EURO-FINANZ-SERVICE ZRT

EFS Euro Finanz Service Biztosításközvetítő Zártkörűen Működő Részvénytársaság

Adatkezelési Tájékoztató és
Adatvédelmi és Adatbiztonsági Szabályzat

SZÁMA: 9/2025

EFS Euro Finanz Service Zrt
Cg.: 01-10-046631
1074ut Budapest, Dohány utca 12-14.

Hatályba lépés napja: 2025.05.01.

TARTALOMJEGYZÉK

I. A szabályzat tárgya és célja

1. A jelen szabályzat az EFS Euro Finanz Service Biztosításközvetítő Zártkörűen Működő Részvénytársaságnak (továbbiakban: „**Társaság**") az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről – (a továbbiakban: „**GDPR**") – valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: „**Info tv.**") rendelkezéseinek megfelelően elkészített adatvédelmi és adatbiztonsági szabályzata (a továbbiakban: „**Szabályzat**").

2. A Szabályzat célja, hogy a személyes adatok védelméhez fűződő jogok érvényesülése és a Társaság által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a szervezeten belüli személyes adatok védelmének és kezelésének szabályait, a személyes adatok biztonságára vonatkozó követelményeket, valamint ennek megfelelően biztosítsa a GDPR és az Info tv. előírásainak és valamennyi egyéb, a személyes adatok védelmére és biztonságára vonatkozó előírásoknak a Társaság szervezetén belüli maradéktalan érvényesülését a Társaság által folytatott tevékenység során.

II. Értelmező rendelkezések

A Szabályzatban szereplő alábbi fogalmak a következő jelentéstartalommal bírnak:

Adatállomány: az egy nyilvántartásban kezelt adatok összessége;

Bit.: a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény;

Hpt.: a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény.

Munkatárs: a Társaság vezető tisztségviselője, cégvezetője, munkavállalója;

Megbízott: valamennyi olyan megbízott, alvállalkozó, ügynök, illetve egyéb közreműködő, aki a Társaság nevében vagy érdekében – közvetlenül vagy közvetve – adatkezelést vagy adatfeldolgozást végez;

Megbízotti Munkatárs: a Megbízott vezető tisztségviselője, cégvezetője, munkavállalója;

NAIH: Nemzeti Adatvédelmi és Információszabadság Hatóság.

III. A Szabályzat hatálya és kapcsolata egyéb belső szabályzatokkal

3.1 *Személyi hatály*

3.1.1 A Szabályzat személyi hatálya kiterjed a Társaság valamennyi szervezeti egységére, Munkatársára és Megbízottjára.

3.1.2 A Társaság csak olyan Megbízottat vehet igénybe, aki a jelen Szabályzatot a szerződéses jogviszony létesítésekor kötelezőnek fogadja el magára nézve, és vállalja, hogy valamennyi Megbízotti Munkatárs a Szabályzatban foglalt rendelkezéseknek megfelelően jár el a Társaság megbízásából vagy érdekében végzett adatkezelési vagy adatfeldolgozási tevékenysége során.

3.1.3 A Társaság ügyvezetésének biztosítania kell, hogy a jelen Szabályzat hatályba lépésekor a Társaság Megbízottjának minősülő személy a jelen Szabályzatot haladéktalanul megismerje, és valamennyi Megbízotti Munkatárssal megismertesse, magára nézve kötelezőnek fogadja el, valamint biztosítsa, hogy valamennyi Megbízotti Munkatárs a Szabályzatban foglalt szabályoknak megfelelően jár el a Társaság megbízásából vagy érdekében végzett adatkezelési vagy adatfeldolgozási tevékenysége során.

3.2 Tárgyi hatály

3.2.1 A Szabályzatban foglaltakat kell alkalmazni valamennyi olyan tevékenység során, ahol természetes személyek ***személyes adat***ainak a kezelésére (***adatkezelés***) vagy feldolgozására (***adatfeldolgozás***) kerül sor, függetlenül attól, hogy azt manuálisan, illetve teljesen vagy részben automatizált eszközzel végzik.

Személyes adatnak minősül minden olyan adat, amely az ***érintett***el kapcsolatba hozható (pl. név, lakcím, telefonszám), valamint olyan adat, amelyből az érintettre vonatkozóan le lehet vonni bármilyen következtetést (pl. abból, hogy a lakóhelye milyen környéken található, lehet következtetni egy személynek az anyagi körülményeire vagy a végzettsége, foglalkozása alapján arra, hogy milyen jártassággal rendelkezik a hivatalos dokumentumok olvasása, értelmezése terén).

Érintett a személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható személy, amely mindig egy meghatározott személy kell, hogy legyen. Kizárólag természetes személyek minősülnek érintettnek, tehát jogi személyek nem, ezáltal az adatvédelem csak a természetes személyek adatait védi. Viszont személyes adatnak minősül például az egyéni vállalkozó vagy egy cég képviselőjének adata is (pl. telefonszáma, email címe, születési helye, ideje stb.)

Mindezek alapján személyes adatnak minősül különösen, de nem kizárólag:
- az érintett neve, lakcíme, levelezési címe, telefonszáma, email címe, személyi igazolvány száma, adóazonosító jele, valamint
- egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret (pl. vagyoni helyzet, végzettség, képmás).

Az adatkezelés során a személyes adat mindaddig megőrzi ezt a minőségét, amíg a személyes adat és az érintett közötti kapcsolat helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek. Ennek megfelelően a személyes adatok

anonimizálása mindaddig nem következik be, amíg bármilyen módon az adat az adatkezelőnél hozzákapcsolható egy adott személyhez (pl. két különálló adatbázisban levő adatok összekapcsolása révén).

Adatkezelésnek minősül bármely, az adaton végzett művelet vagy műveletek összessége, függetlenül attól, hogy milyen eljárást alkalmazunk. Így adatkezelésnek minősül különösen az adatok:

- gyűjtése, felvétele,
- rögzítése,
- rendszerezése,
- tárolása,
- megváltoztatása,
- felhasználása,
- lekérdezése,
- továbbítása,
- nyilvánosságra hozatala,
- összehangolása vagy összekapcsolása,
- zárolása,
- törlése és megsemmisítése, valamint
- az adat további felhasználásának megakadályozása,
- fénykép-, hang- vagy képfelvétel készítése, valamint
- a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Az ***adatfeldolgozás*** jelentését lásd a X. fejezet alatt.

