykönyvén és a munkáltató jogos érdekeinek érvényesítésén alapul

A munkáltató a munkaszerződés megkötésével egyidejűleg Tájékoztató átadásával tájékoztatja a munkavállalót személyes adatainak kezeléséről és személyhez fűződő jogokról.

8.2.2. Alkalmassági vizsgálatokkal kapcsolatos adatkezelés

A munkavállalóval szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges. A vizsgálat előtt részletesen tájékoztatni kell a munkavállalókat többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabály címéről és a pontos jogszabályhelyről is

A munkaalkalmasságra, felkészültségre irányuló tesztlapok a munkáltató mind a munkaviszony létesítése előtt, mind pedig a munkaviszony fennállása alatt kitöltetheti a munkavállalókkal.

Az egyértelműen munkaviszonnyal kapcsolatos, a munkafolyamatok hatékonyabb ellátása, megszervezése érdekében csak akkor tölthető ki a munkavállalók nagyobb csoportjával pszichológiai, vagy személyiségjegyek kutatására alkalmas tesztlap, ha az elemzés során felszínre került adatok nem köthetők az egyes konkrét munkavállalókhoz, vagyis anonim módon történik az adatok feldolgozása.

A kezelhető személyes adatok köre: a munkaköri alkalmasság ténye, és az ehhez szükséges feltételek.

Az adatkezelés jogalapja: a munkáltató jogos érdeke.

A személyes adatok kezelésének célja: munkaviszony létesítése, fenntartása, munkakör betöltése.

A személyes adatok címzettjei, illetve a címzettek kategóriái: A vizsgálat eredményt a vizsgált munkavállalók, illetve a vizsgálatot végző szakember ismerhetik meg. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját azonban a munkáltató nem ismerheti meg.

A személyes adatok kezelésének időtartama: a munkaviszony megszűnését követően az abból eredő jogi igények elévüléséig.

8.2.3.Felvételre jelentkező munkavállalók adatainak kezelése, pályázatok, önéletrajzok

A kezelhető személyes adatok köre: a természetes személy neve, születési ideje, helye, anyja neve, lakcím, képesítési adatok, fénykép, telefonszám, e-mail cím, a jelentkezőről készített munkáltatói feljegyzés (ha van).

A személyes adatok kezelésének célja: jelentkezés, pályázat elbírálása, a kiválasztottal munkaszerződés kötése. Az érintettet tájékoztatni kell arról, ha a munkáltató nem őt választotta az adott állásra.

Az adatkezelés jogalapja: az érintett hozzájárulása és az adatkezelő jogos érdeke.

A személyes adatok címzettjei, illetve a címzettek kategóriái: a Társaságnál munkáltatói jogok gyakorlására jogosult vezető, munkaügyi feladatokat ellátó munkavállalók.

A személyes adatok tárolásának időtartama: A jelentkezés, pályázat elbírálásáig. A ki nem választott jelentkezők személyes adatait törölni kell. Törölni kell annak adatait is, aki jelentkezését, pályázatát visszavonta.

A munkáltató csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a pályázatokat, feltéve, ha azok megőrzésére a jogszabályokkal összhangban álló adatkezelési célja elérése érdekében szükség van, maximum az eredményes pályázó próbaidejének végéig, de legfeljebb 0 napig.

8.2.4. E–mail fiók használatának ellenőrzésével kapcsolatos adatkezelés

Ha a Társaság e-mail fiókot bocsát a munkavállaló rendelkezésére – ezen e-mail címet és fiókot a munkavállaló kizárólag munkaköri feladatai céljára használhatja, annak érdekében, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel.

A munkavállaló az e-mail fiókot személyes célra nem használhatja, a fiókban személyes leveleket nem tárolhat.

A munkáltató jogosult az e-mail fiók teljes tartalmát és használatát rendszeresen – 3 havonta-ellenőrizni, ennek során az adatkezelés jogalapja a munkáltató jogos érdeke. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a munkavállalói kötelezettségek (Mt. 8.§, 52. §) ellenőrzése.

Az ellenőrzésre a munkáltató vezetője, vagy a munkáltatói jogok gyakorlója jogosult.

Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során.

Az ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor

ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés során a fokozatosság elvét kell alkalmazni, így elsődlegesen az e-mail címéből és tárgyából kell megállapítani, hogy az a munkavállaló munkaköri feladatával kapcsolatos, és nem személyes célú. Nem személyes célú e-mailek tartalmát a munkáltató korlátozás nélkül vizsgálhatja.

Ha jelen szabályzat rendelkezéseivel ellentétben az állapítható meg, hogy a munkavállaló az e-mail fiókot személyes célra használta, fel kell szólítani a munkavállalót, hogy a személyes adatokat haladéktalanul törölje. A munkavállaló távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli. Az e-mail fiók jelen szabályzattal ellentétes használata miatt a munkáltató a munkavállalóval szemben munkajogi jogkövetkezményeket alkalmazhat.

A munkavállaló az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban e szabályzatnak az érintett jogairól szóló fejezetében írt jogokkal élhet.

8.2.E.Számítógép, laptop, tablet ellenőrzésével kapcsolatos adatkezelés

A Társaság által a munkavállaló részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot, tabletet a munkavállaló kizárólag munkaköri feladata ellátására használhatja, ezek magáncélú használatát a Társaság megtiltja, ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezését nem kezelheti, és nem tárolhatja. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti. Ezen eszközök munkáltató általi ellenőrzésére és jogkövetkezményire egyebekben az előbbi pont rendelkezései irányadók.

6. A munkahelyi internethasználat ellenőrzésével kapcsolatos adatkezelés

A munkavállaló csak a munkaköri feladatával kapcsolatos honlapokat tekintheti meg, a személyes célú munkahelyi internet használatot a munkáltató megtiltja.

A munkaköri feladatként a Társaság nevében elvégzett internetes regisztrációk jogosultja a Társaság, a regisztráció során a társaságra utaló azonosítót, jelszót kell alkalmazni. Amennyiben a személyes adatok megadása is szükséges a regisztrációhoz, a munkaviszony megszűnésekor azok törlését köteles kezdeményezni a Társaság.

7. Céges mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

A munkáltató nem engedélyezi a céges mobiltelefon magáncélú használatát, a mobiltelefon csak munkavégzéssel összefüggő célokra használható, és a munkáltató valamennyi kimenő hívás hívószámát és adatait, továbbá a mobiltelefonon tárolt adatokat ellenőrizheti.

A munkavállaló köteles bejelenteni a munkáltatónak, ha a céges mobiltelefont magáncélra használta. Ebben az esetben az ellenőrzés akként folytatható le, hogy a munkáltató hívásrészletezőt kér a telefonszolgáltatótól és felhívja a munkavállalót arra, hogy a dokumentumon a magáncélú hívások esetében a hívott számokat tegye felismerhetetlenné. A munkáltató előírhatja, hogy a magáncélú hívások költségeit a munkavállaló viselje.

8.3.Szerződéshez kapcsolódó adatkezelések

8.3.1. Szerződő partnerek adatainak kezelése – vevők, szállítók nyilvántartása

A Társaság szerződés teljesítése jogcímén a szerződés megkötése, teljesítése, megszűnése, szerződési kedvezmény nyújtása céljából kezeli a vele vevőként, szállítóként szerződött természetes személy:

- nevét, születési nevét, születési idejét, anyja nevét, lakcímét, adóazonosító jelét, adószámát, vállalkozói, őstermelői igazolvány számát, személyi igazolvány számát, lakcímét, székhely, telephely címét,

telefonszámát, e-mail címét, honlap-címét, bankszámlaszámát, vevőszámát (ügyfélszámát, rendelésszámát), online azonosítóját (vevők, szállítók listája, törzsvásárlási listák),

Ezen adatkezelés jogszerűnek minősül akkor is, ha az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

A személyes adatok címzettjei: a Társaság ügyfélkiszolgálással kapcsolatos feladatokat ellátó munkavállalói, könyvelési, adózási feladatokat ellátó munkavállalói, és adatfeldolgozói.

A személyes adatok tárolásának időtartama: a szerződés megszűnését követő 5 év.

Az érintett természetes személlyel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a szerződés teljesítése jogcímén alapul, az a tájékoztatás történhet a szerződésben is. Az érintettet személyes adatai adatfeldolgozó részére történő átadásáról tájékoztatni kell.

8.3.2. Jogi személy ügyfelek, vevők, szállítók természetes személy képviselőinek elérhetőségi adatai

A kezelhető személyes adatok köre: a természetes személy neve, címe, telefonszáma, e-mail címe, online azonosítója.

A személyes adatok kezelésének célja: a Társaság jogi személy partnerével kötött szerződés teljesítése, üzleti kapcsolattartás, jogalapja: az adatkezelő jogos érdeke.

A személyes adatok címzettjei, illetve a címzettek kategóriái: a Társaság ügyfélszolgálattal kapcsolatos feladatokat ellátó munkavállalói.

A személyes adatok tárolásának időtartama: az üzleti kapcsolat, illetve az érintett képviselői minőségének fennállását követő 5 évig.

Amennyiben a személyes adat a nem természetes személy szerződő partnerünk (partner jogi személy) munkavállalójáé (kapcsolattartó), akkor a személyes adatokat a szerződéses partner továbbítja a Társaságunk felé a kapcsolattartáshoz szükséges mértékben. Ilyenkor a szerződéses partnerünk, mint munkáltató a GDPR. 6. cikk (1) bekezdése és a munka törvénykönyvéről szóló 2012, évi I. törvény 10.§ (1) bekezdése alapján szerzi meg és kezeli a személyes adatokat, míg a Társaságunk a GDPR 6. cikk (1) bekezdés (f) pontja szerint vesszük át és kezeljük a személyes adatokat a célhoz szükséges mértékben és ideig.

8.3.3. Látogatói adatkezelés a Társaság honlapján – Tájékoztatás sütik (cookie) alkalmazásáról

A Sütik (cookie-k) rövid adatfájlok, melyeket a meglátogatott honlap helyez el a felhasználó számítógépén. A cookie célja, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolhatóak. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl.: egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Az Európai Bizottság irányelvei alapján cookie-kat [kivéve, ha azok az adott szolgáltatás használatához elengedhetetlenül szükségesek] csak a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni.

