EOS FAKTOR MAGYARORSZÁG

ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

BUDAPEST, 2018.05.25.

Tartalomjegyzék

Bevezetés

1.1. A Szabályzat célja

Az Adatvédelmi és adatbiztonsági szabályzat (a továbbiakban: Szabályzat) célja, hogy biztosítsa az EOS Faktor Magyarország Zártkörűen Működő Részvénytársaság (a továbbiakban: Társaság, székhely: 1132 Budapest, Váci út 30., céget nyilvántartó Bíróság a Fővárosi Törvényszék, mint Cégbíróság: Cg. 01-10-045904, adószám: 14220438-2-41, Pénzügyi Szervezetek Állami Felügyelete engedélyének száma: E-I-67/2008) által végzett adatkezelési tevékenységek tekintetében a természetes személyek alapvető jogainak és szabadságainak védelmét, a Társaság tevékenysége során a személyes adatok védelméhez fűződő információs önrendelkezési jog érvényesülését, továbbá, hogy a Társaság által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat. A Szabályzat kialakítja az adatvédelem szempontjából fontos felelősségi viszonyokat.

2. Szabályzat hatálya

2.1. A Szabályzat személyi hatálya

A Szabályzat személyi hatálya kiterjed a Társaság valamennyi szervezeti egységére, minden alkalmazottjára, valamint a vele szerződéses vagy egyéb kapcsolatban álló, személyes adatkezelést végző személyekre.

2.2. A Szabályzat időbeli hatálya

A Szabályzat az előlapon jelzett időpontban lép hatályba határozatlan időre.

2.3. A Szabályzat tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed a Társaság szervezeti egységei által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére, keletkezésük, kezelésük, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

A Szabályzat hatálya kiterjed a Társaság egyes szervezeti egységei közötti, illetve a Társaság által igénybevett adatfeldolgozók felé irányuló adatáramlásra is.

3. Értelmező rendelkezések

A Szabályzat alkalmazása során:

3.1.1. *érintett:* bármely információ alapján azonosított vagy azonosítható természetes személy

3.1.2. *azonosítható természetes személy:* az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható

3.1.3. *személyes adat:* az érintettre vonatkozó bármely információ

3.1.4. *különleges adat:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok

3.1.5. *egészségügyi adat:* egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról

3.1.6. *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

3.1.7. *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

3.1.8. *adatfeldolgozó:* az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében, érdekében és utasításai szerint az adatkezelő által meghatározott célból és eszközökkel személyes adatokat kezel

3.1.9. *hozzájárulás:* az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez

3.1.10. *címzett:* az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz

3.1.11. *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

3.1.12. *adatkezelés korlátozása:* a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján

3.1.13. *adatzárolás:* az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából

3.1.14. *adatmegjelölés:* az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából

3.1.15. *álnevesítés:* személyes adat olyan módon történő kezelése, amely – a személyes adattól elkülönítve tárolt – további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni

3.1.16. *profilalkotás:* személyes adat bármely olyan – automatizált módon történő – kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul

3.1.17. *adatvédelmi incidens:* az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi

3.1.18. *nyilvánosságra hozatal:* az adat bárki számára történő hozzáférhetővé tétele

3.1.19. *tiltakozás:* az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri

3.1.20. *adattörlés:* az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges

3.1.21. *adatmegsemmisítés:* az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése

3.1.22. *adattovábbítás:* az adat meghatározott harmadik fél részére történő hozzáférhetővé tétele

3.1.23. *közvetett adattovábbítás:* személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása

3.1.24. *harmadik ország:* minden olyan állam, amely nem EGT-tagállam

3.1.25. *nemzetközi szervezet:* a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre

3.1.26. *EGT-állam*: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az

Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez

3.1.27. *üzleti titok*: a gazdasági tevékenységhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a jogosult jogos pénzügyi, gazdasági vagy piaci érdekét sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a vele jogszerűen rendelkező jogosultat felróhatóság nem terheli

3.1.28. *banktitok*: minden olyan, az egyes ügyfelekről a pénzügyi intézmény 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 kötött szerződéseire vonatkozik

3.1.29. *adatvédelem:* a személyes adatok kezelésének normatív szabályozása az érintett információs önrendelkezési jogának érvényesítése érdekében

3.1.30. *információs önrendelkezési jog:* az Alaptörvény VI. cikkében biztosított személyes adatok védelméhez való jognak az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról

3.1.31. *adatbiztonság:* a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége; az adatkezelésnek az az állapota, amelyben a kockázati tényezőket – és ezzel a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a legkisebb mértékűre csökkentik

3.1.32. *adatgazda:* az a személy, aki az adott adatkezelésre vonatkozó döntési jogosultsággal rendelkezik

3.1.33. *betekintési és megismerési jogosultság:* az a jogkör, amelynek birtokában a jogosult számára elérhetővé, megismerhetővé válnak az adott adatállományban kezelt személyes adatok

3.1.34. *közvetlen megismerési jogosultság:* adott adatállomány informatikai alkalmazás igénybevételével kezelt adatainak megismeréséhez adott olyan jogkör, amely a jogosult számára lehetőséget biztosít arra, hogy az ott kezelt adatokhoz az általa megválasztott időpontban közvetlen lekérdezéssel hozzáférjen

3.1.35. *közvetlen lekérdezés:* adott adatállományban kezelt adatokban – az adatkezelő által előzetesen rendelkezésre bocsátott általános lekérdezési jogosultság felhasználásával – előre meghatározatlan időpontban és alkalommal, naplózott formában történő betekintés,

illetve az így megismerhetővé vált információ kinyomtatása, vagy más módon történő rögzítése

3.1.36. *adathordozó:* bármely alakban, bármilyen eszköz felhasználásával és bármilyen eljárással előállított, személyes adatot tartalmazó anyag

3.1.37. *hardver eszköz:* valamennyi olyan eszköz, amelynek feladata az informatikai rendszer folyamatos működésének biztosítása, vagy amely biztonsági adatmentésre, avagy másolatok készítésére szolgál, valamint amely elektronikus vagy egyéb módon a számítógép külső behatás elleni védelmét szolgálja

3.1.38. *hírközlő eszköz:* bármilyen technikai eszköz, technológiai eljárás, amely egy vagy több fogadó személy számára jelzések, adatok és információk továbbítására vagy fogadására alkalmas

4. Az adatvédelem alapelvei

Az adatvédelmi szabályok betartásáért a Társaság a felelős. A Társaság munkavállalói és külső megbízottjai feladataik ellátása körében személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezelhetnek.

A Társaság adatkezelést végző alkalmazottja kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a feladat- és hatáskörének gyakorlása során tudomására jutott személyes adatok jogszerű kezeléséért, a Társaság nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.

4.1. Jogszerűség, tisztességes eljárás és átláthatóság

A személyes adatok kezelését a Társaságnak jogszerűen - megfelelő jogalapon - és tisztességesen - az információs önrendelkezési jog/magánszféra/emberi méltóság tiszteletben tartásával - kell végeznie.

A személyes adatok kezelését a Társaságnak az érintett számára átlátható módon kell végezni. A természetes személyek számára átláthatónak kell lennie, hogy a Társaság a rájuk vonatkozó személyes adataikat hogyan gyűjti, használja fel, azokba hogy tekint bele vagy milyen egyéb módon kezeli, a személyes adatokat milyen mértékben kezeli vagy fogja kezelni.

Az átláthatóság elve megköveteli, hogy a személyes adatok kezelésével összefüggő tájékoztatás, illetve kommunikáció könnyen hozzáférhető és közérthető legyen, valamint hogy azt a Társaság világosan és egyszerű nyelvezettel fogalmazza meg. Ez az elv vonatkozik különösen az érintetteknek a Társaság kilétéről és az adatkezelés céljáról való tájékoztatására, valamint arra a tájékoztatásra, hogy az érintetteknek jogukban áll megerősítést és tájékoztatást kapni a Társaságtól a róluk kezelt adatokról.

A természetes személyt a személyes adatok kezelésével összefüggő kockázatokról, szabályokról, garanciákról és jogokról tájékoztatni kell, valamint arról, hogy hogyan gyakorolhatja az adatkezelés kapcsán megillető jogokat.

4.2. Célhoz kötöttség, adattakarékosság és korlátozott tárolhatóság

A Társaság által a cél megvalósulásához szükséges mértékben és ideig csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas.

A személyes adatkezelés konkrét céljainak mindenekelőtt explicit módon megfogalmazottaknak és jogszerűeknek, továbbá már a személyes adatok gyűjtésének időpontjában meghatározottaknak kell lenniük.

A személyes adatoknak a kezelésük céljára alkalmasaknak és relevánsaknak kell lenniük, az adatok körét pedig a célhoz szükséges minimumra kell korlátozni. Ehhez pedig a Társaságnak biztosítania kell különösen azt, hogy a személyes adatok tárolása a lehető legrövidebb időtartamra korlátozódjon.

Személyes adatok a Társaság által csak abban az esetben kezelhetők, ha az adatkezelés célját egyéb eszközzel észszerű módon nem lehetséges elérni.

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, a Társaság törlési, illetve rendszeres felülvizsgálati határidőket állapít meg.

A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése a Társaság által csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését. Annak megállapításához, hogy a további adatkezelés célja összeegyeztethető-e a személyes adatok gyűjtésének eredeti céljával, a Társaság – az eredeti adatkezelés jogszerűségére vonatkozó valamennyi előírás teljesítését követően – figyelembe veszi többek között az eredeti célok és a tervezett további adatkezelési célok között fennálló összefüggést, az adatgyűjtés körülményeit, ideértve különösen az érintettnek a további adatfelhasználásra vonatkozó, a Társasággal fennálló kapcsolatán alapuló észszerű elvárásait is, továbbá a személyes adatok jellegét, a tervezett további adatkezelés következményeit az érintettekre nézve, valamint a megfelelő garanciák meglétét mind az eredeti, mind a tervezett további személyes adatkezelési műveletek során.

4.3. Pontosság

A pontatlan személyes adatok helyesbítése vagy törlése érdekében minden észszerű lépést meg kell tenni. Ha a Társaság tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni.