3.3 Időbeli hatály

3.3.1 A Szabályzat **2018. május 25.** napjától hatályos. A hatályba lépéssel egyidejűleg valamennyi korábbi, ebben a tárgyban elfogadott szabályzat hatályát veszti.

3.4 A Szabályzat kapcsolata a Társaság egyéb szabályzataival

3.4.1 A Társaság egyéb, adatkezelést és adatfeldolgozást is érintő belső szabályzatát a jelen Szabályzattal összhangban kell értelmezni, figyelemmel a jelen Szabályzatban foglalt előírásokra.

3.4.2 Amennyiben a jelen Szabályzat és a Társaság egyéb szabályzata között az adatvédelmi szabályok vonatkozásában eltérés van, a jelen Szabályzat alkalmazandó.

IV. Adatvédelmi alapelvek

4.1 Célhoz kötöttség követelménye

4.1.1 Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Törvényben elrendelt adatkezelés esetén kizárólag a felhatalmazást adó törvényben meghatározott célból valósulhat meg adatkezelés.

4.1.2 Tilos a személyes adatok „készletre" való gyűjtése, vagyis amelyek nem köthetők valamilyen adatkezelési célhoz, de a Munkatárs, illetve a Megbízott megítélése szerint

valamilyen jövőbeni felhasználásra még jó lehet. Ebben az esetben ugyanis sérül a célhoz kötöttség követelménye.

4.1.3 A Társaság által vagy annak érdekében kezelt személyes adat magáncélra való felhasználása tilos.

4.1.4 Kizárólag olyan személyes adat kezelhető, amely az adatkezelés céljához elengedhetetlen, és a cél elérésére alkalmas. Ezeket az adatokat csak a cél megvalósulásához szükséges mértékben és ideig lehet kezelni.

4.1.5 Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának.

4.2 Adatkezeléshez megfelelő jogalap megléte

4.2.1 A személyes adatok védelméhez való jog a természetes személyek Alaptörvényben biztosított alapjoga, amely garantálja az adatalanyok információs önrendelkezési jogát. Az információs önrendelkezési jog az érintettek hozzájárulása hiányában kizárólag törvényi felhatalmazás alapján korlátozható.

4.2.2 Az információs önrendelkezési jog tiszteletben tartása érdekében személyes adatot csak a GDPR és az Info tv. rendelkezéseinek megfelelő jogalap fennállása esetén lehet kezelni, elsősorban akkor, ha erre törvényi felhatalmazás van vagy ahhoz az érintett kifejezetten hozzájárult.

Különleges adatnak minősül minden olyan személyes adat, amely
- a faji eredetre,
- a nemzetiséghez tartozásra,
- a politikai véleményre vagy pártállásra,
- a vallásos vagy más világnézeti meggyőződésre,
- az érdek-képviseleti szervezeti tagságra,
- a szexuális életre,
- genetikai adatra,
- biometrikus adatra,
- az egészségi állapotra,
- a kóros szenvedélyre vonatkozik, valamint
- a ***bűnügyi személyes adat***.

Bűnügyi személyes adat alatt a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adatot értjük.

Ha a személyes adatot nem az érintett bocsátja az adatkezelő rendelkezésére, akkor az adatot megadó személytől kell megkövetelni annak hitelt érdemlő igazolását, hogy az adatok adatkezelő általi kezeléséhez az érintett hozzájárulását beszerezte.

4.2.3 Az érintett hozzájárulása abban az esetben megfelelő, amennyiben a hozzájárulás önkéntes, határozott és megfelelő tájékoztatáson alapul, mellyel az érintett

félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. Ha az érintett hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell előadni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel.

4.2.4 A különleges adat kezelésére vonatkozó hozzájárulásnak minden esetben írásbelinek kell lennie, míg a személyes adat kezelésére vonatkozó hozzájárulásnak is elsősorban írásban vagy egyéb bizonyítható módon (pl. panaszügyintézés során hangrögzítéssel) kell megtörténnie. Amennyiben bármely személyes vagy különleges adat kezelése kapcsán a Társaság írásbeli hozzájárulás mintát készített és bocsátott a Munkatárs, illetve a Megbízott rendelkezésére, akkor a hozzájárulás beszerzésekor a Munkatársnak, illetve a Megbízottnak az adott mintát kell használnia. Ha az érintettnek bármilyen észrevétele vagy kérdése van a hozzájárulás minta szövegével vagy az adatvédelmi tájékoztatóval kapcsolatban, amelyet a Munkatárs, illetve a Megbízott nem tud megválaszolni vagy az érintett a hozzájárulás minta szövegét módosítani kívánja, akkor a Munkatárs, illetve a Megbízott köteles az érintett kérdéseit, észrevételeit vagy módosítási igényét egyeztetni a Társaság adatvédelmi felelősével.

4.2.5 Személyes adat kivételesen az érintett hozzájárulása hiányában is kezelhető, ha a személyes adat kezelése

a) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges; vagy
b) az adatkezelőre vonatkozó jogi kötelezettség teljesítése céljából szükséges, vagy
c) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából szükséges, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

A jelen pont b) és c) alpontban említett jogalap alapján történő adatkezelés ügyében – a belső adatvédelmi felelős írásbeli véleményének ismeretében – kizárólag a Társaság Igazgatósága jogosult dönteni.

4.2.6 Ha a személyes adat felvételére az érintett hozzájárulásával került sor, a felvett adatokat törvény eltérő rendelkezésének hiányában az adatkezelő

a) a rá vonatkozó jogi kötelezettség teljesítése céljából, vagy
b) az adatkezelő vagy harmadik személy jogos érdekének érvényesítése céljából, ha ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll további külön hozzájárulás nélkül, valamint az érintett hozzájárulásának visszavonását követően is kezelheti.

A jelen pontban említett jogalap alapján történő adatkezelés ügyében kizárólag a Társaság Igazgatósága – a belső adatvédelmi felelős írásbeli véleményének ismeretében – jogosult dönteni.

4.2.7 Amennyiben a személyes adat kezelésének alapjául szolgáló jogalap tekintetében kérdés vagy vita merül fel, akkor a Munkatárs, illetve a Megbízott köteles ez ügyben a Társaság adatvédelmi felelősével egyeztetni.