A felhasználó hozzájárulását nem igénylő sütik esetében a honlap első látogatása során kell tájékoztatást nyújtani. Nem szükséges, hogy a sütikre vonatkozó tájékoztató teljes szövege megjelenjen a honlapon, elegendő, ha a honlap üzemeltetői röviden összefoglalják a tájékoztatás lényegét, és egy linken keresztül utalnak a teljes körű tájékoztató elérhetőségére.

A hozzájárulást igénylő sütik esetében a tájékoztatás kapcsolódhat a honlap első látogatásához is abban az esetben, ha a sütik alkalmazásával együtt járó adatkezelés már az oldal felkeresésével megkezdődik. Amennyiben a süti alkalmazására a felhasználó által kifejezetten kért funkció igénybevételéhez kapcsolódik, akkor a tájékoztatás is megjelenhet e funkció igénybevételéhez kapcsolódóan. Ebben az

esetben sem szükséges az, hogy a sütikre vonatkozó tájékoztató teljes szövege megjelenjen a honlapon, elegendő egy rövid összefoglaló a tájékoztatás lényegéről, és egy linken keresztül utalás a teljes körű tájékoztató elérhetőségére.

A honlapon a sütik alkalmazásáról a látogatót adatkezelési tájékoztatóban tájékoztatni kell. E tájékoztatóval a Társaság biztosítja, hogy a látogató a honlap információs társadalommal összefüggő szolgáltatásainak igénybevétele előtt és az igénybevétel során bármikor megismerhesse, hogy a Társaság mely adatkezelési célokból mely adatfajtákat kezel, ideértve az igénybe vevővel közvetlenül kapcsolatba nem hozható adatok kezelését is.

8.4. Jogi kötelezettségen alapuló adatkezelések

8.4.1. Adatkezelés adó– és számviteli kötelezettségek teljesítése céljából

A Társaság jogi kötelezettség teljesítése jogcímén, törvényben előírt adó és számviteli kötelezettségek teljesítése (könyvelés, adózás) céljából kezeli a vevőként, szállítóként vele üzleti kapcsolatba lépő természetes személyek törvényben meghatározott adatait.

A kezelt adatok az általános forgalmi adóról szóló 2017. évi CXXVII. tv. 169.§, és 202.§-a alapján különösen: adószám, név, cím, adózási státusz, a számvitelről szóló 2000. évi C. törvény 167.§-a alapján:

- név, cím, a gazdasági műveletet elrendelő személy vagy szervezet megjelölése, az utalványozó és a rendelkezés végrehajtását igazoló személy, valamint a szervezettől függően az ellenőr aláírása; a készletmozgások bizonylatain és a pénzkezelési bizonylatokon az átvevő, az ellennyugtákon a befizető aláírása, a személyi jövedelemadóról szóló 1995. évi CXVII. törvény alapján: vállalkozói igazolvány száma, őstermelői igazolvány száma, adóazonosító jel.

A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 8 év.

A személyes adatok címzettjei: a Társaság adózási, könyvviteli, bérszámfejtési, társadalombiztosítási feladatait ellátó munkavállalói és adatfeldolgozói.

IX. ADATBIZONSÁGI INTÉZKEDÉSEK és ADATVÉDELMI INCIDENS

1. Adatbiztonsági intézkedések

A Társaság minden olyan dolgozójának, aki az adatvédelem szempontjából nevesített munkakört lát el, ez irányú feladatkörét a munkaköri leírásában meg kell jeleníteni.

Az adatkezelő szervezeti egység vezetője köteles gondoskodni a hatáskörében kezelt adatok biztonságáról, továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek jelen szabályzat szerint szükségesek az alábbiak alapján.

1.1. Informatikai biztonság

A Társaság adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve a Társaság belső szabályozásában hozzáférés–korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok).

1.2. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket. Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

A védelmi intézkedések kiterjednek: az alkalmazott hardver eszközökre és azok működési biztonságára, az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra, az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig, az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszerszoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára.

1.3. Védelmi eszközök

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

1.4. A védelem felelőse

A védelem felelőse a mindenkori informatikai vezető és rendszergazdák. A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Társaság vezetőinek kell gondoskodnia.

1.5. Felelősségi körök

Informatikai vezető feladatai:

- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására,
- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása, az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységét adminisztrálja,
- ellenőrzi a szoftverek használatának jogszerűségét.

Rendszergazda feladatai:

- a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli,
- felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok
- készítéséért és karbantartásáért,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
- feladata a védelmi eszközök működésének folyamatos ellenőrzése,
- felelős a Társaság informatikai rendszer hardver eszközeinek karbantartásáért,

- nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
- gondoskodik a folyamatos vírusvédelemről
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását,
- ellenőrzi a rendszer adminisztrációját.

1.6. Az informatikai vezető ellenőri feladatai

- évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását,
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságát,
- előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

1.7. Az informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Társaság vezetőjénél
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

2. Az informatikai biztonsági szabályzat alkalmazásának módja

Az informatikai biztonsági szabályzat megismerését az érintett dolgozók részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni. Az adatvédelmi és adatkezelési szabályzattal érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni a szabályzat előírásainak megfelelően.

2.1. Az informatikai biztonsági szabályzat karbantartása

A szabályzatot az informatikában – valamint a Társaságnál – a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az informatikai biztonsági belső szabályok folyamatos karbantartása az informatikai vezető feladata.

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik. Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell. Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető. A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a Társaság vezetőjének jelenteni kell. A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek. Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás – során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

2.2. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
- földrengés, árvíz, tűz, villámcsapás stb.
- környezeti kár:
- légszennyezettség, nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés, a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por),
- közüzemi szolgáltatásba bekövetkező zavarok,
- feszültség–kimaradás,
- feszültségingadozás,
- elektromos zárlat,
- csőtörés.

Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

1. behatolás az informatikai rendszerek környezetébe,
2. illetéktelen hozzáférés (adat, eszköz)
3. adatok– eszközök eltulajdonítása,
4. rongálás (gép, adathordozó),

E. megtévesztő adatok bevitele és képzése,

6. zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

1. figyelmetlenség (ellenőrzés hiánya),
2. szakmai hozzá nem értés,
3. a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
4. a megváltozott körülmények figyelmen kívül hagyása,

E. vírusfertőzött adathordozó behozatala,
6. biztonsági követelmények és gyári előírások be nem tartása,
7. adathordozók megrongálása (rossz tárolás, kezelés),
8. a karbantartási műveletek elmulasztása.

A szükséges biztonsági–, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

3. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

3.1. Tervezés és előkészítés során előforduló veszélyforrások

1. a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
2. hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

3.2. A rendszerek megvalósítása során előforduló veszélyforrások

1. hibás adatállomány működése,
2. helytelen adatkezelés,
3. programtesztelés elhagyása.

3.3. A működés és fejlesztés során előforduló veszélyforrások

1. emberi gondatlanság,
2. szervezetlenség és képzetlenség,
3. szándékosan elkövetett illetéktelen beavatkozás,
4. illetéktelen hozzáférés,
E. üzemeltetési dokumentáció hiánya.

4. Az informatikai eszközök környezetének védelme

4.1. Vagyonvédelmi előírások

1. a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,
2. a gépterembe való be– és kilépés rendjét szabályozni kell,
3. a gépterembe, szerverterembe történő illetéktelen behatolás tényét a Társaságvezetőjének
4. azonnal jelenteni kell,
E. az informatikai eszközöket csak a Társaság arra felhatalmazott alkalmazottai használhatják,
6. az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

4.2. Adathordozók

1. könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
2. az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni
3. a használni kívánt adathordozót (floppy, CD) a tárolásra kijelölt helyről kell kivenni, és oda
4. kell vissza is helyezni,

E. a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek,

6. adathordozót másnak átadni csak engedéllyel szabad,
7. a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

4.3. Tűzvédelem

A gépterem, illetve kiszolgáló helyiség a „D" tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent. A nagy fontosságú, pl. törzsadat–állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos szekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

5. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

A. számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

2. Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése. Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik. A munkák szervezésénél figyelembe kell venni:

- •a gyártó előírásait, ajánlatait,
- •a tapasztalatokat.

Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

6. Az informatikai feldolgozás folyamatának védelme

6.1. Az adatrögzítés védelme

a. adatbevitel hibátlan műszaki állapotú berendezésen történjen,
b. tesztelt adathordozóra lehet adatállományt rögzíteni,
c. a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
d. az adatrögzítő szoftver védelme.

Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.

Hozzáférési lehetőség:

- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető kezeli.

Az adatrögzítés folyamatához kapcsolódó dokumentációk:

1. adatrögzítési utasítások,
2. ellenőrző rögzítési utasítások,
3. tesztelő és törlő programok kezelési utasításai,
4. megőrzési utasítások,

E. gépkezelési leírások.

6.2. Az adathordozók nyilvántartása és tárolása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

Az adathordozók tárolására műszaki–, tűz– és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

6.3. Az adathordozók megőrzése, selejtezése, másolása, leltározása

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani. A selejtezést a Társaság selejtezésének szabályzata alapján kell lefolytatni. Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági, illetve archív adatállomány előállítása másolásnak számít. A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

6.4. Mentések, file-ok védelme és a szoftverek védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata. A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető, illetve a rendszergazdák a felelősek.

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára. Programhoz való hozzáférés, programvédelem A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek. Programok megőrzése, nyilvántartása A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a Társaságoknak az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni. A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja

az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét. A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

7. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől. A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrétfeladatokhoz igazítva kell alkalmazni. A vásárolt szoftverekről biztonsági másolatot kell készíteni. Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell. Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket. A Társaság informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad. A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos. Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése, illetve annak megakadályozása, hogy az megismétlődjön. A munkafolyamatba épített ellenőrzés során a szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

A Társaság bármilyen célú és jogalapú adatkezelése vonatkozásában a személyes adatok biztonsága érdekében köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a Rendelet és az Infotv. érvényre juttatásához szükségesek.

A Társaság az adatokat megfelelő intézkedésekkel védi a véletlen vagy jogellenes megsemmisítés, elvesztés, megváltoztatás, sérülés, jogosulatlan nyilvánosságra hozatal vagy az azokhoz való jogosulatlan hozzáférés ellen.

A Társaság a személyes adatokat bizalmas adatként minősíti és kezeli. A munkavállalókkal a személyes adatok kezelésére vonatkozóan titoktartási kötelezettséget ír elő. A személyes adatokhoz való hozzáférést a Társaság jogosultsági szintek megadásával korlátozza.

A Társaság az informatikai rendszereket tűzfallal védi, és vírusvédelemmel látja el.