4.4. Integritás és bizalmas jelleg

A Társaságnak a személyes adatokat olyan módon kell kezelnie, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

Az adatkezelés biztonsága körében a Az Európai Parlament és a Tanács 2016/679 Rendelete (a továbbiakban: Rendelet) előírja a Társaság számára, hogy a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajtson végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

- a személyes adatok álnevesítését és titkosítását;
- a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;
- fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;
- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

Ezeket az intézkedéseket a Társaság felülvizsgálja és szükség esetén naprakésszé teszi.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

A Társaság intézkedéseket hoz annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag a Társaság utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

4.5. Elszámoltathatóság

A Társaság felelős a személyes adatok kezelésére vonatkozó elvek betartásáért, továbbá képesnek kell lennie e megfelelés igazolására (anyagi felelősség).

Az elszámoltathatóság elvének lényege kettős: egyrészt azt várja el a Társaságtól, hogy kialakítsa azokat a belső szabályokat, folyamatokat, mechanizmusokat, amelyek a rendeletből fakadó kötelezettségek teljesítéséhez szükségesek, másrészt a megfelelés bemutatásának képességét várja el.

A Társaság elszámoltathatósági intézkedései különösen az alábbiak:

- belső felülvizsgálat
- írásbeli és kötelező adatvédelmi politikák
- adatkezelési eljárások feltérképezése
- képzés és oktatás
- érintetti jogok gyakorlásának felügyelete

- belső panaszkezelés
- sérülékenységi vizsgálat elvégzése
- adatvédelmi hatásvizsgálat elvégzése
- audit
- ellenőrzés
- a beépített és alapértelmezett adatvédelemre vonatkozó elvárásnak való megfelelés (adatminimalizálás, átláthatóság, álnevesítés, adatbiztonsági intézkedések stb.)
- a megfelelő adatfeldolgozók kiválasztása és igénybe vétele
- az adatkezelési tevékenységek nyilvántartása
- a megfelelő adatbiztonsági intézkedések megtétele
- adatvédelmi incidensek megfelelő kezelése
- az adatvédelmi tisztviselő kijelölése.

5. Az adatkezelés jogalapjai

A személyes adatok Társaság általi kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:

- *szerződés:* 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
- *jogi kötelezettség:* az adatkezelés a Társaságra vonatkozó jogi kötelezettség teljesítéséhez szükséges
- *jogos érdek:* az adatkezelés a Társaság jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek
- *hozzájárulás:* az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez.

Az adatkezelés megfelelően kiválasztott jogalapja befolyásolja az érintett rendelkezésére álló egyes jogok gyakorolhatóságát:

	Törléshez való jog	Adathordozhatósághoz való jog	Tiltakozáshoz való jog
Szerződés	✓	✓	**X**
Jogi kötelezettség	**X**	**X**	**X**
Jogos érdek	✓	**X**	✓
Hozzájárulás	✓	✓	**X – de! visszavonhatja**

5.1. Szerződés

A szerződés (tágabb értelemben a kötelem) lényege, hogy az a felek között létrejövő olyan jogviszony, amelyből eredően az egyik fél jogosult lesz a másik felet jogi eszközökkel rászorítani arra, hogy

valamit tegyen, ne tegyen vagy eltűrjön. A kötelem magában foglalja a véghezviteli parancsot, a felelősséget, a szankciót és a követelés alapjául szolgáló keresetjogot is. A „szerződés" a szerződés megkötésétől annak bármilyen módon történő teljesedésbe menéséig, a teljesedésbe menés meghiúsulása esetén pedig az igény elenyészéséig terjedő időszakban a feleket megillető jogok és kötelezettségek összessége.

A GDPR 6. cikk (1) bekezdés b) pontjában foglalt szerződéses jogalap kellő jogalapul szolgál a szerződés nem-teljesítése esetére igénybe vett jogi lépésekhez (az igénynek a szerződés biztosítékaiból való közvetlen kielégítése, engedményezés, perindítás, végrehajtás kezdeményezése, stb.) szükséges adatok kezelésére.

A szerződés nem-teljesítése esetén történő vagy a nem-teljesítés esetére szükséges adatkezelés az igényt érvényesítő fél jogszabályban biztosított és egyoldalúan gyakorolható jogai érvényesítéséhez szükséges.

5.2. Jogi kötelezettség

A Társaság részére jogi kötelezettség teljesítését célzó adatkezelést ír elő különösen:

- a központi hitelinformációs rendszerről szóló 2011. évi CXXII. törvény (a továbbiakban: KHR. tv.) 6. § (3). bekezdése, 8. § - 9. §-ai, 11 – 13/A. §-ai
- a számvitelről szóló 2000. évi C. törvény (a továbbiakban: Számv. tv.) 12. § (1) bekezdése, 169. § (2) bekezdése
- a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII törvény (a továbbiakban: Hpt.) 161. § (2) bekezdése, 288. § (2)-(3) bekezdései
- a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet 3. § (2) bekezdése
- a Munka Törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.) 81. § (1) bekezdése
- az adózás rendjéről szóló 2003. évi XCII. törvény (a továbbiakban: rArt.) 47. § (4) bekezdése
- az adózás rendjéről szóló 2017. évi CL. törvény (a továbbiakban: Art.) 50. § (1)-(2) bekezdései, 78. § (4) bekezdése, 1. sz. melléklet 3. pontja
- a személyi jövedelemadóról szóló 1995. évi CXVII. törvény (a továbbiakban: Szja. tv.) 48. § (1) bekezdése, 48. § (3)-(3a) bekezdései
- a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény (a továbbiakban: Tbj.) 46. § (2) bekezdése, 47. § (1) bekezdése
- a pénzügyi szervezetek panaszkezelésére vonatkozó szabályokról szóló 28/2014. (VII. 23.) MNB rendelet 5. § (1) bekezdése, 1. sz. melléklet II.1.3., II.1.7., III.1., V.1 - V.2. pontjai
- a befektetési vállalkozások, a pénzforgalmi intézmények, az elektronikuspénz-kibocsátó intézmények, az utalványkibocsátók, a pénzügyi intézmények és a független pénzügyi szolgáltatás közvetítők panaszkezelésének eljárásával, valamint panaszkezelési

szabályzatával kapcsolatos részletes szabályokról szóló 435/2016. (XII. 16.) Korm. rendelet 3. § (3) bekezdése

5.3. Jogos érdek

A jogos érdek fennállásának megállapításához a Társaságnak meg kell vizsgálnia többek között azt, hogy az érintett az adatkezeléssel összefüggésben számíthat-e észszerűen arra, hogy az adott célból személyes adatainak kezelésére kerülhet sor.

Jogos érdekről lehet szó, amikor releváns kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett a Társaság ügyfele vagy annak alkalmazásában áll.

A Társaság érdekének jogossága akkor állapítható meg, ha az

- törvényes (azaz az összhangban van az Európai Unió jogával és a nemzeti joggal)
- pontosan megfogalmazott annak érdekében, hogy az érdekmérlegelési teszt során összemérhető legyen az adatalany érdekeivel és alapvető jogaival
- valós érdeket képvisel (azaz nem elméleti jellegű).

A jogos érdek meglétének, az adatkezelés szükségességének, valamint az érintett jogkorlátozása arányosságának vizsgálata ún. érdekmérlegelési teszt elvégzésével vizsgálható, illetve igazolható. A jogos érdeken alapuló adatkezelés eseteiben az érdekmérlegelési teszt lépései a következők:

- *első lépés:* annak meghatározása, hogy mi az adatkezelés célja
- *második lépés:* annak meghatározása, hogy az adatkezelés feltétlenül szükséges-e a cél eléréséhez
- *harmadik lépés:* a Társaság jogos érdekének meghatározása, az érdek jogszerűségének vagy nem jogszerű voltának megállapítása
- *negyedik lépés:* milyen személyes adatok meddig tartó adatkezelését igényli a jogos érdek
- *ötödik lépés:* az érintett lehetséges érdekeinek meghatározása (azok a szempontok, amelyeket felhozhat az adatkezeléssel szemben)
- *hatodik lépés:* annak meghatározása, hogy miért korlátozza arányosan a Társaság érdeke az érintett alapvetői jogait és szabadságait.

5.4. Hozzájárulás

A hozzájáruláson alapuló adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez.

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 adatkezelés hozzájáruláson alapul, a Társaságnak képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

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. Az érintett hozzájárulását tartalmazó ilyen nyilatkozat bármely olyan része, amely sérti e követelményt, kötelező erővel nem bír.

Hozzájáruláson alapuló adatkezelés esetében a Társaság törekszik arra, hogy előre megfogalmazott hozzájárulási nyilatkozatot biztosítson az érintett részére, amelyet érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel bocsát rendelkezésre.

Ahhoz, hogy a hozzájárulás tájékoztatáson alapulónak minősüljön, az érintettnek legalább tisztában kell lennie a Társaság kilétével és a személyes adatok kezelésének céljával. A hozzájárulás megadása nem tekinthető önkéntesnek, ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna.

A hozzájárulás nem tekinthető önkéntesnek, ha nem tesz lehetővé külön-külön hozzájárulást a különböző személyes adatkezelési műveletekhez.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

6. A személyes adatok különleges kategóriáinak kezelése

Az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok egyedi védelmet igényelnek, mivel az alapvető jogokra és szabadságokra nézve a kezelésük körülményei jelentős kockázatot hordozhatnak.

Különleges adatnak minősül:

- a faji vagy etnikai származásra utaló személyes adat
- a politikai véleményre utaló személyes adat
- a vallási vagy világnézeti meggyőződésre utaló személyes adat
- a szakszervezeti tagságra utaló személyes adat
- a genetikai és biometrikus adat
- az egészségügyi adat
- a szexuális életre vagy szexuális irányultságra vonatkozó személyes adat.

Az ilyen adatok nem kezelhetők, kivéve, ha az adatkezelés a Rendeletben meghatározott egyedi esetekben megengedett, azt is figyelembe véve, hogy a nemzeti (tagállami) jog különös rendelkezéseket állapíthat meg az adatok védelmére vonatkozóan.