4.3 Megfelelő tájékoztatás követelménye

4.3.4 Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés hozzájáruláson alapul, a szerződés teljesítéséhez szükséges vagy kötelező. A Munkatárs, illetve a Megbízott köteles az érintettet az adatkezelés megkezdése előtt tájékoztatni a személyes adatai kezelésére vonatkozó minden tényről, ideértve különösen, de nem kizárólag

- a kezelt adatokról, illetve azok forrásáról;
- az adatkezelés céljáról és jogalapjáról;
- az adatkezelő nevéről és címéről, webcíméről, egyéb elérhetőségeiről (pl. email cím);
- az adatfeldolgozásra jogosult személyek nevéről, címéről és adatkezeléssel összefüggő tevékenységéről;
- az adatkezelés időtartamáról;
- arról, ha az érintett személyes adatait az adatkezelő a hozzájárulás visszavonása esetén a 4.2.6. pont alapján kezeli;
- arról, hogy kik ismerhetik meg az adatokat;
- az érintett személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről;
- az érintett adatkezeléssel kapcsolatos jogairól és jogorvoslati lehetőségeiről, és azokról az elérhetőségről, ahova az érintett fordulhat, amennyiben jogait érvényesíteni akarja (Társaság levelezési címe, email címe, NAIH elérhetőségei).

4.3.5 Amennyiben bármely adatkezelés kapcsán a 4.3.4. pontban foglaltakról a Társaság írásbeli adatvédelmi tájékoztatót készített és bocsátott a Munkatárs, illetve a Megbízott rendelkezésére, akkor a tájékoztatási kötelezettségnek mindenkor az adatvédelmi tájékoztató az érintettnek való átadásával vagy megküldésével köteles a Munkatárs, illetve a Megbízott eleget tenni. A tájékoztatót az adatkezelés megkezdése előtt kell átadni az érintettnek, és megfelelő időt kell biztosítani arra, hogy azt átolvassa. Amennyiben az érintett a tájékoztatóban foglaltakkal kapcsolatban felvilágosítást kér, azt részére meg kell adni.

4.4 Törvényes és tisztességes adatkezelés

4.4.1 Az adatok felvételének és kezelésének mindenkor tisztességesnek és törvényesnek kell lennie.

4.4.2 A Társaság valamennyi adatkezelést vagy adatfeldolgozást végző Munkatársa, illetve Megbízottja felelősséggel tartozik azért, ide értve, de nem kizárólagosan a kártérítési, szabálysértési és büntetőjogi felelősséget is, hogy valamennyi a Társaság nevében és érdekében végzett tevékenységük során a személyes adatokat jogszerűen, a vonatkozó jogszabályi előírásoknak és a jelen Szabályzatban foglaltaknak megfelelően kezelje, illetve dolgozza fel.

4.5 Személyes adatok pontossága és teljessége

4.5.1 Amennyiben bármely Munkatárs, illetve Megbízott tudomására jut, hogy az általa kezelt adat hibás, hiányos vagy nem naprakész, akkor köteles azt helyesbíteni vagy köteles az adat helyesbítését az arra jogosult Munkatársnál, illetve Megbízottnál kezdeményezni.

V. Biztosítási titok és a banktitok megőrzésének kötelezettsége, ezzel kapcsolatos adatok kezelése

5.1 Biztosítási titok

5.1.1 A kezelt személyes adatok bizonyos esetekben a Bit. szerinti biztosítási titoknak minősülhetnek.

> ***Biztosítási titok***nak minősül minden olyan - minősített adatot nem tartalmazó -, a biztosító, a viszontbiztosító, a biztosításközvetítő rendelkezésére álló adat, amely a biztosító, a viszontbiztosító, a biztosításközvetítő ***ügyfeleinek*** - ideértve a károsultat is - személyi körülményeire, vagyoni helyzetére, illetve gazdálkodására vagy a biztosítóval, illetve a viszontbiztosítóval kötött szerződéseire vonatkozik.
>
> Ebből a szempontból ***ügyfél***nek minősülnek az alábbi személyek: a szerződő, a biztosított, a kedvezményezett, a károsult, a biztosító számára szerződéses ajánlatot tett és a biztosító szolgáltatására jogosult más személy, továbbá a független biztosításközvetítő esetében az a személy is, aki a független biztosításközvetítővel alkuszi megbízási szerződést kötött.

5.1.2 A biztosításközvetítő az ügyfelek azon biztosítási titkait jogosult kezelni, amelyek a biztosítási szerződéssel, annak létrejöttével, nyilvántartásával, a szolgáltatással összefüggnek. Az adatkezelés célja csak a biztosítási szerződés megkötéséhez, módosításához, a biztosítás fenntartásához, a biztosítási szerződésből származó követelések megítéléséhez szükséges, vagy a Bit. által meghatározott egyéb cél lehet. Az ettől eltérő célból végzett adatkezelést a biztosításközvetítő csak az ügyfél előzetes hozzájárulásával végezhet. A hozzájárulás megtagadása miatt az ügyfelet nem érheti hátrány és annak megadása esetén részére nem nyújtható előny.

5.1.3 A biztosítási titok tekintetében, időbeli korlátozás nélkül - ha törvény másként nem rendelkezik - titoktartási kötelezettség terheli a biztosításközvetítő tulajdonosait, vezetőit, alkalmazottait és mindazokat, akik ahhoz a biztosításközvetítővel kapcsolatos tevékenységük során bármilyen módon hozzájutottak.

5.1.4 A Bit. rendelkezései alapján a biztosításközvetítő

a) a személyes adatokat a biztosítási, viszontbiztosítási, illetve a megbízási jogviszony fennállásának idején, valamint azon időtartam alatt kezelheti, ameddig a biztosítási, viszontbiztosítási, illetve a megbízási jogviszonnyal kapcsolatban igény érvényesíthető;

b) a létre nem jött biztosítási szerződéssel kapcsolatos személyes adatokat kezelhet, ameddig a szerződés létrejöttének meghiúsulásával kapcsolatban igény érvényesíthető;

c) köteles törölni minden olyan, ügyfeleivel, volt ügyfeleivel vagy létre nem jött szerződéssel kapcsolatos személyes adatot, amelynek kezelése esetében az adatkezelési cél megszűnt, vagy amelynek kezeléséhez az érintett hozzájárulása nem áll rendelkezésre, illetve amelynek kezeléséhez nincs törvényi jogalap.