A Társaság az elektronikus adatfeldolgozást, nyilvántartást számítógépes program útján végzi, amely megfelel az adatbiztonság követelményeinek. A program biztosítja, hogy az adatokhoz csak célhoz kötötten, ellenőrzött körülmények között csak azon személyek férjenek hozzá, akiknek a feladataik ellátása érdekében erre szükségük van.

A személyes adatok automatizált feldolgozása során a Társaság és az adatfeldolgozó további intézkedésekkel biztosítja:

1. a jogosulatlan adatbevitel megakadályozását;
2. az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
3. annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;

4. annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
E. e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és
6. f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

A Társaság a személyes adatok védelme érdekében gondoskodik az elektronikus úton folytatott bejövő és kimenő kommunikáció ellenőrzéséről.

A folyamatban levő munkavégzés, feldolgozás alatt levő iratokhoz csak az illetékes ügyintézők férhetnek hozzá, a személyzeti, a bér- és munkaügyi és egyéb személyes adatokat tartalmazó iratokat biztonságosan elzárva kell tartani.

Biztosítani kell az adatok és az azokat hordozó eszközök, iratok megfelelő fizikai védelmét.

A Társaság a személyes adatok kezeléséhez a szolgáltatás nyújtása során alkalmazott informatikai eszközöket úgy választja meg és üzemelte}, hogy a kezelt adat:

1. az arra feljogosítottak számára hozzáférhető (rendelkezésre állás)
2. hitelessége és hitelesítése biztosított (adatkezelés hitelessége)
3. változatlansága (adatintegritás)
4. a jogosulatlan hozzáférés ellen védett (adat bizalmassága) legyen.

A Társaság az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés ellen.

Az adatkezelő olyan műszaki, szervezése és szervezeti intézkedésekkel gondoskodik az adatkezelés biztonságának védelméről, amely az adatkezeléssel kapcsolatban jelentkező kockázatoknak megfelelő szintet nyújt.

Az adatkezelő az adatkezelés során megőrzi:

1. a titkosságot, ezért megvédi az információt, hogy csak az férhessen hozzá, aki erre jogosult,
2. a sértetlenséget, ezért megvédi az információnak és a feldolgozás módszerének a pontosságát és teljességét,
3. a rendelkezésre állást, ezért gondoskodik arról, hogy amikor a jogosult használónak szüksége van rá, valóban hozzá tudjon férni a kívánt információhoz, és rendelkezésre álljanak az ezzel kapcsolatos eszközök.

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

1. az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
2. a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
3. a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
4. a társaság. adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
E. a Társaság adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
6. amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az adatkezelő.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az adatkezelő az alábbi intézkedéseket és garanciális elemeket alkalmazza:

1. az adatkezelés során használt számítógépek a Társaság
2. tulajdonát képezik, vagy azok fölött tulajdonosi jogkörrel megegyező joggal bír az adatkezelő;

3. a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről az adatkezelő rendszeresen gondoskodik;
4. a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;

E. amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;

6. a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

8. A munkavállalók általános felelőssége

Valamennyi munkavállaló (gyakornok, önkéntes), aki a jelen szabályzatban meghatározott adatokhoz hozzáfér a megszerzett adatokat kizárólag a munkavégzése körében és céljából kezelheti, rögzítheti, tarthatja nyilván.

A Társaság biztosítja, hogy a munkavállalók képzés/oktatás keretében megismerhessék a pontos teendőiket és faladataikat, valamint felelősségüket az adatvédelem és az adatkezelés tekintetében.

A munkavállalók kötelesek valamennyi birtokukba jutott adatot biztonságosan kezelni, munkavégzésük során elővigyázatosnak lenni és a jelen adatvédelmi szabályzatban meghatározott feladatokat végrehajtani.

A munkavállaló köteles a szoftveres hozzáférés esetén erős és titkos jelszavakat alkalmazni, a jelszót megosztani, másnak felfedni szigorúan titkos.

Arra fel nem hatalmazott személlyel nem oszthat meg személyes adatokat, sem a Társaságon belül, se azon kívül.

A munkavállaló köteles rendszeresen felülvizsgálni és aktualizálni a rendelkezésre álló adatokat annak érdekében, hogy személyes adat szükségtelenül ne kerüljön sem tárolásra, sem egyéb kezelésre. A már szükségtelenné váló adatok törlése a munkavállaló felelőssége.

Amennyiben a munkavállaló bizonytalan a helyes adatkezelés vagy az adatvédelmi szempontok tekintetében, úgy köteles tanácsért a vezetőjéhez vagy az adatvédelmi tisztségviselőhöz fordulni.

Ha a munkavállaló tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy a helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

Az Adatkezelő adatkezelést végző alkalmazottja fegyelmi, kártérítési, szabálysértési és büntetőjogi-felelősséggel tartozik a munkavégzés során tudomására jutott személyes adatok jogszerű kezeléséért, az Adatkezelő nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.

9. Papír alapú adatkezelés

A jelen bekezdés célja annak a meghatározása, hogy az adatokat hol és milyen módon szükséges kezelni ahhoz, hogy az adatok biztonsága biztosítható legyen. Az adattárolásra vonatkozó további esetleges kérdésekkel a vezető munkatárshoz fordulhat a Társaság munkatársa.

A papír alapon kezelt adatokat olyan biztonságos helyen szükséges tárolni, ahol arra jogosulatlan személy nem ismerheti meg.

Azokat az elektronikus úton érkezett vagy kezelt adatokat, melyek valamely okból nyomtatásra kerülnek elzárt irattartókban, illetőleg elkülönítetten szükséges kezelni. A Társaság munkatársai kötelesek gondoskodni arról, hogy a kinyomtatott iratokhoz arra jogosulatlan személyek ne férjenek hozzá. A

kinyomtatott adatokat tartalmazó iratokat azonnal szükséges megsemmisíteni akkor, amikor a kinyomtatás oka megszűnik.

10. Elektronikus adatkezelés

Az elektronikusan tárolt adatokat védeni szükséges a jogosulatlan eléréstől, véletlen törléstől és kémprogramokkal, vírusokkal, illetéktelen rendszer feltörésekkel és rendszertámadásokkal szemben.

Az adatokat erős jelszavakkal szükséges védeni, melyek cseréjére rendszeresen, de legalább fél évente sor kerül. A jelszavak titkosnak, hozzáférhetetlennek kell lenniük, a munkavállalók/vezetők nem oszthatják meg azt sem egymás között, sem más személyekkel.

Amennyiben az adat hordozható adattárolón (cd, DVD, pendrive, SSD) kerül rögzítésre ezeket az adattároló eszközöket a használatot követően biztonságos helyen, jogosulatlan személyek számára hozzáférhetetlenül szükséges tárolni.

Adatokat csak az arra kijelölt szervereken és hardver eszközökön szabad tárolni. Felhő alapú szolgáltatás igénybevételével adat csak a kijelölt és maghatározott szolgáltatóval kötött szerződés alapján és szerint tárolható. A Társaság vezetője az adattárolás megkezdése előtt meggyőződik arról, hogy a felhő alapú szolgáltatást biztosító partner megfelel az adatvédelem jogszabályi és technikai követelményének.

Valamennyi adattárolásra szolgáló szervert és számítógépet szükséges tűzfallal és vírusirtóval védeni. A

tárolt adatokat rendszeresen szükséges felülvizsgálni.

A személyes adatokat tartalmazó szervereket a nyitott irodahelységen kívüli elkülönített helyen szükséges tárolni.

Az adattárolásra alkalmazott szoftvereket rendszeresen frissíteni szükséges. A frissítés megkezdése előtt a szoftverfrissítési metódust az adatvesztés elkerülése érdekében tesztelni szükséges.

A személyes adatokat tilos közvetlenül a laptopra vagy egyéb mobileszközre (tablet, okostelefon) menteni.

11. Technológia az eszközök és a hozzáférések menedzselésére

Az Adatkezelő. szegmentálja és korlátozza a hálózatának azon részeire vonatkozó hozzáférést, amelyek tárolják és feldolgozzák a rendkívül érzékeny személyes adatokat. A hálózati sebezhetőségek és külső fenyegetések felismerése és elemzése, amelyek célja az adatlopás és adatmegsemmisítés. A hálózat folyamatos figyelemmel kísérése és védelme a megoldás annak érdekében, hogy a személyes adatok sérülését célzó fenyegetések ellen hatékonyan fellépjen.

12. Az adatok fizikai tárolási helye

Személyes adatok az alábbi módon kerülhetnek az Adatkezelő kezelésébe: egyfelől elektronikus levélben másfelől, az ügyfél személyes adatszolgáltatása útján. Az adatkezelő számítástechnikai rendszere és más adatmegőrzési rendszere a székhelyén és az adatfeldolgozójánál találhatóak meg.

Az adatkezelő székhelye és az adatfeldolgozó székhelye és számítástechnikai rendszere védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá számítógép vírusok, a számítógépes betörések és a szolgálatmegtagadásra vezető támadások ellen. Személyes adatok az alábbi módon kerülhetnek az adatkezelő kezelésébe egyfelől elektronikus levélben másfelől, az ügyfél személyes adatszolgáltatása útján. Az adatkezelő számítástechnikai rendszere és más adatmegőrzési rendszere a székhelyén és az adatfeldolgozójánál találhatóak meg.

Az adatkezelő székhelye és az adatfeldolgozó székhelye és számítástechnikai rendszere védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá számítógép vírusok, a számítógépes betörések és a szolgálatmegtagadásra vezető támadások ellen. Az adatkezelő a biztonságról szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik.

A Társaság az adatkezelés eltérő célja alapján ügyviteli és nyilvántartási célú adatkezeléseket végez. Az ügyvitelhez kapcsolódó adatkezelés a szerződés/megállapodás nyilvántartásaihoz (iktatásához), feldolgozásához kapcsolódik. Alapvető célja az adott szerződéshez/megállapodáshoz tartozó feladatok elvégzéséhez (szerződések teljesítése), az adatkezelés szereplőinek azonosításához és a szerződés lezárásához szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott szerződés irataiban és az ügyviteli segédletekben szerepelnek, kezelésük ebből a célból csak az alapul szolgáló irat selejtezéséig lehetséges.

