JÓVÁHAGYÓ LAP / APPROVAL SHEET

Készítette:
Prepared by:

Minőségügyi mérnök

Dátum / Date: 2021.02.01.

A kiadást engedélyezte:
Authorized for release by:

Tóth Sándor
IT Igazgató

Dátum / Date: 2021.02.01.

Jóváhagyta:
Approved by:

Ügyvezető Igazgató

Dátum / Date: 2021.02.01.

TARTALOM JEGYZÉK

MÓDOSÍTÁSI ÉS ELOSZTÁSI JEGYZÉK

A dokumentum módosításának okát és a módosítás érvénybe lépésének dátumát, az elosztási lista szerinti közzétételét az alábbi táblázatban kell napra készen vezetni. A napra készen tartás a folyamatgazda feladata, aki az adott revízió közzétételét az aláírásával igazolja a táblázat megfelelő rovatában.

Elosztási lista:	**szervezet neve:**	**elérés módja:**
1.	ACE	papíralapú példány
2.	Hatóság	ftp-szerver e-másolat
3.		

Revízió	*Módosítás dátuma*	*Módosítás oka*	*Kiadva*
00	2021. 02. 01.	első kiadás	2021. 02. 01.

1. ÁLTALÁNOS RENDELKEZÉSEK

Az **AEROPLEX Közép-Európai Légijármű Műszaki Központ Kft.** a továbbiakban: **Adatkezelő**) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), valamint az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR) alapján a személyes adatok védelmét, illetve közérdekű adatokkal kapcsolatos feladatok ellátásnak rendjét a következők szerint állapítja meg.

1.1. A szabályzat célja

Jelen szabályzat célja, hogy

- ismertesse az Adatkezelő munkavállalóival ill. az Adatkezelő rendszereinek felhasználóival a személyes adatok kezelése során érvényesítendő szabályokat és eljárásokat,
- a társaság tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülésének biztosítása, illetve az általa kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat.

1.2. A szabályzat hatálya

a) **Szervezeti hatálya:** kiterjed a Társaság minden olyan szervezeti egységére, amely tevékenysége során személyes adatot kezel.

b) **Személyi hatálya:**

- kiterjed az Adatkezelő valamennyi munkavállalójára, a munkavégzésre irányuló egyéb jogviszonyban álló magánszemélyekre, valamint az Adatfeldolgozási szerződésekben rögzítettek szerint, az Adatfeldolgozási szerződést aláírt külső szervezetek mindazon munkavállalóira és egyéb közreműködőire, akik az Adatkezelő informatikai rendszereit használják, üzemeltetik, működtetik vagy fejlesztik, azaz az Adatkezelő adatvagyonához hozzáférhetnek.
- kiterjed a Társaság valamennyi munkavállalójára, és a Társaság feladatainak végrehajtásában polgári jogi jogviszonyban közreműködő azon személyekre, akik tevékenységük során ilyen adatot kezelnek.

c) **Tárgyi hatálya:** a személyes adatokkal kapcsolatos adatkezelésre terjed ki, beleértve az adattovábbítást is.

A szabályzat hatálya nem terjed ki az informatikai eszközökkel összefüggő technikai adatvédelemre, amelyről az Informatikai Biztonsági Szabályzat (IBSZ) rendelkezik.

1.3. Vonatkozó jogszabályok

(1) Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),

(2) Az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR),

(3) A GDPR 29-es cikk szerint létrehozott Adatvédelmi Munkacsoport iránymutatásai,

(4) A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlásai.

1.4. Értelmező rendelkezések

a) ***adatkezelő szerv:*** a Társaság;

b) ***adatbirtokos:*** a Társaság adatkör szerint érintett szervezeti egységének azon vezetője, aki önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja;

c) ***személyes adat:*** a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) szerinti személyes adat;

d) ***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;

e) ***adatfeldolgozó:*** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;

f) ***adattovábbítás:*** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

g) ***üzleti titok:*** az üzleti titok védelméről szóló 2018. évi LIV. törvényben meghatározott üzleti titok;

h) ***nyilvánosságra hozatal:*** az adat bárki számára történő hozzáférhetővé tétele;

i) ***érintett:*** bármely információ alapján azonosított vagy azonosítható természetes személy;

j) ***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;

k) ***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;

A szabályzatban szereplő fogalmakat a GDPR 4. cikkében és az Info tv. 3. §-ában meghatározott tartalommal kell értelmezni és alkalmazni.

1.5. A munkavállalók adatvédelemmel kapcsolatos tájékoztatása

A munkavállalók adatvédelemmel kapcsolatos tájékoztatását jelen szabályzat 1. számú melléklete tartalmazza.
1.számú melléklet: Adatvédelmi tájékoztató a társaság munkavállalói részére

2. RÉSZLETES RENDELKEZÉSEK

2.1. A személyes adatok kezelésére vonatkozó elvek

A Társaság a személyes adatok kezelése során az alábbi elveket alkalmazza:

a) Jogszerűség, tisztességes eljárás és átláthatóság elve

A személyes adatok kezelésére csak és kizárólag a megfelelő jogalap megléte esetén kerülhet sor. Az adatkezelésre vonatkozó jogszabályok betartásán túl, a Társaság tiszteletben tartja az érintettek személyes adataikhoz fűződő jogát és az emberi méltóságát az adatkezelés során. A Társaság az adatkezelést átláthatóan végzi, az adatkezelésről hatékony és teljes körű tájékoztatást nyújt az érintettek részére.