5.2 Banktitok

5.2.1 A kezelt személyes adatok bizonyos esetekben a Hpt. szerinti banktitoknak minősülhetnek.

Banktitoknak minősül minden olyan, az egyes ***ügyfelek***ről a pénzügyi intézmény vagy annak közvetítője rendelkezésére álló tény, információ, megoldás vagy adat, amely ügyfél személyére, adataira, vagyoni helyzetére, üzleti tevékenységére, gazdálkodására, tulajdonosi, üzleti kapcsolataira, valamint a pénzügyi intézmény által vezetett számlájának egyenlegére, forgalmára, továbbá a pénzügyi intézménnyel vagy közvetítőjével kötött szerződéseire vonatkozik.

Ebből a szempontból ***ügyfél***nek minősül mindenki, aki (amely) a pénzügyi intézménytől pénzügyi szolgáltatást vesz igénybe. A banktitokra vonatkozó szabályokat alkalmazni kell arra a személyre is, aki szolgáltatás igénybevétele céljából lép kapcsolatba a pénzügyi intézménnyel vagy annak közvetítőjével, de a szolgáltatást nem veszi igénybe.

5.2.2 A banktitkot időbeli korlátozás nélkül meg kell őrizni.

5.2.3 A Hpt. rendelkezései szerint a pénzügyi közvetítő:

a) köteles törölni minden olyan, ügyfeleivel, volt ügyfeleivel vagy létre nem jött szerződéssel kapcsolatos személyes adatot, amelynek kezelése esetében az adatkezelési cél megszűnt, vagy amelynek kezeléséhez az érintett hozzájárulása nem áll rendelkezésre, illetve amelynek kezeléséhez nincs törvényi jogalap;

b) a létre nem jött szolgáltatási szerződéssel kapcsolatos banktitkot képező ügyféladatokat, személyes adatokat addig kezelheti, ameddig a szerződés létrejöttének meghiúsulásával kapcsolatban igény érvényesíthető. Az igényérvényesítés szempontjából - törvény eltérő rendelkezése hiányában - a Polgári Törvénykönyvről szóló 2013. évi V. törvényben meghatározott általános elévülési idő az irányadó.

VI. Az érintett jogainak érvényesítése, a tiltakozási jog gyakorlása és az azokkal összefüggő feladatok

6.1 Érintettek jogai

6.1.1 Az érintettek az alábbiakkal fordulhatnak az adataik kezelését végző személyhez:

a) tájékoztatást kérhetnek arról, hogy milyen módon kezelik a személyes adatait,
b) kérhetik személyes adatainak helyesbítését,
c) kérhetik személyes adatainak - a kötelező adatkezelés kivételével – kezelésének korlátozását vagy törlését,
d) kérhetik, hogy személyes adataikat tagolt, széles körben használt, géppel olvasható formátumban megkapják, továbbá, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsák, ha az adatkezelés hozzájáruláson, vagy szerződésen alapul és az adatkezelés automatizált módon történik,
e) tiltakozhatnak a személyes adatainak kezelése ellen.

6.1.2 Minden esetben meg kell bizonyosodni, hogy a jogai érvényesítését az arra jogosult érintett kezdeményezi, és ebben a körben kérhető, hogy az érintett szükség esetén igazolja a személyazonosságát (például személyazonosító igazolvány bemutatásával), azonban ilyen esetben is figyelembe kell venni az adatvédelmi alapelveket (IV. fejezet) és annak megfelelően kell eljárni.

6.1.3 A helyesbítésről, a korlátozásról, a megjelölésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban a személyes adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel és adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

6.1.4 Ha az érintett helyesbítés, korlátozás vagy törlés iránti kérelme nem kerül teljesítésre, az érintettel közölni kell a helyesbítés, korlátozás vagy törlés iránti kérelem elutasításának ténybeli és jogi indokait a kérelem kézhezvételét követő 25 napon belül írásban vagy az érintett hozzájárulásával elektronikus úton. Ezen kívül a helyesbítés, korlátozás vagy törlés iránti kérelem elutasítása esetén az érintettet tájékoztatni kell a bírósági jogorvoslat, továbbá a felügyeleti hatósághoz (NAIH) fordulás lehetőségéről.

6.1.5 A tájékoztatás, a helyesbítés, a korlátozás vagy a törlés csak akkor tagadható meg, ha tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban, az állam külső és belső biztonsága, így a honvédelem, a nemzetbiztonság, a bűncselekmények megelőzése vagy üldözése, a büntetés-végrehajtás biztonsága érdekében, továbbá állami vagy önkormányzati gazdasági vagy pénzügyi érdekből, az Európai Unió jelentős gazdasági vagy pénzügyi érdekéből, a bírói függetlenség és a bírósági eljárások védelme érdekében, valamint a foglalkozások gyakorlásával összefüggő fegyelmi és etikai vétségek, a munkajogi és munkavédelmi kötelezettségszegések megelőzése és feltárása céljából - beleértve minden esetben az ellenőrzést és a felügyeletet is -, az érintett vagy mások jogainak és szabadságainak védelme, továbbá polgári jogi követelések érvényesítése érdekében.

6.2 Tájékoztatáshoz való jog

6.2.1 Az érintett által kért tájékoztatást annak kézhezvételétől számított legrövidebb idő alatt, legfeljebb azonban 25 napon belül, közérthető formában, írásban kell megadni.

6.2.2 Az érintett által kért tájékoztatás ingyenes, ha a tájékoztatást kérő a folyó évben azonos adatkörre vonatkozóan tájékoztatási kérelmet még nem nyújtott be. Egyéb esetekben az adatszolgáltatásra a Társaság Igazgatósága költségtérítést állapíthat meg, amelynek fedeznie kell a tájékoztatással kapcsolatban felmerült közvetlen költségeket. A már megfizetett költségtérítést vissza kell téríteni, ha a személyes adatokat jogellenesen kezelték, vagy a tájékoztatás kérése a személyes adat helyesbítéséhez vezetett.

6.2.3 Ha nincs olyan körülmény, ami miatt a tájékoztatást meg kellene tagadni, az érintettet tájékoztatni kell a kezelt adatokról, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá - az érintett személyes adatainak továbbítása esetén - az adattovábbítás jogalapjáról és címzettjéről.

6.2.4 A tájékoztatás megtagadása esetén írásban kell közölni az érintettel, hogy a felvilágosítás megtagadására a GDPR illetve az Info tv. mely rendelkezése alapján került sor. Amennyiben kétség merül fel azzal kapcsolatban, hogy a tájékoztatás megtagadható-e, illetve annak mi a pontos jogalapja, azt kötelező a belső adatvédelmi felelőssel egyeztetni. A felvilágosítás megtagadása esetén tájékoztatni kell az érintettet a bírósági jogorvoslat, továbbá a felügyeleti hatósághoz (NAIH) fordulás lehetőségéről.