A nyilvántartási célú adatkezelés az egyes adatfajtákból álló adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, lekérdezhetőségét. A személyes adatok kezelésének célja a Társaság üzletviteli tevékenysége során történő felhasználása, ennek megfelelően az alábbi feladatok azonosíthatóak:

1. az adatkezelővel munkavégzésre irányuló jogviszonyban álló személyek adatait tartalmazza,
2. a foglalkozás–egészségügyi ellátásban kezelt személy betegségére, egészségügyi állapotára vonatkozó személyes adatokat tartalmaz, gyógykezelés vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából,
3. az érintett anyagi vagy egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik
4. a Társasággal szerződéses kapcsolatba került személyek személyes adataira vonatkozik (ügyviteli célú adatkezelés)

E. a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve, hogy a törvényben meghatározottak szerint, az adatok érintettel való kapcsolatának megállapítását véglegesen lehetetlenné teszik,

6. tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra
7. levéltári őrzésre átadott iratokkal összefüggésben valósul meg.

Az adatok jogszerű és célhoz kötött használata során az alábbiak betartása kötelező:

1. a személyes adatokkal dolgozó munkavállalók a munkaterület elhagyása során kötelesek a felhasznált eszközt képernyőzárral védeni, melyhez egyedi belépési azonosító, illetőleg kód kapcsolódik
2. személyes adat csak olyan levelezőrendszeren küldhető tovább, melynek biztonsága és zárt jellege garantált, továbbá olyan címzett számára, aki megfelelő és biztos módon beazonosítható olyan személyként, aki a fogadott személyes adatokat jogszerűen megismerheti
3. a személyes adatokat tartalmazó fájlokat, üzeneteket kóddal, vagy egyéb módon titkosítani szükséges
4. a személyes adatok Európai Gazdasági Térségen túli továbbítása fő szabály szerint tilos, amennyiben annak továbbítása mégis szükségessé válik, úgy azt csak olyan fogadó részére szabad továbbítani, aki igazoltan megfelel a GDPR–ban foglalt valamennyi adatvédelmi követelménynek.

E. a Társaság napi operatív tevékenysége során tilos a saját gépre személyes adatokat menteniük, valamennyi adatot kötelező a Társaság saját belső rendszerére menteni

6. a Társaság működése során nem vihetők ki a személyes adatokat tartalmazó iratok a Társaság székhelyéről/telephelyéről. Amennyiben ez mégis szükségessé válna, úgy ebben a tekintetben a munkavállalók kötelesek azt bejelenteni és egyedi jóváhagyást kérni a felettesüktől.

13. Az adatok pontosságának biztosítása

A Társaság jogszabályi kötelessége az általa kezelt személyes adatok naprakész és pontos nyilvántartása.

A Társaság kiemelt figyelmet fordít az esetlegesen és szükségesen nyilvántartott különleges adatok naprakészségére és pontosságára.

A fentiek okán a Társaság valamennyi munkavállalójának kiemelt feladata, hogy a tőle telhető legjobb módon az adatokat naprakészen és pontosan tartsa nyilván. Az adatokat a lehető legkevesebb adattároló helyen szükséges tartani, a Társaság munkavállalói feleslegesen és engedély nélkül semmilyen egyéb nyilvántartást vagy személyes adatokat tartalmazó egyéb forrást nem készíthetnek.

A Társaság az érintettek számára folyamatosan biztosítja az adatpontosítás lehetőségét.

Amennyiben a kezelt adatok körében pontatlan adatok kerülnek elő, azt haladéktalanul pontosítani szükséges, így különösen, ha az ügyfél az általa megadott telefonszámot vagy e-mail címet közöl. Az elektronikus levelezés mindaddig elérhetőnek tekinthető, ameddig az ügyfél a cím megváltoztatását nem jelen} be, vagy onnan a kézbesítés sikertelenségére vonatkozó rendszerüzenet vissza nem érkezik.

Az érintett jelzések hiányában is pontatlannak bizonyult adatot valamennyi rendszerből és adattárolóból a pontatlanság megállapítása után haladéktalanul törölni kell.

A Társaság marketingért felelős munkatársának a feladata a marketing levelezési és adatrendszerének naprakészen tartása, azzal, hogy annak teljes felülvizsgálata legalább fél évente különösebb ok nélkül is ütemezetten kötelező.

14. Adat bekerülésének és feldolgozásának folyamata és hozzáférési jogosultságok

Személyes adatokat az ügyfelektől a Társaság bármely alkalmazottja gyűjthet és azt munkaköri leírásának és ennek a Szabályzatnak megfelelően kezelheti.

9.1E. Eljárás eszközhiba esetén

Eszközhiba észlelése esetén a munkavállalók kötelesek értesíteni az ügyvezetőt és a rendszergazdát. A meghibásodott eszközt a hálózatról azonnal le kell választani és mechanikai, azaz hardveres hiba esetén azonnal áramtalanítani kell. Szoftverhiba vagy jogosulatlan tevékenység észlelése esetén a munkaállomást a hálózatról le kell kapcsolni, de áramtalanítani nem szabad.

16. Eljárás természeti katasztrófa esetén

Természeti katasztrófa esetén a munkaállomást áramtalanítani kell, majd amennyire lehetséges biztonságba helyezni és értesíteni az ügyvezetőt és a rendszergazdát.

17. Az adatvédelmi incidens fogalma

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; (Rendelet 4. cikk 12.)

A leggyakoribb jelentett incidensek lehetnek például: a laptop vagy mobil telefon elvesztése, személyes adatok nem biztonságos tárolása (pl. szemetesbe dobott fizetési papírok); adatok nem biztonságos továbbítása, ügyfél- és vevő- partnerlisták illetéktelen másolása, továbbítása, szerver elleni támadások, honlap feltörése.

18. Adatvédelmi incidensek kezelés, orvoslása

Adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása a Társaság vezetőjének feladata.

Az informatikai rendszereken naplózni kell a hozzáféréseket és hozzáférési kísérleteket, és ezeket folyamatosan elemezni kell.

Amennyiben a társaság ellenőrzésre jogosult munkavállalói a feladataik ellátása során adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell a Társaság vezetőjét.

A Társaság munkavállalói kötelesek jelenteni a Társaság vezetőjének, vagy a munkáltatói jogok gyakorlójának, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek.

Adatvédelmi incidens bejelenthető a Társaság központi e-mail címén, telefonszámán, amelyen a munkavállalók, szerződő partnerek, érintettek jelenteni tudják az alapul szolgáló eseményeket, biztonsági gyengeségeket.

Adatvédelmi incidens bejelentése esetén a Társaság vezetője – az informatikai, pénzügyi és működési vezető bevonásával – haladéktalanul megvizsgálja a bejelentést, ennek során azonosítani kell az incidenst, el kell dönteni, hogy valódi incidensről, vagy téves riasztásról van szó. Meg kell vizsgálni és meg kell állapítani:

1. az incidens bekövetkezésének időpontját és helyét,
2. az incidens leírását, körülményeit, hatásait,
3. az incidens során kompromittálódott adatok körét, számosságát,
4. a kompromittálódott adatokkal érintett személyek körét,
E. az incidens elhárítása érdekében tett intézkedések leírását,
6. a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni és el kell különíteni és gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és megőrzéséről. Ezt követően lehet megkezdeni a károk helyreállítását és a jogszerű működés visszaállítását.

19. Adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensekről nyilvántartást kell vezetni, amely tartalmazza:

1. az érintett személyes adatok körét,
2. az adatvédelmi incidenssel érintettek körét és számát,
3. az adatvédelmi incidens időpontját,
4. az adatvédelmi incidens körülményeit, hatásait,
E. az adatvédelmi incidens orvoslására megtett intézkedéseket,
6. az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A Társaság nyilvántartja továbbá az adatvédelmi incidensekhez kapcsolódóan az alábbi információkkal:

1– – az adatvédelmi incidenshez kapcsolódó tények,
2– – annak hatásai és
3– – az orvoslására tett intézkedések.

A fen} nyilvántartásba a felügyeleti hatóság betekinthet és ellenőrizheti a GDPR 33. cikk rendelkezéseinek betartását.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

9. 20 Adatok törlésének folyamata

Adatok törlésére a tervezett adatvagyon felülvizsgálat esetén évente, illetve az ügyfelek megkeresése alapján, kérelem alapján kerülhet sor. Mindkét esetben szükséges betartani jelen szabályzat vonatkozó szabályait, valamint az iratmegsemmisítési szabályzatot. Elektronikus adat törlését a rendszergazda végzi.

X. AZ ÁLTALÁNOS ADATKEZELÉSI SZABÁLYOK

1. Az adatvédelmi eljárásrend szervezeti kialakítása

Az ügyvezető

a) jóváhagyja a személyes és különleges adatokat tartalmazó, adatszolgáltatási, adattovábbítási, valamint az adatvédelemmel és adatkezeléssel kapcsolatos nyilvántartásokat,
b) engedélyezi a nyilvántartási rendszerekhez a hozzáférési jogosultságot,
c) szükség esetén gondoskodik az adatvédelmi ismeretek oktatásáról a foglalkoztatottjai részére,
d) a tudomására jutott visszásság esetén utasítja az érintett foglalkoztatottat a jogszerűtlen adatkezelés megszüntetésére, szükség esetén fegyelmi eljárást kezdeményez a foglalkoztatottal szemben,

A munkatárs

a) köteles az adatvédelemmel kapcsolatos jogszabályokat és a Szabályzatot megismerni és maradéktalanul betartani,
b) köteles tájékoztatni közvetlen felettesét, szükség esetén az ügyvezetőt, a feladatkörében felmerült bármely adatvédelmi problémáról, észrevételeiről, a számítástechnikai eszközök bárminemű meghibásodásáról, az adatállomány kezelhetőségében bekövetkezett problémáról,
c) köteles a tudomására jutott, az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszüntetni,
d) vezeti a munkakörébe tartozó adat–, adatszolgáltatási és adattovábbítási nyilvántartást,
e) gondoskodik arról, hogy az általa vezetett nyilvántartás adataihoz illetéktelen személy ne férhessen hozzá, ügyel a nyilvántartás biztonságos tárolására,
f) elvégzi a kezelésében lévő adatok biztonsági mentését, gondoskodik azok biztonságos tárolásáról,
g) a jogszabály által felhatalmazott személynek vagy szervezetnek adatot szolgáltat, adatot továbbít,
h) köteles közvetlen felettesét, szükség esetén az ügyvezetőt tájékoztatni minden olyan eseményről, amikor őt jogszerűtlen adatkezelésre kérték fel, utasították,
i) haladéktalanul jelzi közvetlen felettesének, ha az adatállományba jogosulatlan hozzáférést vagy bárminemű változást tapasztal,
j) fegyelmi és kártérítési felelősséggel tartozik azért, hogy tevékenységét az adatkezelésre és az adatok védelemére vonatkozó jogszabályoknak, valamint a Szabályzatnak, az adatkezelést elrendelő jogszabály hiányában pedig az érintett hozzájárulásának megfelelően végezze
k) – kötelezettsége, hogy az 1. 2. f) pont szerinti éves adatvédelmi jelentéshez vezetője útján adatot szolgáltasson.
l) – kötelezettsége, hogy részt vegyen az adatvédelmi oktatáson.