A személyes adatok ilyen különleges kategóriáinak kezelésére vonatkozó általános tilalomtól való eltérést enged a Rendelet például az alábbi esetekben:

- az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez
- az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése érdekében szükséges.

7. Az érintett jogai

Az érintett jogosult arra, hogy a Társaság és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában

- az adatkezeléssel összefüggő tényekről - az adatkezelés megkezdését megelőzően - tájékoztatást kapjon (a továbbiakban: (*előzetes) tájékoztatáshoz való jog*),
- kérelmére személyes adatait és az azok kezelésével összefüggő információkat a Társaság a rendelkezésére bocsássa (a továbbiakban: *hozzáféréshez való jog*),
- kérelmére, valamint jogszabályban meghatározott további esetekben személyes adatait a Társaság helyesbítse, illetve kiegészítse (a továbbiakban: *helyesbítéshez való jog*),
- kérelmére, valamint jogszabályban meghatározott további esetekben személyes adatai kezelését a Társaság korlátozza (a továbbiakban: *adatkezelés korlátozásához való jog*),
- kérelmére, valamint jogszabályban meghatározott további esetekben személyes adatait a Társaság törölje (a továbbiakban: *törléshez való jog*),
- kérelmére a rá vonatkozó, általa a Társaság rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja (a továbbiakban: *adathordozhatósághoz való jog*)
- a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen (a továbbiakban: *tiltakozáshoz való jog*)
- a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság) eljárását kezdeményezhesse (a továbbiakban: *hatósági jogorvoslathoz való jog*) és
- a bíróság eljárását kezdeményezhesse (a továbbiakban: *bírósági jogorvoslathoz való jog*).

Az érintetti jogok érvényesítésével kapcsolatos általános elvárásokat jelen Szabályzat, míg az eljárási részletszabályokat külön szabályzat, az Érintetti jogokról szóló szabályzat tartalmazza.

7.1. Tájékoztatáshoz való jog

A tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól. A Társaság olyan további információt is az érintett rendelkezésére bocsát, amelyek a tisztességes és átlátható adatkezelés biztosításához szükségesek, figyelembe véve a személyes adatok kezelésének konkrét körülményeit és kontextusát. Az érintettet továbbá a profilalkotás tényéről és annak következményeiről tájékoztatni kell. Ha a személyes adatokat a Társaság az érintettől gyűjti, az érintettet arról is tájékoztatni kell, hogy köteles-e a személyes adatokat közölni, valamint, hogy az adatszolgáltatás elmaradása milyen következményekkel jár.

Az érintettre vonatkozó személyes adatok kezelésével összefüggő tájékoztatást az adatgyűjtés időpontjában kell az érintett részére megadni, illetve ha az adatokat a Társaság nem az érintettől, hanem más forrásból gyűjtötte, az ügy körülményeit figyelembe véve, észszerű határidőn belül kell megadni.

Ha a személyes adatok jogszerűen közölhetőek más címzettel, a címzettel történő első közléskor arról az érintettet tájékoztatni kell.

Ha a Társaság a személyes adatokat a gyűjtésük eredeti céljától eltérő célból kívánja kezelni, a további adatkezelést megelőzően az érintettet erről az eltérő célról és minden egyéb szükséges tudnivalóról tájékoztatnia kell. Ha a Társaság nem tud tájékoztatást nyújtani az érintett részére a személyes adatok eredetéről, mivel azok különböző forrásokból származnak, általános tájékoztatást kell adni.

Mindazonáltal a tájékoztatás nyújtására vonatkozó kötelezettség előírása nem szükséges, ha az érintettnek ez az információ már a birtokában van, vagy ha a személyes adat rögzítését, illetve közlését valamely jogszabály kifejezetten előírja, vagy ha az érintett tájékoztatása lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényelne.

Az alábbi táblázat összegzi azokat az információkat, amelyekről az érintetteket tájékoztatni kell:

Milyen információt kell megadni?	**Érintettől gyűjtött személyes adat**	**Nem az érintettől gyűjtött személyes adat**
az adatkezelő kiléte és elérhetőségei	✓	✓
az adatvédelmi tisztviselő kiléte és elérhetőségei	✓	✓
az adatkezelés célja, valamint jogalapja	✓	✓
jogos érdeken alapuló adatkezelés esetén az adatkezelő jogos érdeke	✓	✓
az érintett személyes adatok kategóriái	**X**	✓
a személyes adatok címzettjei, illetve a címzettek kategóriái	✓	✓
a személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbításának ténye és a megfelelő és alkalmas garanciák megjelölése	✓	✓
az adatkezelés időtartama	✓	✓
érintetti jogok, ideértve a hatósági jogorvoslathoz való jogot is	✓	✓
hozzájáruláson alapuló adatkezelés esetén a hozzájárulás bármely időpontban történő visszavonásához való jog	✓	✓
a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e	**X**	✓

a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, az érintett köteles-e a személyes adatokat megadni, milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása	✓	**X**
automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint az alkalmazott logikára és arra vonatkozó érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír	✓	✓

Az alábbi táblázat összefoglalja azokat az időpontokat, amikor az érintetteket tájékoztatni kell:

	Mikor kell az információt megadni?
Érintettől gyűjtött személyes adat	▪ a személyes adatok megszerzésének időpontjában
Nem az érintettől gyűjtött személyes adat	▪ a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül ▪ ha a személyes adatokat az érintettel való kapcsolattartás céljára használja a Társaság, legalább az érintettel való első kapcsolatfelvétel alkalmával ▪ ha várhatóan más címzettel is közli az adatokat a Társaság, legkésőbb a személyes adatok első alkalommal való közlésekor

Az átláthatóság elve megköveteli, hogy az érintettnek nyújtott tájékoztatás tömör, könnyen hozzáférhető és könnyen érthető legyen, valamint hogy azt a Társaság világos és közérthető nyelven fogalmazza meg. Az ilyen tájékoztatás nyújtható elektronikus formátumban is, így például közölhető a Társaság honlapján.

7.2. Hozzáféréshez való jog

Az érintett jogosult arra, hogy hozzáférjen a rá vonatkozóan gyűjtött adatokhoz, valamint arra, hogy egyszerűen és észszerű időközönként, az adatkezelés jogszerűségének megállapítása és ellenőrzése érdekében gyakorolja e jogát. E jogát oly módon kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg.

A hozzáféréshez való jog érvényesülése érdekében az érintettet kérelmére a Társaság tájékoztatja arról, hogy személyes adatait maga a Társaság, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó kezeli-e.

Minden érintett számára biztosítani kell a jogot arra, hogy megismerje különösen

- a személyes adatok kezelésének céljait
- az érintett személyes adatok kategóriáit
- ha lehetséges, azt, hogy a személyes adatok kezelése milyen időtartamra vonatkozik
- a személyes adatok címzettjeit
- az érintetti jogait, ideértve a hatósági jogorvoslathoz való jogot is
- az adatok forrására vonatkozó információt

- az érintett személyes adatainak kezelésével összefüggésben felmerült adatvédelmi incidensek bekövetkezésének körülményeit, azok hatásait és az azok kezelésére tett intézkedéseket
- a személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbításának tényét és a megfelelő és alkalmas garanciákat
- azt, hogy a személyes adatok automatizált kezelése milyen logika alapján történt, valamint
- azt, hogy az adatkezelés – legalább abban az esetben, amikor az profilalkotásra épül – milyen következményekkel járhat, továbbá, hogy
- minderről tájékoztatást kapjon.

Ha a Társaság nagy mennyiségű információt kezel az érintettre vonatkozóan, kérheti az érintettet, hogy az információk közlését megelőzően pontosítsa, hogy kérése mely információkra vagy mely adatkezelési tevékenységekre vonatkozik.

A Társaságnak a tájékoztatást díjmentesen, indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 25 napon belül írásban postai úton, vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton kell megadnia.

A tájékoztatást a Társaság megtagadhatja, ha

- a tájékoztatást kérő személy nem a saját adataira vonatkozóan kér tájékoztatást
- a tájékoztatást kérő személy nem tudja hitelt érdemlő módon igazolni, hogy ő lenne az adatkezeléssel érintett személy.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

7.3. Helyesbítéshez való jog

A helyesbítéshez való jog érvényesülése érdekében a Társaság, ha az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatok pontatlanok, helytelenek vagy hiányosak, azokat – különösen az érintett kérelmére – haladéktalanul pontosítja vagy helyesbíti, illetve ha az az adatkezelés céljával összeegyeztethető, az érintett által rendelkezésére bocsátott további személyes adatokkal vagy az érintett által a kezelt személyes adatokhoz fűzött nyilatkozattal kiegészíti. A valóságnak nem megfelelő adatot a Társaság – amennyiben a szükséges adatok rendelkezésre állnak (pl. közhiteles nyilvántartásból) – köteles helyesbíteni.

Mentesül e kötelezettség alól a Társaság, ha

- a pontos, helytálló, illetve hiánytalan személyes adatok nem állnak rendelkezésére és azokat az érintett sem bocsátja rendelkezésére, vagy
- az érintett által rendelkezésére bocsátott személyes adatok valódisága kétséget kizáróan nem állapítható meg.

Ha a Társaság az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatokat helyesbíti, annak tényéről és a helyesbített személyes adatról tájékoztatja azt az adatfeldolgozót, amely részére a helyesbítéssel érintett személyes adatot továbbította.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

Az elutasított helyesbítés iránti kérelmekről a Társaság adatvédelmi tisztviselője nyilvántartást vezet, melyről a tárgyévet követő január 31-éig írásban tájékoztatja a Hatóságot.

7.4. Törléshez való jog

A törléshez való jog érvényesítése érdekében a Társaság indokolatlan késedelem nélkül törli az érintett személyes adatait, ha

- az adatkezelés jogellenes, így különösen, ha az adatkezelés
    - az adatvédelmi alapelvekkel ellentétes
    - célja megszűnt vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához
    - törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy
    - jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja
- az érintett az adatkezeléshez adott hozzájárulását visszavonja és az adatkezelésnek nincs más jogalapja
- az adatok törlését jogszabály, az Európai Unió jogi aktusa, a Hatóság vagy a bíróság elrendelte
- a személyes adatokat a Társaságra alkalmazandó uniós vagy nemzeti jogban előírt jogi kötelezettség teljesítéséhez törölni kell, vagy
- az érintett tiltakozik az adatkezelés ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre.