6.2.5 Az elutasított kérelmekről a belső adatvédelmi felelős nyilvántartást vezet, melyről évente a tárgyévet követő év január 31-éig köteles értesíteni a NAIH-t az Info. tv-ben meghatározottak szerint.

6.2.6 Biztosítási titoknak vagy banktitoknak minősülő személyes adatok egyes szervek vagy személyek felé való továbbításáról törvény kötelezően alkalmazandó rendelkezése alapján az érintettek bizonyos esetekben nem tájékoztathatók, ezért amennyiben biztosítási titoknak vagy banktitoknak minősülő személyes adatok továbbításáról kér az érintett tájékoztatást, a tájékoztatás megadhatósága tekintetében kötelező egyeztetni a belső adatvédelmi felelőssel.

6.3 Személyes adat helyesbítése

6.3.1 A valóságnak nem megfelelő adatot az érintett kérésére helyesbíteni kell, feltéve, hogy az ehhez szükséges adat rendelkezésre áll.

6.4 Törléshez való jog

6.4.1 A kezelt adatot ***törölni*** kell, ha

a) kezelése jogellenes;
b) az érintett kéri (ide nem értve azt, ha a személyes adat kezelését törvény rendeli el vagy arra már jogalap van);
c) az hiányos vagy téves - és ez az állapot jogszerűen nem orvosolható -, feltéve, hogy a törlést törvény nem zárja ki;
d) az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;
e) azt a bíróság vagy a NAIH elrendelte.

Személyes adat ***törlés***e alatt az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges. Ennek során az elektronikus úton tárolt adatokat olyan módon kell törölni, hogy azok helyreállítása technikailag ne legyen lehetséges, illetve a papír alapon tárolt adatokat végleges jelleggel meg kell semmisíteni olyan módon, hogy azokhoz harmadik személyek se férjenek semmilyen módon hozzá (így például iratmegsemmisítő használatával).

6.4.2 A Társaság Igazgatóságának erre vonatkozó határozata esetén törlés helyett a Társaság ***korlátozz***a a személyes adatot, ha az érintett ezt kéri, vagy ha a rendelkezésére álló információk alapján feltételezhető, hogy a törlés sértené az érintett jogos érdekeit. Az így korlátozott személyes adat kizárólag addig kezelhető, ameddig fennáll az az adatkezelési cél, amely a személyes adat törlését kizárta.

Személyes adat ***korlátozás***a alatt az adat azonosító jelzéssel ellátását értjük az adat további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

6.5 Tiltakozási jog

Tiltakozás alatt az érintett azon nyilatkozatát értjük, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri.

6.5.1 Az érintett tiltakozhat személyes adatának kezelése ellen,

- ha a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén;
- ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik; valamint
- a tiltakozás jogának gyakorlását egyéb törvény lehetővé teszi.

6.5.2 A tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül meg kell vizsgálni, annak megalapozottsága kérdésében döntést hozni, és döntésről a kérelmezőt írásban tájékoztatni. Amennyiben kétség merül fel a tiltakozási jog megalapozottságának kérdésében, kötelező a Társaság adatvédelmi felelőséhez fordulni ebben a kérdésben.

6.5.3 Ha a tiltakozás megalapozott, az adatkezelést - beleértve a további adatfelvételt és adattovábbítást is – meg kell szüntetni haladéktalanul, és az adatokat zárolni kell, valamint a tiltakozásról, továbbá az annak alapján tett intézkedésekről értesíteni kell mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbították, akik szintén kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

6.5.4 Ha az érintett a Társaság döntésével nem ért egyet, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 napon belül - bírósághoz fordulhat.

VII. A Társaság nyilvántartásaival kapcsolatos szabályozás, belső adatkezelési nyilvántartás

7.1 A Társaság a tevékenysége során egyes jogszabályok alapján, úgy a GDPR 30. cikke értelmében is, fennálló kötelezettség alapján vagy a Társaság belső működése céljából meghatározott adatkörök alapján gyűjtött adatfajtákból Adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, lekérdezhetőségét.

7.2 Biztosítani kell, hogy a nyilvántartásokban a szükséges módosítások naprakész módon megtörténjenek, és ennek megfelelően a szükséges módosítások (új adatok felvétele, adatok módosítása, helyesbítése stb.) haladéktalanul bevezetésre kerüljenek a nyilvántartásba, vagy amennyiben ez más személy feladatkörébe tartozik, haladéktalanul bejelentsék a nyilvántartást vezető személynek, aki köteles a megfelelő változásokat a nyilvántartáson átvezetni.

7.3 Az új Adatállomány kialakítását az annak kialakításáért felelős szervezeti egység vezetője, illetve – szervezeti egység hiányában – személy, köteles bejelenteni a belső adatvédelmi felelősnek. A belső adatvédelmi felelős az Adatállományt köteles a belső adatkezelési nyilvántartásba bejegyezni.

7.4 Az adatkezelési nyilvántartásba az alábbi adatfajtákat szükséges bejelenteni:

a) az adatkezelés célját,
b) az adatkezelés jogalapját,
c) az érintettek körét,
d) az érintettekre vonatkozó adatok leírását,
e) az adatok forrását,
f) az adatok kezelésének időtartamát,
g) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló adattovábbításokat is,
h) az adatkezelő, valamint az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
i) az alkalmazott adatfeldolgozás technikai és szervezési intézkedések általános leírását,
j) a belső adatvédelmi felelős alkalmazása esetén annak nevét és elérhetőségi adatait.

t.

VIII. Az adatbiztonság követelménye

8.1 Adatbiztonság alatt valamennyi olyan szervezési, technikai megoldásokat, intézkedéseket és eljárási szabályok összességét értjük, amelynek célja a személyes adatok jogosulatlan kezelésének, így különösen megszerzésének, feldolgozásának,

megváltoztatásának és megsemmisítésének megakadályozása, mellyel az adatkezelés során a kockázati tényezőket – és ezzel a fenyegetettséget – a legkisebb mértékűre lehet csökkenteni és ezzel a kockázat mértékének megfelelő szintű adatbiztonságot garantálni.