2. Az adatkezelés részletes szabályai

A munkatársak az irodát és az irat és adattárolásra használt berendezéseket munkaidőben fokozott gondossággal kötelesek őrizni. A munkatárs köteles a számítógépét és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a számítógépet kikapcsolni, az irodahelyiség ajtaját bezárni és a helyiség kulcsát az őrzés helyén leadni.

A munkatárs a nála lévő iratokat köteles munkaidőn túl – és amelyeket lehetséges munkaidőben is – elzárt helyen tartani. Munkaidőben iratok csak a munkavégzés céljából és a munkavégzéshez szükséges időtartamban lehetnek a munkatársnál.

Személyes adatokat is tartalmazó iratot vagy más adathordozót (a továbbiakban együtt: irat) az Adatkezelő helyiségéből kivinni – munkaköri feladat ellátásának kivételével – csak indokolt esetben, a felettes vezető egyetértésével lehet. A munkatárs ez esetben is köteles gondoskodni arról, hogy az irat ne vesszen el, ne rongálódjon vagy semmisüljön meg és tartalma illetéktelen személy tudomására ne jusson.

A kiskorúakról készült minden személyes adatot tartalmazó feljegyzést zárható szekrényben tárolni.

Munkavállalónál lévő iratba az ügyintéző személyen kívül más csak akkor tekinthet be, ha ezt szabály lehetővé teszi. A betekintési jog gyakorlása közben úgy kell eljárni, hogy ezáltal mások személyes adatainak védelméhez fűződő jogai, és személyiségi jogai ne sérülhessenek. Jelen pont rendelkezéseit kell alkalmazni a másolat és a kivonat készítésekor is.

A munkavégzésre, illetve feladatellátásra használt eszközt, amelyen az Adatkezelő által kezelt vagy feldolgozott személyes adat is megtalálható, minden esetben jelszóval kell védeni. A munkatárs köteles az Adatkezelő által biztosított készüléken képernyőzárat létrehozni, továbbá a készüléket folyamatosan jelszavas védelemmel ellátva használni. A hozzáférési kódokat az alkalmazottak bizalmasan kötelesek kezelni. A munkatárs köteles a kódot az eszköz visszaadásának napján az Adatkezelő számára megadni vagy az eszközt kóddal nem védett állapotban visszaadni.

A munkavégzés vagy feladatellátás céljára szolgáló eszközökön a személyes adatot is tartalmazó dokumentumot az alkalmazottak nem nyithatják meg. Amennyiben valamely okból ez elkerülhetetlen, akkor a helyi másolatot minden esetben véglegesen és visszaállíthatatlanul törölni kell az eszközről.

A munkavégzés vagy feladatellátás céljára átadott eszközöket kizárólag az alkalmazottak használhatják, hozzátartozóik vagy más személy számára a használat tilos.

3. Az adatkezelésre vonatkozó különös szabályok

A papír alapú, személyes adatot tartalmazó dokumentumokat munkavégzésen kívül olyan módon kell tárolni, hogy azokat csak az erre a feladatra feljogosított megbízott érhesse el.

Ha a papír alapú, személyes adatokat tartalmazó munkadokumentumok használata szükségtelenné válik, olyan módon kell megsemmisíteni, hogy a megsemmisítést követően ne lehessen tartalmát reprodukálni.

Tilos magánhasználatú eszközön az adatkezelő kezelésében vagy feldolgozásában lévő személyes adatot tárolni, kivéve, ha a tárolás a munkavégzéshez elengedhetetlenül szükséges és a tárolást a munkavégzést követően megszüntetik.

A munkatárs feladatellátásra szolgáló jogviszonya megszűnése esetén minden személyes adatot is tartalmazó papír alapú és elektronikus iratot, adatot köteles a foglalkoztatásának utolsó napját megelőzően az Adatkezelő részéra visszaszolgáltatni, azokról másolatot nem tarthat magánál, melyről átadás–átvételi ügyvezetőkönyvet kell készíteni.

Minden munkatárs köteles az általa használt munkaterületet olyan módon használni, hogy azon az Adatkezelő kezelésében vagy feldolgozásában lévő, személyes adatot is tartalmazó dokumentumok lehetőség szerint szabadon ne legyenek hozzáférhetőek. Ilyen intézkedésnek minősül különösen: a számítástechnikai eszközök jelszavas védelme, az üzlethelyiség zárása, az iratok elhelyezése zárt és védett tárolóba. Az Adatkezelő minden munkatársa köteles biztosítani és a megfelelő intézkedéseket megtenni annak érdekében, hogy az Adatkezelő valamennyi irodai és üzleti területére az Adatkezelővel feladatvégzésre irányuló jogviszonyban nem álló személy csak munkatárs kíséretében léphessen be. Az Adatkezelő területére belépni jogosult személyek az Adatkezelő által kezelt személyes adatok megismerésére nem minden esetben jogosultak. A munkatársak kötelesek megtenni mindent annak érdekében, hogy az Adatkezelő kezelésében álló személyes adatok biztonságban legyenek, az ennek megsértéséből az Adatkezelőt ért kárért az adatvédelmi incidenst előidéző személy teljes felelősséggel tartozik.

Személyes adatok csak biztonságos kommunikációs csatorna alkalmazásával, illetve megfelelő titkosítási megoldással adhatók át más személynek.

Amennyiben az Adatkezelő más adatkezelőtől, az adathoz kapcsolódó rendelkezéssel fogad személyes adatot, valamennyi, az adattal érintkező felhasználónak kötelessége az adattovábbító rendelkezéseit figyelembe venni.

Harmadik személynek titoktartási nyilatkozat hiányában személyes adatot tartalmazó információ nem adható ki.

4. Az adatvédelmi incidens kezelési rendje

Adatvédelmi incidens fogalma: 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; (Rendelet 4. cikk 12.)

A leggyakoribb jelentett incidensek lehetnek például: a laptop vagy mobil telefon elvesztése, személyes adatok nem biztonságos tárolása (pl. szemetesbe dobott fizetési papírok); adatok nem biztonságos továbbítása, ügyfél- és vevő- partnerlisták illetéktelen másolása, továbbítása, szerver elleni támadások, honlap feltörése. Adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása az Adatkezelő feladata.

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, hátrányos megkülönböztetést, személyazonosság–lopást vagy a személyazonossággal való visszaélést, anyagi veszteséget, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, egyéb jelentős szociális hátrányt.

A jelen szabályzat hatálya alá tartozó személyek, bármely, az Adatkezelő által vagy közreműködésével működtetett informatikai rendszer vagy manuális adatkezelés esetében haladéktalanul, de legkésőbb 24 órán belül kötelesek jelenteni az ügyvezető számára, ha adatvédelmi incidens gyanúja merül fel, vagy ha biztos tudomása van arról, hogy adatvédelmi incidens következett be.

A bejelentést elsősorban munkaidőben, telefonon keresztül kell megtenni, és azt követően elektronikus levél formájában is meg kell erősíteni.

Az ügyvezető és az egyéb érintett munkatársak a számukra jelzett, vagy saját feladat– vagy hatáskörükben megállapított adatvédelmi incidens felderítése és súlyosságának megállapítása érdekében az alábbi eljárásrend szerint kötelesek eljárni.

Az Adatkezelő minden szükséges intézkedést megtesz az adatvédelmi incidensek elkerülése érdekében.

Amennyiben mégis adatvédelmi incidens következik be, az ügyvezető felveszi a kapcsolatot az adatvédelmi incidenssel érintett informatikai rendszer rendszergazdájával, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával, és ha azonosítható, az incidenst előidéző személlyel.

Az ügyvezető a felderítés során az alábbi kategóriák egyikébe sorolja be a bekövetkezett eseményt az European Union Agency for Network and Information Security (ENISA) 2013. évi Útmutatója alapján:

a) Alacsony szintű adatvédelmi incidens: amely az érintetteknek kellemetlenséget jelent. Ilyen a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési tevékenység,
b) Közepes szintű adatvédelmi incidens: amelyben az érintettek komoly következményekkel számolhatnak, melyet nagy nehézséggel hozhatnak helyre. Ilyen a személyes adatok nagyobb körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési tevékenység,
c) Magas szintű adatvédelmi incidens: melyben az érintettek jelentős következményekkel számolhatnak, melyet nem tudnak helyrehozni. Ilyen a személyes adatok – viselkedés, pénzügyi vagy érzékeny adatokat is tartalmazó – széles körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési tevékenység, illetve az adtok körétől függetlenül minden olyan eset, amikor biztosra vehető, hogy az érintettre jelentős hatással lesz.

Kötelező intézkedések adatvédelmi incidens estén az ügyvezető:

Megállapítja az adatvédelmi incidens várható súlyosságát az 1.3. pont

szerint. Alacsony szintű adatvédelmi incidens esetén,

a) Legkésőbb a tudomásszerzéstől számított 48 órán belül az érintett IT rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére.
b) Rögzíti az adatvédelmi incidenst az adatvédelmi incidens

nyilvántartásba. Közepes szintű adatvédelmi incidens esetén,

a) haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az IT rendszergazda, az adatkezelési folyamat adatgazdája és az Adatkezelő vezetője,
b) Rögzíti az adatvédelmi incidenst az adatvédelmi incidens nyilvántartásba.
c) az ügyvezető értesíti a Nemzeti Adatvédelmi és Információszabadság Hatóságot 72 órán belül

d) az adatvédelmi incidensről, ha az valószínűsíthetően kockázattal jár az érintett vagy más személy jogaira és szabadságára nézve és a munkacsoport meghatározza az adatvédelmi incidens kezelésének lépéseit és módját és felhívja intézkedésre jogosult személyt az incidens kezelésére.