Ugyanakkor a személyes adatok törlésére irányadó fenti szabály nem alkalmazandó, ha az adatkezelés valamely jogi kötelezettségnek való megfelelés miatt, illetve jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges.

Ha a Társaság az általa, illetve a megbízásából vagy rendelkezése szerint eljáró adatfeldolgozó által kezelt személyes adatokat törli, ezen intézkedés tényéről és annak tartalmáról értesíti azon adatfeldolgozókat, amelyek részére az adatot ezen intézkedését megelőzően továbbította, annak érdekében, hogy azok a törlést a saját adatkezelésük tekintetében végrehajtsák.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

Az elutasított törlés iránti kérelmekről a Társaság adatvédelmi tisztviselője nyilvántartást vezet, melyről a tárgyévet követő január 31-éig írásban tájékoztatja a Hatóságot.

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

7.5. Az adatkezelés korlátozásához való jog

Az adatkezelés korlátozásához való jog érvényesülése érdekében a Társaság korlátozza az adatkezelést

- ha az érintett vitatja a Társaság, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatok pontosságát, helytállóságát és a kezelt személyes adatok pontossága, helytállósága kétséget kizáróan nem állapítható meg, a fennálló kétség tisztázásának időtartamára
- az adatkezelés jogellenes, így különösen, ha az adatkezelés
    - az adatvédelmi alapelvekkel ellentétes
    - célja megszűnt vagy az adatok további kezelése már nem szükséges az adatkezelés céljának megvalósulásához
    - törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott időtartama eltelt, vagy
    - jogalapja megszűnt és az adatok kezelésének nincs másik jogalapja

  és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását a törlés mellőzését megalapozó jogos érdek (pl. jogi igény előterjesztése) fennállásának időtartamára
- az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy a Társaság jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

Az adatkezelés korlátozásának időtartama alatt a korlátozással érintett személyes adatokkal a Társaság, illetve az általa megbízott vagy rendelkezése alapján eljáró adatfeldolgozó a tároláson túl egyéb adatkezelési műveletet kizárólag az érintett hozzájárulásával, az érintett jogos érdekének érvényesítése céljából vagy törvényben, nemzetközi szerződésben, illetve az Európai Unió kötelező jogi aktusában meghatározottak szerint végezhet.

A Társaság az érintettet, akinek a kérésére korlátozták az adatkezelést, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

A személyes adatok kezelésének korlátozására alkalmazott módszerek közé tartozhat többek között a szóban forgó személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezése vagy a felhasználók számára való hozzáférhetőségük megszüntetése. Az adatkezelés korlátozását az automatizált nyilvántartási rendszerekben alapvetően technikai eszközökkel kell biztosítani, oly módon, hogy a személyes adatokon további adatkezelési műveleteket ne végezzenek el és azokat ne

lehessen megváltoztatni. Azt a tényt, hogy a személyes adatok kezelése korlátozott, egyértelműen jelezni kell a rendszerben.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

Az elutasított korlátozás iránti kérelmekről a Társaság adatvédelmi tisztviselője nyilvántartást vezet, melyről a tárgyévet követő január 31-éig írásban tájékoztatja a Hatóságot.

A Társaság minden olyan címzettet tájékoztat a korlátozásról, akivel, illetve amellyel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére a Társaság tájékoztatja e címzettekről.

7.6. Az adathordozhatósághoz való jog

Ha a személyes adatok kezelése automatizált módon történik, az érintettek számára – a saját adataik feletti rendelkezés további erősítése érdekében – lehetővé kell tenni azt is, hogy az általuk a Társaság rendelkezésére bocsátott, rájuk vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban megkapják, és azokat egy másik adatkezelő részére továbbítsák.

Egy dokumentum akkor tekinthető számítógéppel olvasható formátumú dokumentumnak, ha olyan fájlformátumú, amely lehetővé teszi a szoftveres alkalmazások számára, hogy a benne lévő egyedi adatokat könnyen azonosítsák, felismerjék és kinyerjék.

Az interoperabilitás az eltérő és különböző szervezetek együttműködési képessége a kölcsönösen hasznos és kölcsönösen megállapított közös célok érdekében, ideértve az információk és ismeretek megosztását a szervezetek között az általuk támogatott munkafolyamatokon keresztül, a saját IKT-rendszereik közötti adatcsere segítségével.

Ez a jog abban az esetben gyakorolható, ha az érintett a személyes adatokat a hozzájárulása alapján bocsátotta rendelkezésre, illetve ha az adatkezelés szerződés teljesítéséhez szükséges. E jog nem gyakorolható akkor, ha az adatkezelés jogalapja a hozzájárulástól vagy szerződéstől eltérő egyéb jogalap.

Ha egy adott személyes adatállomány egynél több érintettre vonatkozik, a személyes adatok megszerzéséhez való jog nem sértheti az egyéb érintettek jogait.

Az érintett jogosult arra, hogy az adatokat az adatkezelők egymás között közvetlenül továbbítsák, ha ez technikailag megvalósítható.

A Társaságnak a kérelmet díjmentesen, indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 25 napon belül teljesítenie kell.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet az intézkedés

elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

Az elutasított kérelmekről a Társaság adatvédelmi tisztviselője nyilvántartást vezet, melyről a tárgyévet követő január 31-éig írásban tájékoztatja a Hatóságot.

7.7. A tiltakozáshoz való jog

Bármely érintett számára akkor is biztosítani kell a jogot arra, hogy az egyedi helyzetére vonatkozó adatok kezelése ellen tiltakozzon, ha a személyes adatok jogszerűen kezelhetők, mert az adatkezelésre a Társaság vagy egy harmadik fél jogos érdekei alapján van szükség. Ebben az esetben a Társaság a személyes adatokat nem kezelheti tovább, kivéve, ha 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.

A Társaságnak a tiltakozáshoz való jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívnia annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

A Társaságnak a kérelmet díjmentesen, indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 15 napon belül teljesítenie kell.

Ha a Társaság nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 15 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be a Hatóságnál, és élhet bírósági jogorvoslati jogával.

Ha a Társaság egyetért a tiltakozási kérelemmel, az adatkezelést megszünteti, és a tiltakozásról, illetve intézkedéséről értesíti mindazokat, akik részére korábban az adatokat továbbította.

7.8. Hatósági jogorvoslathoz való jog

Az érintett jogai megsértése esetén panaszával a Hatósághoz fordulhat.

A Hatóság feladata a személyes adatok védelméhez való jog érvényesülésének ellenőrzése és elősegítése.

A Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll. A kérelemben tájékoztatni kell a Hatóságot minden olyan körülményről, amely a vizsgálat lefolytatásához szükséges lehet.

A Hatóság az érintett panaszát csak abban az esetben vizsgálja ki, amennyiben a Hatóságnál tett bejelentését megelőzően már megkereste a Társaságot a bejelentésben megjelölt jogainak gyakorlásával kapcsolatban.

Elérhetőségek:

Nemzeti Adatvédelmi és Információszabadság Hatóság

Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c

Levélcím: 1530 Budapest, Pf.: 5.

Telefon: +36 1 391-1400 Fax: +36 1 391-1410

E-mail: ugyfelszolgalat@naih.hu

Honlap: http://naih.hu

A Hatóság vizsgálati hatáskörében eljárva:

- értesítheti a Társaságot az adatvédelmi előírások feltételezett megsértéséről
- hozzáférést kaphat a Társaságtól a feladatainak teljesítéséhez szükséges minden személyes adathoz és minden információhoz, és
- az uniós vagy nemzeti eljárásjoggal összhangban hozzáférést kaphat az adatkezelő vagy az adatfeldolgozó bármely helyiségéhez, ideértve minden adatkezeléshez használt felszerelést és eszközt.

A Hatóság korrekciós hatáskörében eljárva:

- elmarasztalhatja a Társaságot, ha adatkezelési tevékenysége megsértette az adatvédelmi előírásokat
- utasíthatja a Társaságot, hogy teljesítse az érintettnek a jogai gyakorlására vonatkozó kérelmét
- utasíthatja a Társaságot, hogy adatkezelési műveleteit – adott esetben meghatározott módon és meghatározott időn belül – hozza összhangba az adatvédelmi előírásokkal
- átmenetileg vagy véglegesen korlátozhatja az adatkezelést, ideértve az adatkezelés megtiltását is
- elrendelheti a személyes adatok helyesbítését, vagy törlését, illetve az adatkezelés korlátozását, valamint elrendelheti azon címzettek erről való értesítését, akikkel vagy amelyekkel a személyes adatokat közölték
- legfeljebb 20 000 000 EUR összegű, illetve az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összegű közigazgatási bírságot szabhat ki, azzal, hogy a kettő közül a magasabb összeget kell kiszabni.

7.9. Bírósági jogorvoslathoz való jog

A Hatóság döntésétől függetlenül az érintett jogainak megsértése esetén a Társaság ellen a székhely szerint illetékes bírósághoz fordulhat, melynek eredményeként, jogsérelem megállapítása esetén azon túl, hogy a bíróság az érintetti jogok gyakorlását a Társaság kötelezése révén kikényszeríti, az érintett kártérítésre, illetve sérelemdíjra tarthat igényt.

Azok a személyiségi jog megsértése miatt indult perek, amelyekben felróhatóságtól független (objektív) és nem vagyonjogi szankciók (így a jogsértés tényének bírósági megállapítása, a jogsértés abbahagyására és a jogsértéstől való eltiltásra kötelezés, elégtétel adására kötelezés, a sérelmes helyzet megszüntetése, helyreállításra, megsemmisítésre kötelezés) alkalmazását kéri az érintett,

törvényszéki hatáskörbe tartoznak; míg a fizetési kötelezettséget eredményező szankciók (így a vagyoni előny átengedése, a sérelemdíj vagy kártérítés) érvényesítése a vagyonjogi per fogalma alá tartozik, így a járásbíróság hatáskörében bírálandó el, amennyiben a 30 000 000 millió HUF értékhatárt nem haladja meg. Ha ugyanabban a perben a személyiségi jog megsértése miatt az érintett az objektív szankciók valamelyikét kívánja érvényesíteni a vagyonjogi igénnyel együtt keresethalmazatban, a per elbírálására a törvényszéknek van hatásköre, ugyanis ha valamelyik pertársra vagy kereseti kérelem elbírálására a törvényszéknek van hatásköre, a per a törvényszék hatáskörébe tartozik, feltéve, hogy a pertársaság vagy a keresethalmazat törvény által megengedett.

8. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást is

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 (pl. befolyásolja szerződéses jogait) vagy őt hasonlóképpen jelentős mértékben érintené (pl. e-toborzás történik humán beavatkozás nélkül). E szabály nem alkalmazandó abban az esetben, ha a döntés:

- az érintett és a Társaság közötti szerződés megkötése vagy teljesítése érdekében szükséges
- meghozatalát a Társaságra alkalmazandó olyan uniós vagy nemzeti jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy
- az érintett kifejezett hozzájárulásán alapul.

Ha az automatizált döntéshozatal az érintett és a Társaság közötti szerződés megkötése vagy teljesítése érdekében szükséges, illetve az érintett kifejezett hozzájárulásán alapul,.a Társaság köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy a Társaság részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

Az alábbi táblázat összegzi a profilalkotás és az automatizált döntéshozatal közötti eltéréseket:

Profilalkotás	Automatizált döntéshozatal
Személyes jellemzők automatizált értékelése, amelyet az egyén értékelésére, viselkedésének előrejelzésére használnak	Kizárólag automatizált folyamatban hozott, joghatással járó döntés is születik a profilalkotáson túl
Adatvédelmi hatásvizsgálat Adatvédelmi tisztviselő szakmai tanácsa Tájékoztatás a profilalkotás módszeréről	Adatvédelmi hatásvizsgálat Adatvédelmi tisztviselő szakmai tanácsa Tájékoztatás a profilalkotás módszeréről Jogalap kifejezett hozzájárulás, szerződés vagy jogszabály
Beskatulyáz és valaki ebből esetleg következtetéseket von le	A beskatulyázásnak gépi úton megállapított (kikalkulált) következménye van

Automatizált döntéshozatal esetében - ideértve a profilalkotást is – a Társaságnak adatvédelmi hatásvizsgálatot kell végeznie.

9. Adatfeldolgozó igénybevétele

Ha a Társaság adatfeldolgozót bíz meg az adatkezelési tevékenységek elvégzésével, csakis olyan adatfeldolgozókat vehet igénybe, amelyek megfelelő garanciákat nyújtanak – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – arra vonatkozóan, hogy a GDPR követelményeinek teljesülését biztosító technikai és szervezési intézkedéseket végrehajtják, ideértve az adatkezelés biztonságát is.

Az adatfeldolgozó a Társaság előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja a Társaságot minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget a Társaságnak arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

A Társaság kötelezettségei teljesítésének bizonyítására felhasználható, ha az adatfeldolgozó csatlakozik valamelyik jóváhagyott magatartási kódexhez vagy jóváhagyott tanúsítási mechanizmushoz.

Az adatkezelés adatfeldolgozó általi elvégzését uniós vagy tagállami jog alapján létrejött szerződés vagy egyéb jogi aktus szabályozza, amely köti az adatfeldolgozót az adatkezelővel szemben, meghatározza az adatkezelés tárgyát és időtartamát, az adatkezelés jellegét és céljait, a személyes adatok típusát és az érintettek kategóriáit, figyelembe véve az adatfeldolgozóra az elvégzendő adatkezelés kapcsán háruló konkrét feladatokat és felelősségeket, valamint az érintettek jogait és szabadságait érintő kockázatot is.

Az alábbi táblázat összegzi azokat a tartalmi követelményeket, amelyeket az adatfeldolgozói szerződésben rögzíteni kell:

	Tartalmi elemek
Kötelezően feltüntetendő adatok	az adatfeldolgozás tárgya és időtartama
	az adatfeldolgozás jellege és célja
	az adatfeldolgozással érintett személyes adatok típusa, az érintettek kategóriái
	az adatkezelő jogai és kötelezettségei
Kötelező szerződési feltételek	az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli
	az adatfeldolgozó biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak
	az adatfeldolgozó megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja

	az adatfeldolgozó kizárólag az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása alapján vehet igénybe további adatfeldolgozót
	az adatfeldolgozó köteles együttműködni az adatkezelővel az adatalanyi jogok gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében
	az adatfeldolgozó köteles segíteni az adatkezelőt kötelezettségeinek (adatbiztonság, adatvédelmi incidenskezelés, adatvédelmi hatásvizsgálat) teljesítésében
	az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat
	az adatkezelő rendelkezésére bocsát minden olyan információt, amely a Rendelet 28. cikkében meghatározott 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
Adatfeldolgozó közvetlen felelőssége	az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli
	az adatfeldolgozó kizárólag az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása alapján vehet igénybe további adatfeldolgozót
	az adatfeldolgozó feladatai végrehajtása során a felügyeleti hatósággal – annak megkeresése alapján – együttműködik
	az adatfeldolgozó megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja
	az adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról
	az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek (rendezni kell az incidenskezelési gyakorlatot)
	az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki a Rendeletben előírt esetekben
	ha az adatfeldolgozó a Rendelet 28. cikkét sértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni
Egyéb szerződéses feltételek	az adatfeldolgozó alanya lehet a felügyeleti hatóság vizsgálati/korrekciós hatáskörében lefolytatott eljárásának
	az adatfeldolgozó közigazgatási bírsággal sújtható, ha megsérti a Rendelet előírásait
	az adatfeldolgozóval szemben a Rendelet megsértése esetén további szankciók is alkalmazhatók
	az adatfeldolgozó felelősséggel tartozik az adatkezelés által okozott károkért, ha nem tartotta be a Rendeletben meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el
	a Rendelet megszegéséből eredő felelősségi és kártalanítási szabályokat szerződésben kell rögzíteni

Az adatkezelésnek a Társaság nevében való elvégzését követően az adatfeldolgozó a Társaság választása szerint visszaszolgáltatja vagy törli a személyes adatokat, kivéve, ha az adatfeldolgozóra alkalmazandó uniós vagy nemzeti jog előírja azok tárolását.

A biztonság fenntartása és a Rendeletet sértő adatkezelés megelőzése érdekében a Társaság vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmaz. Ezek az intézkedések biztosítják a megfelelő szintű biztonságot – ideértve a bizalmas kezelést is –, figyelembe véve a tudomány és technológia állását, valamint a végrehajtás kockázatokkal és a védelmet igénylő személyes adatok jellegével összefüggő költségeit. Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat (például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés) mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhoz vezethetnek.

10. Az adatkezelési tevékenységek nyilvántartása

Minden adatkezelő – így a Társaság is - és adatfeldolgozó a Rendeletnek való megfelelés bizonyítása érdekében nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Az adatkezelő és az adatfeldolgozó köteles a Hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.

Az adatkezelői nyilvántartásban a Társaság rögzíti:

- az adatkezelő – azaz a Társaság -, ideértve minden egyes közös adatkezelőt is, valamint az adatvédelmi tisztviselő nevét és elérhetőségeit
- az adatkezelés céljait
- az érintettek, valamint a kezelt adatok körét
- személyes adatok továbbítása vagy tervezett továbbítása esetén az adattovábbítás címzettjeinek – ideértve a harmadik országbeli címzetteket és nemzetközi szervezeteket – körét
- nemzetközi adattovábbítás esetén a továbbított adatok körét, a megfelelő garanciák leírását
- profilalkotás alkalmazása esetén annak tényét
- az adatkezelési műveletek – ideértve az adattovábbítást is – jogalapjait
- a kezelt személyes adatok törlésének időpontját
- a végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását.

Az adatfeldolgozói nyilvántartásban az adatfeldolgozó rögzíti:

- az adatkezelő – azaz a Társaság -, az adatfeldolgozó, a további adatfeldolgozók, valamint az adatfeldolgozó adatvédelmi tisztviselőjének nevét és elérhetőségeit
- a Társaság megbízásából vagy rendelkezése szerint végzett adatkezelési műveletek típusait
- a Társaság kifejezett utasítására történő nemzetközi adattovábbítás esetén a nemzetközi adattovábbítás tényét, valamint a címzett harmadik ország vagy nemzetközi szervezet megjelölését, a megfelelő garanciák leírását

- a végrehajtott műszaki és szervezési biztonsági intézkedések általános leírását.

11. Beépített és alapértelmezett adatvédelem

A természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli a Rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy a Társaság igazolni tudja a Rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit.

Az említett intézkedések magukban foglalhatják

- a személyes adatok kezelésének minimálisra csökkentését
- a személyes adatok mihamarabbi álnevesítését
- a személyes adatok funkcióinak és kezelésének átláthatóságát, valamint azt, hogy
- az érintett nyomon követhesse az adatkezelést, az adatkezelő pedig biztonsági elemeket hozhasson létre és továbbfejleszthesse azokat.

A Társaság a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a Rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

A Társaság megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

A jóváhagyott tanúsítási mechanizmus felhasználható annak bizonyítása részeként, hogy a Társaság teljesíti a beépített és alapértelmezett adatvédelem követelményeit.

12. Adatvédelmi hatásvizsgálat

12.1. Az adatvédelmi hatásvizsgálat célja

Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

Az adatvédelmi hatásvizsgálatra vonatkozó előírások be nem tartása esetén a Hatóság bírságot szabhat ki. Amennyiben az adatkezelést kötelező adatvédelmi hatásvizsgálatnak alávetni, annak elmulasztása, helytelen elvégzése, vagy szükség esetén a Hatósággal való egyeztetés elmulasztása közigazgatási bírsággal sújtható, amelynek összege legfeljebb 10 millió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2%-a; a kettő közül a magasabb összeget kell kiszabni.