8.2 A Munkatárs, illetve a Megbízott köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét, és ebben a körben köteles betartani a Társaság, illetve annak ügyvezetése, adatvédelmi felelőse, illetve a Munkatárs a saját felettese által adott utasításokat és munkafolyamatokat.

8.3 A Társaság, valamint tevékenységi körükben a Megbízottak kötelesek gondoskodni az adatok biztonságáról, kötelesek továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani és megvalósítani azokat az eljárási szabályokat, amelyek a GDPR-ban, az Info tv-ben, a Bit.-ben és a Hpt.-ben előírt, valamint a Szabályzatban foglalt adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

8.4 Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

8.5 Papír alapú adatkezelés biztonsága:

a) *Tűz- és vagyonvédelem:* az iratokat jól zárható, tűz- és vagyonvédelemmel ellátott helyiségben kell tárolni.
b) *Hozzáférés-védelem:* az adatokhoz csak az illetékes ügyintézők és azok felettesei férhetnek hozzá, és illetéktelenek elől elzárva kell tartani, zárral védett és lezárt szekrényben vagy helyiségben. Amennyiben a helyiség, ahol az adatokat tárolják kifejezetten erre a célra lett kialakítva (pl. archív vagy irattároló szoba), a helyiség ajtajának zárhatóságáról kell gondoskodni mechanikus berendezéssel (pl. zár) vagy elektronikus berendezéssel (pl. kártyaolvasó és elektronikus ajtónyitó).

8.6 A számítógépes hálózaton tárolt adatok védelme:

a) *Biztonsági mentés:* a személyes adatokat tartalmazó Adatállományokról napi mentést kell végezni egy külső adathordozóra, amelynek őrzését biztosítani kell egy erre a célra kialakított páncéldobozban vagy széfben, tűzbiztos helyen és módon;
b) *Vírusvédelem:* a számítógépes rendszereket megfelelő vírusvédelemmel kell ellátni;
c) *Hozzáférés-védelem:* a számítógépes hálózaton kezelt személyes adatokhoz, Adatállományokhoz való hozzáférését felhasználói névvel és jelszóval kell biztosítani;
d) *Hálózati védelem:* A rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával meg kell akadályozni, hogy a hálózathoz illetéktelen személyek hozzáférhessenek;
e) *Fizikai védelem:* biztosítani kell, hogy a szervert tárolásául szolgáló szobába kizárólag az arra feljogosítottak lépjenek be, és a helyiséget zárva kell tartani, valamint korszerű tűz- és vagyonvédelmi berendezésekkel kell ellátni;

f) *Áramellátás:* a szerver(ek) áramellátását szünetmentes áramforrással kell biztosítani, amely áramszünet esetén a rendszer biztonságos, adatvesztést nem okozó leállításához szükséges ideig zavartalan továbbüzemelést biztosít.

8.7 Hozzáférés az adatokhoz

A személyes adatokhoz csak az arra jogosult és kijelölt személy férhet hozzá. Hozzáférésre jogosult csak olyan személy lehet, akinek az adatokhoz a munkája ellátásához van szükség.

8.8 Eljárás adatvesztés vagy adathordozó megsemmisülése, megrongálódása esetén

Az adatvesztés, a megrongálódás/megsemmisülés tényét annak megtörténtét vagy felfedezését követő 3 munkanapon belül jegyzőkönyvben kell rögzíteni. A jegyzőkönyv elkészítése az adatok kezeléséért felelős személy feladata. A jegyzőkönyvnek legalább az alábbi adatokat kell tartalmaznia:

- az adat és az adathordozó azonosításához szükséges adatok,
- az esemény leírása,
- az esemény történésének, illetve felfedezésének ideje,
- a felfedező és az előidéző adatai (név, beosztás, szervezeti egység, szervezet),
- adatrekonstrukció érdekében tett eljárás és annak eredménye,
- az adat kezeléséért felelős személy és annak felettesének aláírása,
- a jegyzőkönyv felvételének helye és ideje.

Az esetet jelenteni kell az adatvédelmi felelősnek, és meg kell küldeni részére a jegyzőkönyvet. Az elveszett adatokat, a megrongálódott adathordozót, amennyire lehetséges, helyre kell hozni és arról egy hiteles másolatot készíteni.

8.9 A különböző nyilvántartásokban elektronikusan kezelt Adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok - kivéve ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. Ennek megfelelően az elektronikus Adatállományokat jelszóvédelemmel kell ellátni, és biztosítani kell, hogy kizárólag az Adatállományok kezelésére jogosultak férjenek hozzá az Adatállományhoz.

8.10 A személyes adatok automatizált feldolgozása során a Társaság és a Megbízottak további intézkedésekkel kötelesek biztosítani:

a) a jogosulatlan adatbevitel megakadályozását;
b) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
c) annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbítottak vagy továbbíthatják;
d) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
e) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és

f) azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön.

8.11 A Társaságnak és a Megbízottaknak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lennie a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmet biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

8.12 A Társaság az adatvédelmi felelőse útján nyilvántartást vezet az ***adatvédelmi*** incidensekről, amely tartalmazza:

- az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát,
- a belső adatvédelmi felelős vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit,
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket, valamint
- az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Adatvédelmi incidensnek számít a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes ***megsemmisítés***ét, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Megsemmisítés alatt a személyes adatot tartalmazó adathordozó teljes fizikai megsemmisítését értjük.

A nyilvántartás vezetésének célja az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása.

8.13 Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak (NAIH), kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

8.14 Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

8.15 Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, indokolatlan késedelem nélkül tájékoztatni kell az érintettet az adatvédelmi incidensről úgy, hogy világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell a fenti 9.12 pontban említett információkat és intézkedéseket.

IX. Adatfeldolgozás

9.1 Amennyiben egyes adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzésével, vagyis ***adatfeldolgozás***sal más személy kerül megbízásra, akkor mindenkor be kell tartani a GDPR, az Info tv., a Bit., a Hpt. és a jelen Szabályzat erre vonatkozó rendelkezéseit.

Adatfeldolgozásnak minősül az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik.

Adatfeldolgozás esetén továbbra is az adatkezelő határozza meg az adatkezelés célját és hozza meg az adatkezelésre vonatkozó döntéseket, és az adatfeldolgozóval kötött szerződésben határozza meg az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit, míg az adatfeldolgozó:

- az adatkezelést érintő érdemi döntést nem hozhat,
- a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel,
- saját céljára adatfeldolgozást nem végezhet, továbbá
- a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni.