Magas szintű adatvédelmi incidens esetén,

a) az ügyvezető haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az IT rendszergazda, az adatkezelési folyamat adatgazdája és az Adatkezelő vezetője,
b) a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről,
c) az ügyvezető rögzíti az adatvédelmi incidenst az adatvédelmi incidensek nyilvántartásába,
d) az ügyvezető értesíti a Nemzeti Adatvédelmi és Információszabadság Hatóságot 72 órán belül.

Amennyiben az érintett ezt kéri, az ügyvezető tájékoztatást ad az érintett személyes adatára is kiterjedő adatvédelmi incidensekkel kapcsolatban. Az Adatkezelő nem köteles tájékoztatni az érintettet az adatvédelmi incidensről, ha

a) az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta (pl. titkosítás), amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat,
b) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságára jelentett magas kockázat a továbbiakban nem valósul meg,
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé az Adatkezelő részéről. Ebben az esetben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell tenni, mely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

Ha az Adatkezelő nem értesítette az érintettet az adatvédelmi incidensről, az incidens bejelentését követően a felügyeleti hatóság miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár–e, elrendelheti az érintett tájékoztatását, vagy megállapíthatja, hogy az érintett tájékoztatása valamely ok miatt nem szükséges.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, az Adatkezelő indokolatlan késedelem nélkül köteles írásban, vagy ha rendelkezésére áll e–mail cím, akkor e–mailben tájékoztatni az érintettet az adatvédelmi incidensről. A tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat:

a) az ügyvezető vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségét
b) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket
c) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

10.5.Adatfeldolgozónál bekövetkező adatvédelmi incidens

Ha az adatfeldolgozó rendszerében észlel adatvédelmi incidenst, indokolatlan késedelem nélkül köteles bejelenteni az Adatkezelőnek, illetve amennyiben nem lehetséges az információkat egyidejűleg közölni, azokat köteles további indokolatlan késedelem nélkül akár részletekben is közölni.

Amennyiben az adatkezelő észlel adatvédelmi incidenst valamely adatfeldolgozójánál, vagy adatvédelmi incidens gyanúja merül fel, akkor az Adatkezelő az adatfeldolgozó egyidejű értesítésével lefolytatja az adatvédelmi incidens azonosításával és kezelésével kapcsolatos eljárását.

Az adatfeldolgozó az – Adatfeldolgozói szerződésben foglalt kötelezettségei szerinti – az adatkezelővel egyeztetve köteles az incidens kezelésében együttműködni, illetve köteles minden olyan megfelelő technikai és szervezési intézkedéseket végrehajtani, ami a hasonló vagy ugyanilyen adatvédelmi incidens elkerülése érdekében szükséges, és az incidens ismételt bekövetkezésének lehetőségét kizárja.

Az adatvédelmi incidens bejelentésének elmaradásából, az incidens nem megfelelő kezeléséből és az együttműködési kötelezettség megszegéséből fakadó felelősség az adatfeldolgozót terheli.

XI. AZ ADATKEZELÉSI NYILVÁNTARTÁSOK

1. Adatkezelések és adattovábbítások nyilvántartása a GDPR 30. cikk szerint.

A Társaság a felelősségébe tartozóan végzett adatkezelési tevékenységekről írásban, ideértve az elektronikus dokumentumot is, nyilvántartást köteles vezetni a GDPR 30. cikke szerin} tartalommal, ami a következő információkat tartalmazza:

1. az adatkezelés célja
2. az érintett kör
3. az adatkezelés jogalapja
4. az adatok forrása
5. az adattovábbítás jogalapja
6. az adattovábbítás címzettje
7. az adatfeldolgozó (igen/nem)
8. a személyes adatok kategóriái
9. különleges adatok felsorolása (igen/nem)
10. gyermekek adatainak felsorolása (igen/nem)
11. az adat tárolásának helye az adatkezelőnél fizikálisan
12. az adat tárolásának helye elektronikusan
13. szükséges tájékoztatás módja
14. hozzájárulás új érintettek részére (igen/nem)
15. érdekmérlegelés (igen/nem)
16. adatfeldolgozási megállapodás (igen/nem)
17. kockázat mértéke: 1-nincs kockázat, 2-van kockázat, 3-magas kockázat (DIPA)

A Társaság köteles a nyilvántartást megkeresés alapján az eljáró felügyeleti hatóság részére hozzáférhetővé tenni.

2. Ügyfélmegkeresések nyilvántartása

A Társaság az alábbi tartalommal nyilvántartást vezet az érintettektől érkező megkeresésekről:

1. sorszám
2. a megkeresés beérkezésének időpontja
3. érintett neve

4. a megkeresés tárgya
5. a megtett intézkedés megnevezése
6. a megtett intézkedés időpontja

3. Adattovábbítások nyilvántartása

1. sorszám
2. az adattovábbítás időpontja
3. a címzett megnevezése
4. a továbbított személyes adatok köre

E. jogszabályban meghatározott továbbítandó adatok köre

4. Adatkezelés megszűntetés nyilvántartás

1. sorszám
2. kérelem beérkezésének időpontja
3. érintett neve és azonosító adatai
4. a kérelem tartalma

E. a megtett intézkedések megnevezése

6. az intézkedés időpontja

5. Hozzájárulások nyilvántartása

1. sorszám
2. a hozzájárulás megadásának időpontja
3. a személyes adatok köre, melyre a hozzájárulást megadták
4. a hozzájárulás célja

E. a hozzájáruló neve és postacíme, e–mail címe

XII. A KÖZÖS ADATKEZELÉS ÉS AZ ADATFELDOLGOZÁS

A Társaság nagy gondossággal jár el minden olyan esetben, amikor valamely adatkezelés megvalósítása során több szereplő működik együtt, gondosan értékeli, hogy az adatkezelési együttműködés körében az alábbi lehetőségek közül mely merülhet fel:

- több önálló adatkezelő együttműködése,
- közös adatkezelés, vagy
- adatfeldolgozás.

Az adatkezelő definíciójából következik, hogy az adatkezelés céljainak és eszközeinek meghatározása az adatkezelői státusz központi eleme, mely az adatfeldolgozástól való elhatárolás alapját képezi.

Az adatkezelés céljának és eszközeinek a meghatározása történhet egyetlen adatkezelő által önállóan, vagy több adatkezelő által közösen. Közös adatkezelés esetében a személyes adatok kezelésének céljait és eszközeit a közös adatkezelők együttesen határozzák meg (például két adatkezelő közös terméke és az esetlegesen ahhoz kapcsolódó szolgáltatások megvalósítása eredményezhet közös adatkezelést). A célok, illetve eszközök lényeges elemeinek együttes, illetve közös meghatározása azonban nem jelen} azt, hogy a közös adatkezelőknek egyenlő mértékben kellene megosztaniuk a célok és eszközök meghatározásával kapcsolatos kompetenciákat. A döntési jogosultságokat eltérő formában és mértékben gyakorolhatják, e tekintetben ahhoz, hogy közös adatkezelőnek minősüljenek, önmagában az is elegendő lehet, hogy vagy az adatkezelés célját, vagy annak egyéb lényeges elemeit (például a gyűjtendő adatok körét) együtt határozzák meg.

Az adatfeldolgozó az adatkezelő nevében kezel személyes adatot. Az adatfeldolgozó tevékenysége olyan (elsősorban technikai jellegű) adatkezelési műveletek végrehajtását jelen}, melyet az adatkezelő mással végeztet el. Az informatikai szolgáltatók bevonására például jellemzően adatfeldolgozóként kerül sor.

Amennyiben az adatkezelő adatfeldolgozó közreműködését veszi igénybe adott adatkezelési műveletek elvégzéséhez, az adatfeldolgozónak az adatkezelő utasításai szerint kell eljárnia, az adatkezelő nevében és érdekében végzi tevékenységét, valamint az adatkezelővel szemben tájékoztatási kötelezettsége van.

Az adatfeldolgozó beazonosításnál a Társaság a konkrét tevékenység tisztázásából indul ki és a tényleges műveletekre vonatkozó döntési kompetenciák alapján lehet megállapítani, hogy adatfeldolgozónak minősül-e az adott tevékenységet végző entitás. Mivel az adatfeldolgozó tevékenységét az adatkezelő döntése alapján végzi, tevékenysége során a felek között létrejött szerződésben foglaltaknak megfelelően köteles eljárni, az adatfeldolgozó a rá az adatkezelő által delegált feladatokat végzi. Amennyiben ezt a megbízást túllépi, és a közreműködő szerepet vállal az adatkezelés céljának és eszközei lényegi elemeinek akár részbeni meghatározásában, közös vagy önálló adatkezelővé válik az érintett adatkezelés vonatkozásában.

Az adatkezeléssel kapcsolatos együttműködések vizsgálata során a Társaság első lépésként a fentiek 的figyelembevételével beazonosítja az egyes szereplők státuszát.

1. A közös adatkezelés elhatárolása az adatfeldolgozástól

A közös adatkezelést és az adatfeldolgozást az köti össze, hogy ezek

- ugyanazon cél megvalósítása érdekében folyatott adatvédelmi folyamatba illeszkedő,
- egymást kiegészítő jellegű személyes adatokat érintő tevékenységek. Az elhatárolás fő kérdése az adatkezelési cél és eszköz meghatározására vonatkozó döntési kompetencia, azaz hogy az adatvédelmi folyamatban résztvevő szereplők közül melyik hozza az adatkezelés lényegét érintő érdemi kérdéseket.

Az adatkezelés céljának és eszközének meghatározása alapvetően a „miért” és „hogyan” kérdések megválaszolását jelen}, azaz annak meghatározását, miért kerül sor az adatok kezelésére, és hogyan kerül sor arra. Fontos kérdés azonban ennek kapcsán – mely különösen az eszközök meghatározása esetében merül fel – hogy melyek a célok és eszközök lényegi elemei, azaz milyen szintig kell az adatkezelőnek ezeket a lényegi elemeket meghatározni az adatfeldolgozó számára, mekkora mozgástere lehet ezen a téren az adatfeldolgozónak. Annak értékelése, hogy közös adatkezelés, vagy adatfeldolgozás valósul-e meg, funkcionális szempontok alapján történik, azaz a fő kérdés az, hogy az adatkezelés célját, eszközeit és azok lényegi elemeit többen határozzák-e meg.

Az előzőekben leírtak alapján egyértelmű, hogy az adatfeldolgozókén} minősítés alapvető követelménye, hogy az adatfeldolgozó az adatok feldolgozását az adatkezelő érdekében, annak utasításai szerint végzi. A cél – azaz az adatkezelés miértjének – meghatározása ennek megfelelően az elhatárolás szempontjából kevésbé problematikus, hiszen mindig adatkezelő az, aki az adatkezelés célját meghatározza.