12.2. Kockázatalapú megközelítés

A Rendelet arra kötelezi az adatkezelőket, hogy a rendelkezései betartásának biztosítása és bizonyítása céljából hajtsanak végre megfelelő intézkedéseket, többek között a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével. Az adatkezelőknek az adatvédelmi hatásvizsgálat elvégzésére vonatkozó kötelezettségét a személyes adatok kezeléséből eredő kockázatok megfelelő kezelésére vonatkozó általános kötelezettséggel összefüggésben kell értelmezni.

A „kockázat” olyan eshetőség, amely a súlyosság és valószínűség szempontjából jellemez valamilyen eseményt és annak következményeit. A „kockázatkezelés” viszont a Társaság kockázati vonatkozású irányítására és ellenőrzésére szolgáló összehangolt tevékenységek összességeként határozható meg.

Az érintettek jogaira és szabadságaira való utalás elsősorban az adatvédelemhez és a magánélet tiszteletben tartásához való joghoz kapcsolódik, de érinthet más alapvető jogokat, úgymint a szólásszabadságot, a gondolatszabadságot, a mozgás szabadságát, a hátrányos megkülönböztetés tilalmát, a szabadsághoz való jogot, valamint a lelkiismereti és vallásszabadságot is.

12.3. Adatvédelmi hatásvizsgálat tárgya

Az adatvédelmi hatásvizsgálatok azoknak az új helyzeteknek a módszeres elemzésére irányulnak, amelyek a természetes személyek jogaira és szabadságaira nézve magas kockázattal járhatnak, ezért a már vizsgált esetekben (vagyis meghatározott körülmények között és konkrét céllal végzett adatkezelési műveletnél) nincs szükség adatvédelmi hatásvizsgálatra.

12.4. Kötelező adatvédelmi hatásvizsgálat

A kockázatalapú megközelítéssel összhangban nem mindegyik adatkezelési művelet esetében kötelező adatvédelmi hatásvizsgálatot végezni. Ehelyett csak akkor van szükség adatvédelmi hatásvizsgálatra, ha az adatkezelés valamely fajtája valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

A Társaságnak folyamatosan értékelnie kell az adatkezelési tevékenységeikből eredő kockázatokat, hogy felismerje, ha az adatkezelés valamely fajtája valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

Adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek
- személyes adatok különleges kategóriái, vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése; vagy nyilvános helyek nagymértékű, módszeres megfigyelése.

Előfordulhatnak olyan magas kockázatú adatkezelési műveletek, amelyek ugyan nem szerepelnek a felsorolásban, mégis hasonlóan nagy kockázattal járnak. Az ilyen adatkezelési műveletek esetében szintén adatvédelmi hatásvizsgálatot kell végezni.

12.5. Mérlegelendő szempontok

Az alábbiakban összegzett szempontoknak megfelelő adatkezelés esetében lehet szükséges az adatvédelmi hatásvizsgálat elvégzése. Minél több szempontnak felel meg az adatkezelés, annál nagyobb a valószínűsége annak, hogy magas kockázattal jár az érintettek jogaira és szabadságaira nézve.

Értékelés vagy pontozás, ideértve a profilalkotást is	különösen az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők alapján
Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal	adatkezelés, amelynek célja a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések meghozatala → az adatkezelés adott esetben például egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti
Módszeres megfigyelés	érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a nyilvános helyek nagymértékű, módszeres megfigyelése → az ilyen jellegű megfigyelés azért tartozik a figyelembe veendő szempontok közé, mivel a személyes adatok gyűjtése olyan körülmények között folyhat, ahol előfordulhat, hogy az érintettek nem tudják, ki gyűjti és hogyan használja fel adataikat
Különleges adatok vagy fokozottan személyes jellegű adatok	bizonyos adatkategóriák tekinthetők úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat → ezek a személyes adatok különlegesnek minősülhetnek, mivel otthoni vagy magánjellegű tevékenységekhez kapcsolódnak (például elektronikus hírközlési tevékenységekhez, amelyek bizalmassága védendő), kihatnak valamely alapvető jog gyakorlására (például helymeghatározó adatok, amelyek gyűjtése megkérdőjelezi a mozgás szabadságát), vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére (például pénzügyi adatok, amelyek csalásra használhatók)

Nagy számban kezelt adatok	az alábbi tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e: a) az érintettek száma konkrét számadatként vagy a lakosság arányában b) a kezelt adatok mennyisége vagy adatfajták köre c) az adatkezelési tevékenység időtartama vagy állandó jellege d) az adatkezelési tevékenység földrajzi kiterjedése
Adatkészletek egymással való megfeleltetése vagy összevonása	például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon
Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása	az ilyen technológiák használatához újfajta adatgyűjtési és felhasználási formák kapcsolódhatnak, ami magas kockázattal járhat az egyének jogaira és szabadságaira nézve → az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek → az adatvédelmi hatásvizsgálat révén az adatkezelő megismerheti és orvosolhatja az ilyen jellegű kockázatokat
Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok	az ilyen jellegű adatok kezelése azért tartozik a figyelembe veendő szempontok közé, mivel nincs hatalmi egyensúly az érintettek és az adatkezelő között, ami azt jelenti, hogy az egyének adott esetben nem tudják adataik kezelését könnyen engedélyezni vagy ellenezni, illetve nem tudják a jogaikat gyakorolni → a kiszolgáltatott helyzetben lévő érintettek közé sorolhatók a gyermekek, a munkavállalók, a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei, valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki
Az adatkezelés önmagában véve megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek	ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek

Előfordulhat, hogy egy adatkezelési művelet ugyan megfelel a fent ismertetett esetek egyikének, a Társaság azonban mégsem úgy ítéli meg, hogy valószínűsíthetően magas kockázattal jár. Ilyenkor a Társaságnak indokolnia és dokumentumokkal igazolnia kell az adatvédelmi hatásvizsgálat mellőzésének okait, és ezzel összefüggésben az adatvédelmi tisztviselő álláspontját is közölnie/rögzítenie kell.

12.6. Nincs szükség adatvédelmi hatásvizsgálatra

A következő esetekben nincs szükség adatvédelmi hatásvizsgálat elvégzésére:

- ha az adatkezelés valószínűsíthetően nem jár magas kockázattal a természetes személyek jogaira és alapvető szabadságaira nézve
- ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat
- ha az adatkezelési műveleteket a Hatóság meghatározott, azóta változatlan feltételek mellett 2018 májusa előtt ellenőrizte
- ha az adatkezelési művelet jogalappal rendelkezik az uniós vagy nemzeti jogban, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat, kivéve, ha a nemzeti jog kimondta, hogy az adatkezelési műveletet megelőzően hatásvizsgálatot szükséges végezni
- ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (Hatóság által összeállított) nem kötelező jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

12.7. Folyamatban lévő adatkezelési műveletek

Az adatvédelmi hatásvizsgálat elvégzésére vonatkozó követelmény azokra a folyamatban lévő adatkezelési műveletekre vonatkozik, amelyeknél valószínűsíthető, hogy magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, és amelyek esetében megváltoztak a kockázatok, figyelemmel az adatkezelés jellegére, hatókörére, körülményére és céljára.

Az adatvédelmi hatásvizsgálatot érdemes folyamatosan – legalább évente - felülvizsgálni, és rendszeresen újraértékelni.

12.8. Adatvédelmi hatásvizsgálat elvégzésének időpontja

Az adatvédelmi hatásvizsgálatot az adatkezelést megelőzően kell elvégezni. Ez összhangban van a beépített adatvédelem és az alapértelmezett adatvédelem elvével.

Az adatvédelmi hatásvizsgálatot az adatkezeléssel kapcsolatos döntések meghozatalát segítő eszköznek kell tekinteni.

Az adatvédelmi hatásvizsgálatot az adatkezelési művelet kialakítása során a lehető leghamarabb meg kell kezdeni, akkor is, ha az adatkezelési műveletek egy része még nem ismert. A projekt időtartama alatt az adatvédelmi hatásvizsgálat folyamatos aktualizálásával biztosítható az adatvédelem és a magánélet figyelembevétele, és ösztönözhető az előírások betartását előmozdító megoldások kidolgozása. Előfordulhat, hogy a kidolgozási folyamat előrehaladásával meg kell ismételni a hatásvizsgálat egyes lépéseit, mivel bizonyos technikai és szervezési intézkedések kiválasztása befolyásolhatja az adatkezelésből eredő kockázatok súlyosságát vagy valószínűségét.

Az adatvédelmi hatásvizsgálatot nem egyetlen alkalommal, hanem folyamatosan kell végezni.

12.9. Adatvédelmi hatásvizsgálat végrehajtása

A Társaságnak kell gondoskodnia arról, hogy az adatvédelmi hatásvizsgálatot elvégezzék. Az adatvédelmi hatásvizsgálatot elvégezheti a szervezeten belül vagy kívül más is, de a Társaságot terheli végső felelősség e feladat teljesítéséért.

A Társaságnak az adatvédelmi tisztviselő tanácsát is ki kell kérnie, a kapott tanácsokat és a Társaság által hozott döntéseket pedig írásba kell foglalni az adatvédelmi hatásvizsgálat során. Az adatvédelmi tisztviselőnek emellett nyomon kell követnie a hatásvizsgálatot.