Adatfeldolgozásnak minősül – a körülményektől függően – például a bérszámfejtés, az adatrögzítés, postai szolgáltatások, futárszolgálat igénybe vétele stb.

Annak kapcsán, hogy valamely a Társaság nevében vagy érdekében végzett adatkezelési művelet adatfeldolgozásnak minősül-e, előzetes egyeztetést kell folytatni a belső adatvédelmi felelőssel.

9.2 A Társaság általi adatfeldolgozó igénybevételére vonatkozó döntést kizárólag a Társaság Igazgatósága hozhat, aki az adatvédelmi és titokvédelmi vonatkozások tekintetében köteles előzetesen a belső adatvédelmi felelőssel egyeztetni. Amennyiben bármely Megbízott igénybe kíván venni adatfeldolgozót, és az érinti a Társaság nevében vagy érdekében kezelt vagy feldolgozott személyes adatokat, köteles a Társaságnak azt bejelenteni, és előzetesen egyeztetni. A Társaság által megbízott adatfeldolgozó kizárólag a Társaság előzetes hozzájárulása esetén vehet igénybe adatfeldolgozót.

9.3 Adatfeldolgozással csak olyan szervezet bízható meg, amely nem érdekelt a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben.

9.4 Az adatfeldolgozóval a GDPR-nak és az Info. tv nek megfelelő adatfeldolgozási szerződést kell kötni írásban. Írásban, előzetesen tájékoztatni kell az adatfeldolgozó igénybevételéről, annak nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről azokat az érintetteket, akiknek az adatai feldolgozását végzi az adatfeldolgozó.

9.5 Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit a jogszabályok, az adatfeldolgozásra vonatkozó szerződés és a jelen Szabályzat keretei között az adatkezelő határozza meg. Az adatkezelő írásban utasítást

ad az adatfeldolgozónak arra vonatkozóan, hogyan lássa el az adatfeldolgozással kapcsolatos tevékenységét. Az adatkezelő által adott utasítások jogszerűségéért az adatkezelő felel. Az adatkezelő felel az adatfeldolgozó által az érintettnek okozott kárért is.

9.6 Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag az adatkezelő rendelkezései szerint dolgozhatja fel, saját céljára adatfeldolgozást nem végezhet, továbbá a személyes adatokat az adatkezelő rendelkezései szerint köteles tárolni és megőrizni ill. azokról a GDPR 30. cikk (2) bekezdés rendelkezéseinek megfelelő adatkezelési nyilvántartást vezetni.

9.7 A jelen 10. pontban foglalt szabályok irányadóak arra az esetre is, ha a megbízott a Társaság adatfeldolgozójaként jár el.

X. Adattovábbítás

Adattovábbítás alatt a személyes adatoknak az érintetten, az adatkezelőn és az adatfeldolgozón kívüli, meghatározott harmadik személy számára történő hozzáférhetővé tételét értjük.

Ennek megfelelően nem csak az adatok tényleges átadása minősül adattovábbításnak, hanem az is, ha például egy meghatározott Adatállományhoz valamely harmadik személy hozzáférési jogot kap.

Az adattovábbítás egy meghatározott adatkezelési művelet, ezért az adatkezelésre irányadó valamennyi rendelkezésnek és előírást is alkalmazni kell az adattovábbításra.

10.1 Magyarország területére történő adattovábbítás esetén az adattovábbítás jogalapja megegyezik azokkal az általános szabályokkal, amelyek általában az adatkezelésre irányadóak (lsd. IV. fejezet – Adatvédelmi alapelvek).

10.2 Az Európai Gazdasági Térségbe tartozó államokba (EGT-államok) irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

Az EGT-államok a jelen Szabályzat kiadásának időpontjában az alábbiak:

Ausztria, Belgium, Bulgária, Ciprus, Csehország, Dánia, Egyesült Királyság, Észtország, Finnország, Franciaország, Görögország, Hollandia, Horvátország, Izland, Írország, Lengyelország, Lettország, Liechtenstein, Litvánia, Luxemburg, Magyarország, Málta, Németország, Norvégia, Olaszország, Portugália, Románia, Spanyolország, Svájc, Svédország, Szlovákia, Szlovénia.

10.3 A Bit. szerinti biztosításközvetítő, valamint a Hpt. szerinti pénzügyi közvetítő bizonyos esetekben az érintett hozzájárulása nélkül is továbbíthat a Bit.-ben meghatározott biztosítási titoknak minősülő személyes adatokat, illetve a Hpt.-ben meghatározott banktitoknak minősülő személyes adatokat az említett törvényekben meghatározott

bíróságoknak, hatóságoknak vagy egyéb harmadik személyeknek. Az ilyen típusú megkereséseket kötelező egyeztetni a belső adatvédelmi felelőssel.

10.4 Személyes adat EGT-tagállamnak nem minősülő harmadik országban adatkezelést folytató meghatározott adatkezelő részére akkor továbbítható, vagy harmadik országban adatfeldolgozást végző meghatározott adatfeldolgozó részére elsősorban akkor adható át, ha ahhoz az érintett kifejezetten (írásban) hozzájárult és az adatkezelő és az adatfeldolgozó teljesíti a GDPR V. fejezetben rögzített feltételeket. Amennyiben ilyen hozzájárulás nem áll rendelkezésre, akkor a belső adatvédelmi felelőssel kell egyeztetni, hogy fennállnak-e a harmadik országba történő adattovábbítás feltételei.

10.5 Az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából köteles – mind a belföldre, mind a külföldre irányuló adattovábbítás esetén – az adatkezelő adattovábbítási nyilvántartást vezetni. Az adattovábbítási nyilvántartás a következőket tartalmazza:

(i) a személyes adatok továbbításának időpontját,

(ii) az adattovábbítás jogalapját és címzettjét, valamint

(iii) a továbbított személyes adatok körének meghatározását,

(iv) az adatkezelést előíró jogszabályban esetlegesen meghatározott egyéb adatokat.

10.6 Biztosítási titok továbbítása harmadik személynek

10.6.1 Biztosítási titok csak akkor adható ki harmadik személynek, ha

a) a biztosításközvetítő ügyfele vagy annak képviselője a kiszolgáltatható biztosítási titokkört pontosan megjelölve, erre vonatkozóan írásban felmentést ad,

b) a Bit. alapján a titoktartási kötelezettség nem áll fenn.