Az eszközök esetében már több kérdés merül fel: az eszközök meghatározása alapvetően a technikai és szervezési/módszertani kérdések meghatározását jelen}, melynek bizonyos elemei azonban delegálhatók az adatfeldolgozók részére tipikusan ilyen például az adatok cél szerin} kezelésére alkalmas hardver, illetve szoftver kiválasztása), az adatkezelőnek csak a lényegi elemeket kell itt meghatároznia. A technikai és szervezési kérdések meghatározása történhet akár kizárólag az adatfeldolgozó által is – azaz nagyon kevés adatkezelői iránymutatással, vagy épp anélkül – ezekben az esetekben azonban a választott eszközöknek az adatkezelés céljának elérésére szolgáló okszerű módszert kell megtestesíteniük, és az adatkezelőt teljes mértékben informálni kell a választott eszközökről.

Abban az esetben tehát, ha bármelyik fél maga határozza meg az adatkezelés célját, akkor ez a fél biztosan önálló, vagy a más ilyen döntést hozó féllel közös adatkezelőnek minősül. Az elkülönítés abban az esetben ütközik nehézségekbe, ha az adatkezelés célját az egyik fél határozza meg önállóan, míg annak eszközeit vagy kizárólag a másik fél, vagy a felek közösen határozzák meg.

Önmagában attól, hogy az adatkezelés egyes eszközeinek meghatározását az adatkezelő az adatfeldolgozóra bízza, az adatfeldolgozó nem válik adatkezelővé. A gyakorlatban azonban sokszor előfordul, hogy az adatkezelési eszközök meghatározása már visszahat az adatkezelés lényegi elemeire is. Így például amennyiben az adatfeldolgozó az adatkezelés eszközeinek meghatározása révén tényleges befolyást gyakorol arra, hogy az adatkezelés mely adatokra terjed ki, azokat milyen időtartamban őrzik meg, vagy mely harmadik felek férhetnek hozzá az adatokhoz, akkor az adatfeldolgozó valójában adatkezelői szerepet tölt be és a felelőssége is ennek a ténynek megfelelően alakul.

Azt tehát, hogy egy társaság adatfeldolgozónak vagy (közös) adatkezelőnek minősül-e, nem kizárólag az adatkezelők, illetőleg az adatkezelő és az adatfeldolgozó között szerződéses rendelkezések alapján, hanem funkcionálisan, a tényleges ténybeli körülmények figyelembevételével kell megállapítani.

2. Közös adatkezelés elhatárolása a többes önálló adatkezeléstől

A közös adatkezelés fogalmát nemcsak az adatfeldolgozástól, hanem a többnyire egymással összefüggésben, egymásra tekintettel történő ún. többes önálló adatkezeléstől is el kell határolni. Ilyennek tekinthető például, ha egy közösen használt adatbázisban található adatokat egy Társaságcsoporton belül a különböző entitások egymásra tekintettel, de a megfelelő jogalap birtokában egymástól elkülönülő célokra használnak.

A közös adatkezelés központi eleme a cél „másokkal együtt” történő meghatározása, azaz, hogy adatkezelőként több alany, autonóm döntés eredményeként, de együttesen határozza meg az adatkezelés célját és eszközeit, illetve azok lényegi elemeit. A „többes” önálló adatkezelésekkel szemben az az elhatárolási szempont, hogy itt nincs meg az adatkezelési folyamatban az egymást kiegészítő jelleg, nem ugyanazon cél érdekében történő együtt döntésről van szó, hanem különálló adatkezelési célokról, melyet minden egyes adatkezelő önállóan maga határoz meg.

Önmagában tehát annak ténye, hogy több adatkezelő egymásra tekintettel dönt az adatkezelési célokkal és eszközökkel kapcsolatban, nem alapozza meg közös adatkezelőnkén} minősülésüket, mivel fennáll akár annak lehetősége is, hogy mindannyian önálló adatkezelőnek minősülnek.

Az elhatárolás itt is funkcionális alapon történik, azaz a közös adatkezelés típusainak széles köre merülhet fel. Az egyes adatkezelők köz} egyszerű kooperáció ténye nem elegendő ahhoz, hogy ezek a szereplők közös adatkezelőnek minősüljenek, amennyiben például ez adatcserét jelent a felek között anélkül, hogy azonos cél vezetné őket, vagy az eszközök lényeges elemeit együtt határoznák meg.

A megítélés azonban változna, amennyiben ezek az adatkezelők közösen hoznának létre egy megosztott infrastruktúrát (például közös adatbázist) saját önálló céljaikra, mivel ebben az esetben az eszközök lényeges elemeit együttesen határozzák meg, így közös adatkezelőnek minősülnének.

3. A státuszok beazonosítása összetett adatkezelési együttműködések esetén

Jellemzően azonban több adatvédelmi műveletből álló összetett adatkezelési folyamat megvalósítására irányul az együttműködés, amelyben

1. több egymásra épülő adatkezelési művelet,
2. akár több párhuzamos és/vagy egymással kapcsolódó adatkezelési cél

rendszerében kell a résztvevő felek státuszát meghatározni és ennek megfelelően a közöttük létrejövő szerződés tartalmát kialakítani.

Amennyiben az együttműködés több különböző adatkezelési cél megvalósítását szolgálja, a szereplők státusza a felek együttműködésének tárgyát képező minden egyes adatkezelési cél kapcsán külön–külön állapítandó meg.

4. Az adatvédelmi státusznak megfelelő szerződéses tartalom kialakítása

Közös adatkezelés és adatfeldolgozási együttműködés esetén a GDPR értelmében az együttműködő felek kötelesek írásbeli szerződést kötni.

A közös adatkezelőkre vonatkozóan a GDPR előírja, hogy azok átlátható módon, a közöttük létrejött írásbeli megállapodásban határozzák meg a kötelezettségeik teljesítéséért fennálló felelősségük megoszlását (kivéve, ha azt – eltérést nem engedő – jogszabály rögzíti).

A megállapodásban különösen egyértelműsíteni kell, hogy a felek milyen módon biztosítják az érintetti jogok, így például a tájékoztatáshoz (hozzáféréshez), az adathordozhatósághoz vagy az elfeledtetéshez való jog gyakorlását, a megállapodás feltételeitől függetlenül azonban az Érintett mindegyik adatkezelő vonatkozásában és mindegyik adatkezelővel szemben gyakorolhatja a GDPR szerinti jogait. A megállapodás lényegét az Érintettek rendelkezésére kell bocsátani.

Tekintettel arra, hogy a GDPR a fentiek szerint az adatfeldolgozói szerződések számos kötelező tartalmi elemét előírja, a Társaság a közös adatkezelői szerződést az alábbi felhasználási módokkal alkalmazhatja:

- a szerződésminta kiegészítő jelleggel alkalmazható az adatfeldolgozói szerződésnek minősülő korábban megkötött szerződések esetén;
- a jövőben kötendő adatfeldolgozói szerződések esetén ennek elemei beépíthetők magába a szerződésbe vagy mellékletként a szerződéshez csatolható.

Adatfeldolgozási együttműködés nem csupán a felek megállapodása alapján jöhet létre, ugyanis az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. Ennek megfelelően az adatkezelő és adatfeldolgozó közötti jogviszony egyes elemeit nemcsak szerződés, de például jogszabály is meghatározhatja.

A GDPR szerint az adatfeldolgozóval kötendő szerződés vonatkozásában az alábbi kötelező elemeket szükséges rögzíteni:

1. annak előírását, hogy az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli (kivéve: ha az adatkezelést az adatfeldolgozóra alkalmazandó jogszabály írja elő; ebben az esetben erről a jogszabályi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja);
2. az adatfeldolgozó biztosítja azt, hogy a személyes adatok kezelésére általa feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

3. az adatfeldolgozó köteles megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy a kockázattal arányos szintű adatbiztonságot garantálja;
4. az adatfeldolgozó további adatfeldolgozót kizárólag az adatkezelő írásbeli (eseti vagy általános) felhatalmazása alapján vehet igénybe;

E. az adatfeldolgozó az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

6. az adatfeldolgozó köteles segíteni az adatkezelőt az adatkezelés biztonságával, az adatvédelmi incidens bejelentésével, az érintett tájékoztatásával, az adatvédelmi hatásvizsgálattal és az előzetes konzultációval kapcsolatos kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
7. az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján az adatfeldolgozó minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha jogszabály az személyes adatok tárolását írja elő;
8. az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely a fenti kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Tekintettel arra, hogy a GDPR a fentiek szerint az adatfeldolgozói szerződések számos kötelező tartalmi elemét előírja, a Társaság az adatfeldolgozói szerződést, az alábbi felhasználási módokkal alkalmazhatja:

1. a szerződésminta kiegészítő jelleggel alkalmazható az adatfeldolgozói szerződésnek minősülő korábban megkötött szerződések esetén;
2. a jövőben kötendő adatfeldolgozói szerződések esetén ennek elemei beépíthetők magába a szerződésbe vagy mellékletként a szerződéshez csatolható.

5. Adatfeldolgozó igénybevétele esetén figyelembe veendő további szempontok

A Társaság kizárólag olyan adatfeldolgozókat vesz igénybe, akik, vagy amelyek megfelelő garanciákat nyújtanak a GDPR követelményeinek való megfelelés, és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Ezen garanciák meglétéről és fenntarthatóságáról az adatkezelőnek meg kell győződnie és már a kiválasztási folyamat során olyan minimumkövetelményeket kell meghatározni az adatfeldolgozóval szemben, amelyek biztosítják a garanciák fennállását.

A Társaság minden szükséges intézkedést megtesz adatfeldolgozóival szemben, amelyek alapján az adatfeldolgozók biztosítják különösen:

1. az érintettek jogainak védelmét és az adatok biztonságát szolgáló megfelelő technikai és szervezési intézkedések végrehajtását, ehhez megfelelő szakértelemmel és erőforrásokkal rendelkeznek;
2. a beépített és az alapértelmezett adatvédelem elveinek érvényesülését, azaz a megoldásaikat, folyamataikat az adatvédelmi szempontok figyelembe vételével alakították ki, a megfelelőség fenntartásáról gondoskodnak;

3. az adatkezelő utasításainak megfelelő határidőn belüli végrehajtására felkészültek;
4. az adatkezelési műveletekben résztvevő alkalmazottjaik megfelelő titoktartást vállalnak;
E. adott esetben az adatok biztonságát szolgáló megfelelő tanúsítvánnyal rendelkeznek, megfelelő magatartási kódexhez csatlakoztak;
6. közreműködnek az érintettek jogainak teljesítésében;
7. lehetővé teszik a fentieknek az adatkezelő általi ellenőrzését.