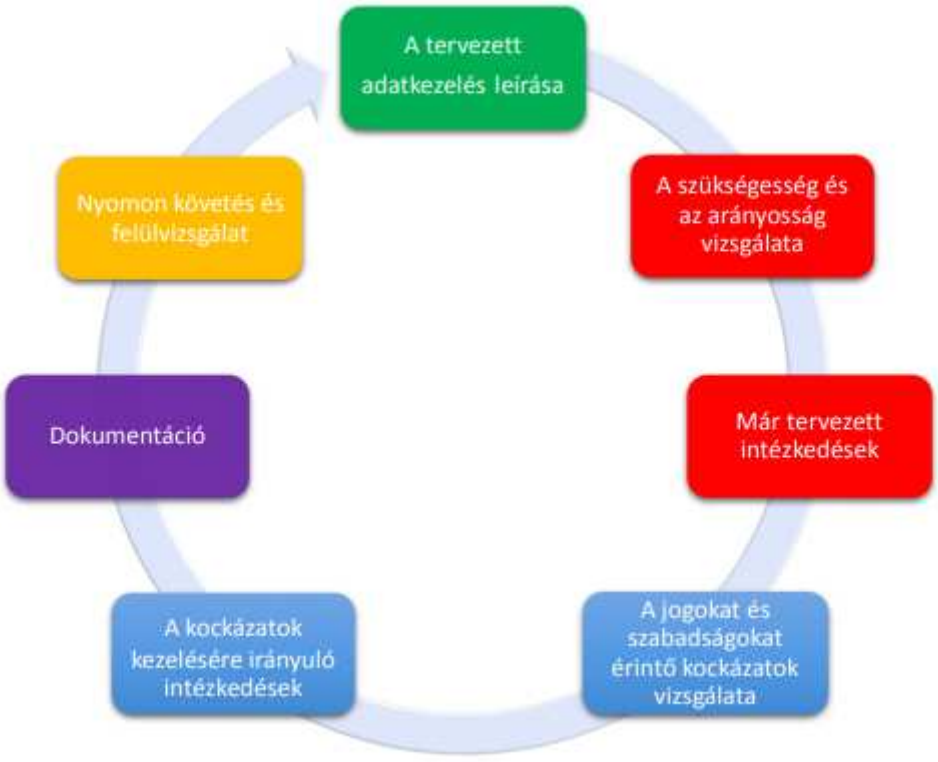
Ha az adatkezelést teljes egészében vagy részben adatfeldolgozó végzi, segítenie kell a Társaságot az adatvédelmi hatásvizsgálat lefolytatásában, és közölnie kell a szükséges információkat.

12.10. Az adatvédelmi hatásvizsgálat elvégzésének folyamata

A Rendelet meghatározza az adatvédelmi hatásvizsgálat alapvető jellemzőit:

- a tervezett adatkezelési műveletek leírása és az adatkezelés céljainak ismertetése
- az adatkezelés szükségességi és arányossági vizsgálata
- az érintett jogait és szabadságait érintő kockázatok vizsgálata
- az alábbiakat célzó intézkedések:
    - a kockázatok kezelése
    - a Rendelettel való összhang igazolása.

Az alábbi ábra az adatvédelmi hatásvizsgálat elvégzésének általános, ismétlődő folyamatát szemlélteti:



A kockázatkezelés szempontjából az adatvédelmi hatásvizsgálat célja, hogy a természetes személyek jogait és szabadságait érintő kockázatokat kezelje a következő eljárások felhasználásával:

- *a körülmények meghatározása:* az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve
- *a kockázatok értékelése:* felmérje a magas kockázat különös valószínűségét és súlyosságát
- *a kockázatok orvoslása:* az említett kockázat mérséklését, a személyes adatok védelmét és a Rendeletnek való megfelelés bizonyítását.

12.11. Hatósággal történő konzultáció

Amennyiben a Társaság nem tud megfelelő intézkedéseket hozni a kockázatok elfogadható szintre való csökkentésére (tehát a fennmaradó kockázatok továbbra is jelentősek), akkor kötelező konzultálni a Hatósággal.

Az alábbi ábra a Rendeletben az adatvédelmi hatásvizsgálattal kapcsolatosan megfogalmazott elveket szemlélteti:

13. Adatvédelmi incidens

13.1. Adatvédelmi incidens típusai

Az adatvédelmi incidens egyfajta biztonsági incidens. Minden adatvédelmi incidens biztonsági incidens, de nem minden biztonsági incidens adatvédelmi incidens. Ez azt jelenti, hogy a biztonság megsértése akkor minősül személyes adatok megsértésének, amikor a megsértett adatok személyes adatok.

Az adatvédelmi incidens típusai:

- titoksértés
- hozzáférhetőségi adatsértés
- sértetlenségi adatsértés.

A körülményektől függően a személyes adatok megsértése a titkossággal, az adatok hozzáférhetőségével, valamint sértetlenségével is kapcsolatos lehet egyidejűleg, illetve előfordulhat ezek bármelyikének kombinációja.

13.2. Adatvédelmi incidens lehetséges következményei

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában

- fizikai
- vagyoni vagy
- nem vagyoni károkat

okozhat a természetes személyeknek, többek között

- a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását,
- a hátrányos megkülönböztetést,
- a személyazonosság-lopást vagy a személyazonossággal való visszaélést,

- a pénzügyi veszteséget,
- az álnevesítés engedély nélküli feloldását,
- a jó hírnév sérelmét,
- a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve
- a szóban forgó természetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.

Következésképpen, amint a Társaság mint adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles a Hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az érintettet a Társaság mint adatkezelő indokolatlan késedelem nélkül tájékoztatja, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket. A tájékoztatásnak tartalmaznia kell

- annak leírását, hogy milyen jellegű az adatvédelmi incidens, valamint
- az érintett a természetes személynek szóló, a lehetséges hátrányos hatások enyhítését célzó javaslatokat.

Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a Hatósággal, és betartva az általa vagy más érintett hatóságok, például bűnüldöző hatóságok által adott útmutatást. Például, ha az érintettek sürgős tájékoztatása a kár közvetlen veszélyének mérsékléséhez szükséges.

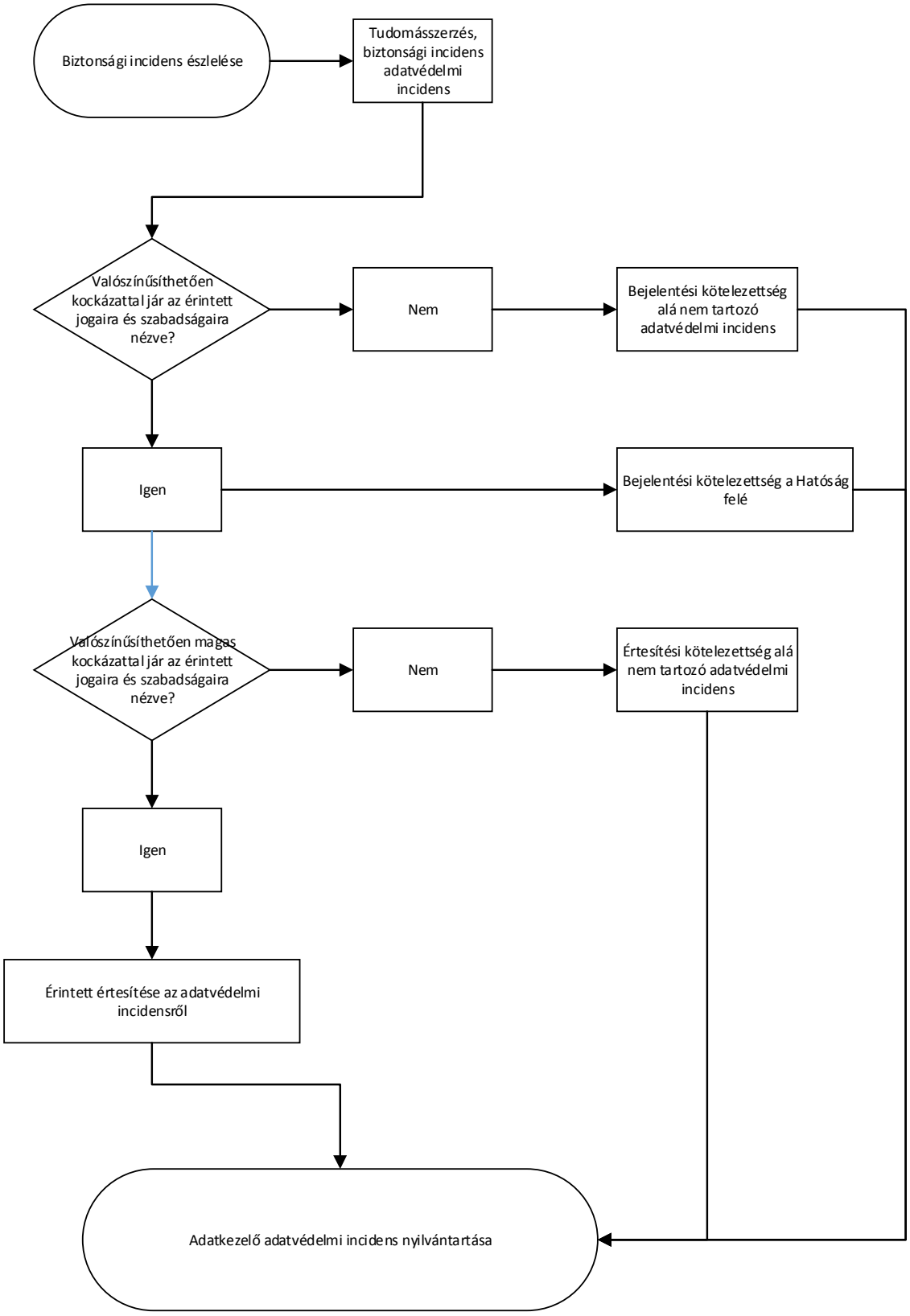
Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen

- az adatvédelmi incidens jellegére és súlyosságára, valamint
- annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira

figyelemmel kell megállapítani.

A Hatóságnak történt bejelentés a Hatóságnak a Rendeletben meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti.

13.3. Az adatvédelmi incidenskezelés folyamatábrája



A Társaság adatvédelmi incidenskezelésének részletes eljárásrendjét az Adatvédelmi incidenskezelési szabályzat tartalmazza.

14. Adatvédelmi tisztviselő

14.1. Az adatvédelmi tisztviselő kijelölése

A Társaság részére adatvédelmi tisztviselő kijelölése kötelező tekintettel arra, hogy a személyes adatok kezelése nagymértékű, illetve nagy számban történik.

Az adatvédelmi tisztviselő lehet a Társaság alkalmazottja, vagy szolgáltatási szerződés keretében láthatja el a feladatait.

Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a tisztviselői feladatok ellátására való alkalmasság alapján kell kijelölni. A szakértői ismeretek szükséges szintjét a Társaság által végzett adatkezelés, valamint az általa kezelendő személyes adatok tekintetében megkövetelt védelem alapján kell meghatározni.

Az adatkezelő vagy az adatfeldolgozó közzéteszi az adatvédelmi tisztviselő nevét és elérhetőségét, és azokat a Hatósággal közli.