Ez utóbbi esetben a Bit. alapján a Bit-ben megjelölt szervek vagy személyek adatkérési megkereséssel fordulhatnak a Társasághoz, amely esetben a Társaság a biztosítási titoknak minősülő személyes adatokat továbbíthatja a megkereső szervnek vagy személynek.

10.6.2 Biztosítási titoknak minősülő személyes adat kiadására vonatkozó megkeresés esetén a megkeresést a belső adatvédelmi felelőssel egyeztetni kell, és az adattovábbítást be kell jegyezni az adattovábbítási nyilvántartásba. Ezeket az adatokat az adattovábbítástól számított 5 év elteltével, a különleges adatokat pedig 20 év elteltével törölni kell.

10.7 Banktitok továbbítása harmadik személynek

10.7.1 Banktitok csak akkor adható ki harmadik személynek, ha

a) az ügyfél, annak törvényes képviselője a rá vonatkozó kiszolgáltatható banktitokkört pontosan megjelölve közokiratba vagy teljes bizonyító erejű magánokiratba foglaltan kéri vagy erre felhatalmazást ad; nem szükséges a közokiratba, teljes

bizonyító erejű magánokiratba foglalás, ha az ügyfél ezt az írásbeli nyilatkozatát a pénzügyi intézménnyel történő szerződéskötés keretében nyújtja,

b) a Hpt. a banktitok megtartásának kötelezettsége alól felmentést ad,

c) a pénzügyi intézmény érdeke ezt az ügyféllel szemben fennálló követelése eladásához vagy lejárt követelése érvényesítéséhez szükségessé teszi.

A b) pont szerinti esetben a Hpt. alapján a Hpt-ben megjelölt szervek vagy személyek adatkérési megkereséssel fordulhatnak a Társasághoz, amely esetben a Társaság a banktitoknak minősülő személyes adatokat továbbíthatja a megkereső szervnek vagy személynek.

10.7.2 Banktitoknak minősülő személyes adat kiadására vonatkozó megkeresés esetén, a megkeresést a belső adatvédelmi felelőssel egyeztetni kell, valamint az adattovábbítást be kell jegyezni az adattovábbítási nyilvántartásba.

XI. Belső adatvédelmi felelős

11.1 Valamennyi, a Bit. hatálya alá tartozó biztosításközvetítést és a Hpt. hatálya alá tartozó pénzügyi közvetítést végző személy, az adatvédelemmel kapcsolatos előírások, így különösen jelen Szabályzat rendelkezéseink betartása valamint az általa végzett adatkezelési tevékenység ellenőrzésének biztosítása érdekében köteles szervezeten belül, közvetlenül a szervezet vezetőjének felügyelete alá tartozó – jogi, közigazgatási, informatikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező – belső adatvédelmi felelőst kinevezni vagy megbízni.

11.2 A belső adatvédelmi felelős:

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
b) ellenőrzi az Info tv. és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszűntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
d) elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
e) vezeti a belső adatkezelési nyilvántartást;
f) gondoskodik az adatvédelmi ismeretek oktatásáról;
g) részt vesz a NAIH által szervezet belső adatvédelmi felelősök konferenciáján.

11.3 A belső adatvédelmi felelős bármely, a jelen Szabályzat hatály alá tartozó adatkezelés vagy adatfeldolgozás vonatkozásában jogosult adatvédelmi auditot lefolytatni. Az audit eredményéről 15 napon belül írásbeli jelentést készít a felettese felé.

11.4 Konkrét adatvédelmi panasz esetében, a panasz súlyának függvényében, a belső adatvédelmi felelős köteles azonnali auditot lefolytatni, és annak eredményéről 8 munkanapon belül írásos jelentést készíteni a felettese felé.

11.5 Az év során tervezett rendszeres adatvédelmi auditokról a belső adatvédelmi felelős minden év január 31. napjáig tervet készít, és jóváhagyás céljából megküldi a felettese számára. Az ily módon elkészített és jóváhagyott terv képezi a rendes ellenőrzések alapját.

11.6 Az ellenőrzés tapasztalatairól a belső adatvédelmi felelős a felettesét írásban tájékoztatja, szükség esetén pedig a kezelendő adatok körének, illetőleg az adatfeldolgozás módszerének megváltoztatására tesz javaslatot.

11.7 A belső adatvédelmi felelős valamennyi Munkatárs és Megbízott számára igény szerint, de legalább kétévente adatvédelmi és adatbiztonsági oktatást tart, melyen valamennyi Munkatárs, illetve Megbízott köteles részt venni.

XII. Az EFS saját cookie kezelése

12.1 A szolgáltató a testre szabott kiszolgálás érdekében a felhasználó számítógépén kis adatcsomagot, ún. sütit (cookie) helyez el és a későbbi látogatás során olvas vissza. Ha a böngésző visszaküld egy korábban elmentett sütit, a sütit kezelő szolgáltatónak lehetősége van összekapcsolni a felhasználó aktuális látogatását a korábbiakkal, de kizárólag a saját tartalma tekintetében.

12.2 Az adatkezelés célja: a felhasználók azonosítása, egymástól való megkülönböztetése, a felhasználók aktuális munkamenetének azonosítása, az annak során megadott adatok tárolása, az adatvesztés megakadályozása. Az adatkezelés jogalapja: az érintett hozzájárulása. A kezelt adatok köre: azonosítószám, dátum, időpont, valamint az előzőleg meglátogatott oldal. Az adatkezelés időtartama: a munkamenet lezárultáig

12.3 A munkamenet lezárultáig érvényes süti csak a böngésző bezárásáig marad a számítógépen. A pontos érvényességi idővel rendelkező (állandó) sütik törlésükig, de legkésőbb érvényességi idejük lejáratáig tárolódnak a számítógépen. A sütit a felhasználó képes törölni saját számítógépéről, illetve letilthatja böngészőjében a sütik alkalmazását. A sütik kezelésére általában a böngészők Eszközök/Beállítások menüjében az Adatvédelem/Előzmények/Egyéni beállítások menü alatt, cookie, süti vagy nyomkövetés megnevezéssel van lehetőség.

12.4 A sütikről az alábbi címen érhető el bővebb információ: http://www.adatvedelmiszakerto.hu/cookie

XIII. Szabályzat módosítása

13.1 A jelen Szabályzat rendelkezéseinek megváltoztatására kizárólag a Társaság Igazgatósága jogosult.

13.2 A Társaság cégvezetője felelősséggel tartozik a Szabályzatban leírtak betartásáért.