Az adatfeldolgozó köteles gondoskodni arról, hogy az általa feljogosított azon személyek, akik a személyes adatokhoz hozzáférnek, megfelelő tartalmú titoktartási kötelezettséget vállaljanak.

Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása alapján veheti igénybe további adatfeldolgozó közreműködését. Ennek megfelelően ellenőrizendő, hogy az adatfeldolgozó ténylegesen vesz–e igénybe további adatfeldolgozót, amennyiben igen, a felhatalmazás rendelkezésre áll–e.

6. Az adatkezelő és az adatfeldolgozó felelőssége

Az adatkezelésben érintett valamennyi adatkezelő felelősséggel tartozik minden olyan kárért, amelyet a GDPR rendelkezéseit 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.

A fentiekre tekintettel az adatfeldolgozói tevékenység fennállásának teljes időszakában biztosítani kell egy olyan belső működést, amely bizonyíthatóvá teszi az adatfeldolgozó számára adott utasítások időpontját, tartalmát és teljesítését. Ezen utasítások a GDPR értelmében kizárólag írásban adhatók (e– mailben, ún. hibajegy kezelő rendszerben vagy bármely más írásbeli formában).

XIII. NEMZETKÖZI ADATTOVÁBBÍTÁS

Harmadik országba személyes adatot továbbítani, kizárólag az alábbi esetekben lehet:

1. Bizottság megfelelőségi határozata

Személyes adatokat EGT államok területén kívülre, elsődlegesen az EU Bizottság megfelelőségi határozata alapján lehet. A Bizottság akkor hoz megfelelőségi határozatot, ha a Bizottság megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.

A határozat meghozatalához a Bizottság a következő tényezőket mérlegeli:

1. jogállamiság kritériumai (az emberi jogok és alapvető szabadságok tiszteletben tartása, adatvédelmi szabályok, hatékony jogorvoslat stb.),
2. létezik-e egy vagy több független és hatékonyan működő felügyeleti hatóság,
3. nemzetközi kötelezettségei vagy egyéb, jogilag kötelező erejű egyezményekből vagy jogi eszközökből, valamint többoldalú vagy regionális rendszerekben való részvételéből eredő – különösen a személyes adatok védelmével kapcsolatos – kötelezettségei.

2. Bizottság megfelelőségi határozat hiányában, megfelelő garanciák alapján

A Társaság vagy az adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat EGT-n kívüli államokba, ha a Társaság vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.

Megfelelő garancia alapján az adattovábbítás történhet a hatóság engedélyével vagy engedélye nélkül is:

- Hatóság engedélye nélkül: kötelező erejű vállalati szabályok, általános adatvédelmi kikötések, jóváhagyott magatartási kódex vagy jóváhagyott tanúsítási mechanizmus által), vagy
- Hatóság engedélyével: Társaság és harmadik országbeli Társaság, feldolgozó vagy címzett között létrejött szerződéses rendelkezések vagy közigazgatási megállapodásba beillesztett rendelkezések.

3. Egyedi helyzetekben biztosított eltérések

Megfelelőségi határozat és megfelelő garanciák nélkül abban az esetben lehet személyes adatot továbbítani, ha az alábbi feltételek közül legalább egy teljesül:

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy a kockázatokról tájékoztatták,
- az adattovábbítás az érintett és a Társaság között szerződés teljesítéséhez, szerződés megkötéséhez,
- az adattovábbítás fontos közérdekből szükséges,
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges,
- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az
- érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására,
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja.

4. Egyéb feltételek teljesülése esetén

Ha az adattovábbítás nem alapulhat megfelelőségi határozaton, nem állnak rendelkezésre megfelelő garanciák és a különleges helyzetekre vonatkozó eltérések egyike sem alkalmazandó, akkor a harmadik országba történő adattovábbítás csak akkor történhet, ha:

1. ha az adattovábbítás nem ismétlődő,
2. korlátozott számú érintettre vonatkozik,
3. a Társaság kényszerítő erejű jogos érdekében szükség, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és
4. a Társaság az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében.

Ilyen esetekben a Társaságnak tájékoztatnia kell a felügyeleti hatóságot az adattovábbításról.

5. Az uniós jog által nem engedélyezett továbbítás és közlés

Valamely harmadik ország bíróságának ítélete vagy közigazgatási hatóságának döntése, ami valamely Társaság vagy adatfeldolgozó számára személyes adatok továbbítását vagy közlését írja elő, kizárólag akkor ismerhető el vagy hajtható végre, ha az adattovábbítás a két ország közötti hatályos nemzetközi megállapodáson alapul (pl. jogsegélyszerződés).

A Társaság nem továbbít személyes adatokat 3. országba.

XIV. ADATVÉDELMI HATÁSVIZSGÁLAT

A GDPR rendelet az alábbi esetekben írja elő az adatvédelmi hatásvizsgálat lefolytatását:

1. nyilvános helyek nagymértékű és módszeres megfigyelése,
2. különleges személyi adatok nagy számban történő kezelése,
3. automatizált adatkezelésen alapuló személyes adatok módszeres és kiterjedt értékelése, ideértve a profilalkotást is, ha erre alapulva joghatással bíró és természetes személyt jelentős mértékben érintő döntések épülnek.
4. és minden olyan adatkezelés tekintetében, amelyek valószínűsíthetően magas kockázattal járnak.

Az adatvédelmi hatásvizsgálat lényegében egy eszköz a Társaság számára, az adatvédelmi megfelelőség kialakítására és igazolására. Eredményeként elkészíti a kockázatmérséklési tervezetet.

Az adatvédelmi hatásvizsgálatban a Társaság

- lefekteti, milyen adatkezelési műveleteket tervez és milyen célból,
- a célok figyelembevételével elvégezi az adatkezelési műveletek szükségességi és arányossági vizsgálatát,
- mérlegeli az érintettek jogaira gyakorolt kockázatokat,
- majd a feltárt kockázatok kivédésére alkalmazott intézkedéseket mutatja be.

A Társaság adatvédelmi hatásvizsgálatot nem végzett.

XV. JOGORVOSLATOK

1E.1. A panasz (Adatvédelmi tisztviselőhöz fordulás)

Amennyiben a Társaságtól adatkezelésével kapcsolatban az érintettnek problémája van, lehetősége van közvetlenül az ügyvezetőhöz fordulni panaszával.

1E.2. Bírósághoz fordulás joga

Az érintett a jogainak megsértése esetén a Társaság ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. Minden olyan személy, aki az adatvédelmi rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért a Társaságtól vagy az adatfeldolgozótól kártérítésre jogosult.

Az adatfeldolgozó csak abban az estben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a jogszabályban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha a Társaság jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.

Ha több Társaság vagy több adatfeldolgozó vagy mind a Társaság, mind az adatfeldolgozó érintett ugyanabban az adatkezelésben és felelősséggel tartozik az adatkezelés által okozott károkért, minden egyes Társaság vagy adatfeldolgozó egyetemleges felelősséggel tartozik a teljes kárért.

A Társaság vagy az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

1E.3. Adatvédelmi hatósági eljárás

Az érintett panaszával a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat:
Név: Nemzeti Adatvédelmi és Információszabadság Hatóság
Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Levelezési cím: 1530 Budapest, Pf.: 5.
Telefon: 06-1-391-1400
E-mail: ugyfelszolgalat@naih.hu
Honlap: www.naih.hu

XVI. ZÁRÓ RENDELKEZÉSEK

1. A Szabályzat megállapítása és módosítása

A Szabályzat megállapítására és módosítására a Társaság ügyvezetője jogosult. Az Adatkezelési Szabályzat 2019. május 22. napján lép hatályba és visszavonásig érvényes. Az Adatkezelési Szabályzat hatályba lépésével minden olyan korábban hatályos belső szabályzat, illetve munkáltatói utasítás hatályát vesz}, amelynek figyelembevételével a Társaság az Adatkezelési Szabályzat hatálya alá személyes adatokat kezelték.

Az Adatkezelési Szabályzat hatályba lépésének fordulónapjával bezárólag minden évben legalább egyszer felülvizsgálatra kerül, azzal, hogy a felülvizsgálat valamennyi melléklet tartalmára is maradéktalanul kiterjed. Amennyiben szükséges, az ügyvezető, mint a Társaságnál kijelölt, a felülvizsgálatért felelős tisztviselő a jogszabályi és a belső szervezeti változásoknak megfelelően intézkedik az Adatkezelési Szabályzat megfelelő módosítása iránt, gondoskodik a módosított Adatkezelési Szabályzat hatályba léptetéséről és kihirdetéséről, valamint arról, hogy az Adatkezelési Szabályzat személyi hatálya alá tartozó személyek a módosítások tartalmáról tudomást szerezzenek.

2. Intézkedések a szabályzat megismertetése

E Szabályzat rendelkezéseit meg kell ismertetni a Társaság valamennyi munkavállalójával (foglalkoztatottjával), és a munkavégzésre irányuló szerződésekben elő kell írni, hogy betartása és érvényesítése minden munkavállaló (foglalkoztatott) lényeges munkaköri kötelezettsége.

Az Adatkezelési Szabályzat rá irányadó szabályainak megismerése és betartása a Társaság minden képviselője, tisztségviselője és megbízottja számára kötelező, feladataikat kötelesek az Adatkezelési Szabályzat előírásainak maradéktalan betartásával ellátni.

Jogszabályváltozás esetén, továbbá a jelen szabályzat egyéb okból történő módosítása esetén a Tájékoztatót a jogszabályi változás alapulvételével, illetve egyéb okból módosítani lehet szükséges. Az Érintettekkel meg kell ismertetni a módosítás szövegét a helyben szokásos módon és a jelen szabályzat közlésével azonos módon.

Jelen Szabályzat a Társaság adatkezelési tevékenységének belső szabályait tartalmazza

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETÉNEK – (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) és a
- 2018. évi XIII. törvény az információs önrendelkezési jogról és az információszabadságról (Infótv) módosításnak való megfelelés céljából.

A Szabályzat megállapítása és módosítása az ügyvezető hatáskörébe tartozik.

Hatályos, 2025. október 22.

_____