A Társaság adatvédelmi tisztviselőjének neve és elérhetőségei:

Név	Dr. Rádi Péter Pál
Cím	1132 Budapest, Váci út 30.
E-mail cím	adatvedelmifelelos@eos-faktor.hu

14.2. Az adatvédelmi tisztviselő jogállása

A Társaság biztosítja, hogy

- az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon
- az adatvédelmi tisztviselő véleményét mindig kellő súllyal figyelembe vegyék az adatvédelmi vonatkozású döntések meghozatala során
- minden releváns információt időben átad az adatvédelmi tisztviselőnek annak érdekében, hogy megfelelő tanácsot adhasson
- haladéktalanul konzultál az adatvédelmi tisztviselővel adatvédelmi incidens bekövetkezése esetén.

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

A Társaság biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. A Társaság az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül a Társaság legfelső vezetésének tartozik felelősséggel.

Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy nemzeti jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

Az adatvédelmi tisztviselő más feladatokat is elláthat. A Társaság biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség. Ez különösen azt jelenti, hogy az adatvédelmi tisztviselő nem tölthet be olyan pozíciót a szervezeten belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit.

14.3. Az adatvédelmi tisztviselő feladatai

Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

- tájékoztat és szakmai tanácsot a Társaság, továbbá az adatkezelést végző alkalmazottak részére a Rendelet, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban
- ellenőrzi a Rendeletnek, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a Társaság személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését
- együttműködik a Hatósággal, és
- az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

15. Általános felelősségi szabályok

A jelen Szabályzatot a Társaság Igazgatóságának elnöke hagyja jóvá. A Szabályzat legalább évente felülvizsgálatra és jóváhagyásra kerül.

A Szabályzat végrehajtásáért saját szervezeti egységeiken belül a felsővezetők felelősek.

Valamennyi munkavállaló kötelezettsége annak bejelentése, ha a Szabályzat megkerüléséről vagy megsértéséről szerez tudomást, vagy ennek gyanúja merül fel. Bejelentés elsődlegesen a közvetlen felettes, a szervezeti egység szerinti felsővezető, vagy a Jogi és Compliance Igazgatóság megkeresése útján tehető.

Az egyes szervezeti egységek vezetői

- felelősek az irányításuk alá tartozó szervezeti egységek adatkezelései jelen Szabályzatnak, a Rendeletnek, valamint az egyéb uniós vagy nemzeti adatvédelmi rendelkezéseknek való megfelelőségéért
- felelősek azért, hogy az általuk vezetett szervezeti egységek adatkezelései során a jelen Szabályzatban foglalt adatbiztonsági előírások maradéktalanul teljesüljenek
- ellenőrzik az adatvédelemmel kapcsolatos előírások, így különösen jelen Szabályzat rendelkezéseink betartását
- az adatvédelmi tisztviselő segítségét kérik, amennyiben adatkezeléssel összefüggésben kérdésük merül fel
- együttműködnek az adatvédelmi tisztviselővel az adatvédelemmel kapcsolatos szabályok érvényesülése érdekében
- biztosítják, hogy beosztottaik az adatvédelmi tisztviselő által szervezett, illetve tartott adatvédelemmel és adatbiztonsággal kapcsolatos képzéseken részt vehessenek.

A tényleges adatkezelést végző alkalmazott feladatai ellátása során

- kezeli és megőrzi a birtokába került adatokat
- ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására
- gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá
- betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat
- indokolatlan késedelem nélkül jelzi a közvetlen felettese részére, amennyiben az adatvédelmi ügyben a felettes vagy az adatvédelmi tisztviselő segítségére szorul.

16. Adattovábbítás

16.1. EGT-államba történő adattovábbítás, belföldi adattovábbítás

Személyes adatot Magyarországon belül, az EGT-államba, valamint az Európai Unió működéséről szóló szerződés V. címének 4. és 5. fejezete szerint létrehozott ügynökségek, hivatalok és szervek részére továbbítani csak a jelen Szabályzatban meghatározott valamely jogalap alapján lehet.

Az EGT-államba, valamint az Európai Unió működéséről szóló szerződés V. címének 4. és 5. fejezete szerint létrehozott ügynökségek, hivatalok és szervek részére irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

16.2. Nemzetközi adattovábbítás

Személyes adatot a Társaság harmadik országban, továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére akkor továbbíthat, ideértve a közvetett adattovábbítást is, (a továbbiakban együtt: nemzetközi adattovábbítás), ha

- a nemzetközi adattovábbításhoz az érintett kifejezetten hozzájárult, vagy
- a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, valamint
    - annak során az adatkezelés jogalapja biztosított, és

  - a harmadik országban, illetve a nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó tekintetében a továbbított személyes adatok megfelelő szintű védelme biztosított, vagy
- a nemzetközi adattovábbítás kivételes esetekben szükséges.

A személyes adatok megfelelő szintű védelmét – az ellenkező bizonyításáig – biztosítottnak kell tekinteni, ha

- az Európai Unió kötelező jogi aktusa azt megállapítja
- az Európai Unió kötelező jogi aktusa hiányában vagy alkalmazásának felfüggesztése esetén az érintetteknek jogai érvényesítésére vonatkozó garanciális szabályokat tartalmazó nemzetközi szerződés alkalmazandó Magyarország és azon harmadik ország, illetve nemzetközi szervezet között, amelynek joghatósága kiterjed a nemzetközi adattovábbítás címzettjére, vagy
- az Európai Unió kötelező jogi aktusa, illetve a harmadik ország és Magyarország között az adatkezelés, illetve az adatfeldolgozás garanciális szabályait tartalmazó nemzetközi szerződés hiányában vagy alkalmazásának felfüggesztése esetén a nemzetközi adattovábbítást megelőzően a Társaság a személyes adatok továbbításának valamennyi körülményét megvizsgálta és megállapította, hogy a személyes adatok megfelelő szintű védelme tekintetében megfelelő garanciák állnak fenn.

Ilyen megfelelő garanciák lehetnek például:

- kötelező erejű vállalati szabályok (BCR) alkalmazása
- az Európai Bizottság által elfogadott általános adatvédelmi kikötések, illetve a Hatóság által elfogadott és az Európai Bizottság által jóváhagyott általános adatvédelmi kikötések
- jóváhagyott magatartási kódex a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő – ideértve az érintettek jogaira vonatkozó – garanciákat
- jóváhagyott tanúsítási mechanizmus a harmadik országbeli adatkezelő vagy adatfeldolgozó arra vonatkozó, kötelező erejű és kikényszeríthető kötelezettségvállalásával együtt, hogy alkalmazza a megfelelő garanciákat, ideértve az érintettek jogait illetően is.

Ha a személyes adatok megfelelő szintű védelme nem vélelmezhető, nemzetközi adattovábbítás kizárólag abban az esetben lehetséges, ha

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy tájékoztatták az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról
- az adattovábbítás az érintett és a Társaság közötti szerződés teljesítéséhez, vagy az érintett kérésére hozott, szerződést megelőző intézkedések végrehajtásához szükséges
- az adattovábbítás a Társaság és valamely más természetes vagy jogi személy közötti, az érintett érdekét szolgáló szerződés megkötéséhez vagy teljesítéséhez szükséges
- az adattovábbítás jogi igények előterjesztése, érvényesítése és védelme miatt szükséges.

Banktitok harmadik személy részére történő kiadására a Hpt. 161-164. §-ában foglalt rendelkezések irányadóak.

17. Adatbiztonsági előírások

A Társaság a kezelt személyes adatok megfelelő szintű biztonságának biztosítása érdekében az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető – így különösen az érintettek különleges adatainak kezelésével járó – kockázatok mértékéhez igazodó műszaki és szervezési intézkedéseket tesz.

A kockázatok mértékéhez igazodó műszaki és szervezési intézkedések kialakítása és végrehajtása során a Társaság figyelembe veszi az adatkezelés összes körülményét, így különösen a tudomány és a technológia mindenkori állását, az intézkedések megvalósításának költségeit, az adatkezelés jellegét, hatókörét és céljait, továbbá az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.

A Társaság meghatározott intézkedésekkel biztosítja különösen:

- az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását
- az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását
- az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását
- az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását
- azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá
- azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére
- azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe
- a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását
- azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
- azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével sem lehessen megváltoztatni.

A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében biztosítani kell, hogy e külön nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

Az alábbi táblázat összegzi azokat az indokolt adatbiztonsági kontrollokat, amelyeket a személyes adatok biztonsága érdekében biztosítani kell:

	Megelőző	Észlelő	Reagáló/Korrekciós
Szervezeti/adminisztratív	szabályozás felelősök kijelölés tudatosítás	Megfelelőség nyomon követése	BCP és DRP szabálytalanságok kezelése
Fizikai	hozzáférés korlátozás (végponthoz, hálózathoz, adathordozóhoz) kontrollált beléptetése	fizikai őrzés monitoring tűzjelzés, vízjelzés	oltóberendezések tartalék áramforrás georedundancia
Határvédelem	Tűzfal, IPS, VPN malware védelem redundáns architektúra tartalomszűrés	malware védelem sérülékenységi vizsgálat	DDos védelem incidenskezelés
Hálózat	titkosított továbbítás zónázás redundáns architektúra	SIEM	Tartalékútvonal
Végpont	felhasználó hitelesítés malware védelem	integritásvédelem malware védelem	Tartalék eszközök biztonsági javítások telepítése
Alkalmazás	biztonságos fejlesztés WAF biztonságos konfiguráció	SIEM sérülékenység-vizsgálat	biztonsági javítások telepítése
Adat	biztonsági mentés jogosultságkezelés adatvagyon leltár	hozzáférés monitorozás DLP	helyreállás mentésből incidensbejelentés

Az informatikai adatbiztonsági előírások részletes meghatározását külön szabályzat, az Információbiztonsági Szabályzat tartalmazza.

18. Záró rendelkezések

Jelen Szabályzat kihirdetésével egyidejűleg a korábban kiadott Szabályzat hatályát veszti, és jelen Szabályzat lép a helyébe.