b) Célhoz kötöttség elve

A Társaság kizárólag előre meghatározott, jogszerű célból kezel adatokat, a céllal, célokkal összeegyeztethető módon.

c) Adattakarékosság elve

A Társaság kizárólag annyi és olyan személyes adatot kezel, mely a meghatározott cél teljesüléséhez szükséges. A Társaság az adatkezeléskor meghatározott cél megvalósulását követően – kivéve, ha jogszabály ezzel ellentétesen rendelkezik, vagy az adattárolás olyan adatkezelési cél elérése érdekében lehetséges, mely összeegyeztethető az eredeti adatkezelési céllal – a személyes adatokat törli.

d) Pontosság elve

A Társaság az általa kezelt személyes adatok pontosságát az adatbirtokos folyamatos felülvizsgálata és az érintett helyesbítéshez való joga gyakorlásának biztosításával garantálja.

e) Korlátozott tárolhatóság elve

A Társaság a személyes adatot tartalmazó dokumentumot az adatkezelési cél elérését vagy az adatkezelési idő leteltét követően – kivéve, ha jogszabály ezzel ellentétesen rendelkezik, vagy az adattárolás olyan adatkezelési cél elérése érdekében lehetséges, mely összeegyeztethető az eredeti adatkezelési céllal – törli vagy anonimizálja, amely révén az érintett a továbbiakban nem azonosítható.

f) Integritás és bizalmas jelleg elve

A Társaság biztosítja a jogosultak számára, hogy az adatokhoz hozzáférjenek, továbbá gondoskodik a személyes adatok védelméről.

g) Elszámoltathatóság elve

A Társaság valamennyi személyes adat kezelésével összefüggő tevékenységét visszakövethető módon dokumentálja, és ezáltal biztosítja az adatkezeléssel kapcsolatosan megtett intézkedések átláthatóságát.

h) Az adatkezelés általános elvei

- Adatkezelő a személyes adatkezelésre vonatkozó gyakorlatát a GDPR, a vonatkozó hatályos egyéb jogszabályok és az adatvédelemre vonatkozóan a szabályzat elkészítésének idején elérhető „jó gyakorlatok" (best practice) alapján alakította – alakítja ki.

- Az adatok kezelésére csak előre meghatározott, az Érintettel előre közölt, tisztességes célból kerül sor. Az adatkezelés célhoz kötöttsége az adatkezelés egész folyamatában és az adatok hozzáférhetővé tétele, ill. esetleges továbbítása esetén is érvényesül.

- Adatkezelő nem kíván olyan adatot kezelni, amely az adatkezelés céljának eléréséhez szükségtelen, ezért igyekszik minden tőle telhetőt megtenni annak érdekében, hogy csak olyan személyes adat adatkezelésére kerüljön sor, amely feltétlenül szükséges az adatkezelés céljának eléréséhez. Ezen kívül minden olyan esetben törekszik az Adatkezelő az adatkezelés minimalizálására, amennyiben ezt az informatikai és az adatkezelés céljának eléréséhez fűződő érdek engedi.

- Adatkezelő folyamatosan gondoskodik az adatok naprakészen tartásáról, amennyiben a munkafolyamatok során kiderül, hogy egy adat elavult, kezdeményezi a módosítását az informatikai rendszerek és az adatkezelés céljának eléréséhez fűződő érdek engedi.

- Adatkezelő törli a személyes adatot minden olyan esetben, amikor az adatkezelés célja megszűnt és jogszabályi kötelezettség, vagy jogos érdek nem áll fenn az adat további tárolásával, kezelésével kapcsolatban.

- Adatkezelő gondoskodik arról, hogy az Érintettek teljeskörű tájékoztatást kapjanak a róluk kezelt személyes adatokról, valamint az adatkezelés körülményeiről. Bármely Érintett kérheti adatai helyesbítését, valamint, amennyiben az adatkezelésre az Adatkezelő jogos érdekére tekintettel kerül sor vagy ha erre jogszabály kifejezetten lehetőséget biztosít – tiltakozhat a személyes adatai kezelése ellen. Az Érintettek az általuk sérelmesnek vélt adatkezelés miatt a Nemzeti Adat-és Információszabadság Hatósághoz, valamint bírósághoz fordulhatnak.

- Adatkezelő biztosítja, hogy bármely Érintett mindenféle negatív jogkövetkezmény nélkül kérheti azon személyes adatainak törlését, amelyet az Adatkezelő az önkéntes hozzájárulása alapján kezel. Amennyiben az adatok törlésére valamilyen jogszabályi tilalom vagy Adatkezelő jogos érdeke miatt nem kerülhet sor, akkor az Adatkezelő a vonatkozó személyes adatokat zárolja, és a zárolásról az Érintettet tájékoztatja.

- Az adatkezelési műveleteket Adatkezelő úgy igyekszik tervezni és végrehajtani, hogy az Érintettek személyes adatainak bizalmas kezelése, az adatok védelme megfelelő módon biztosított legyen. Az Adatkezelő vállalja, hogy a technika mindenkori állását figyelembe véve – megteszi azokat a technikai és szervezési intézkedéseket, valamint kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Ennek keretében az Adatkezelő az adatokat különösen a jogosulatlan hozzáféréstől, azok megváltoztatásától, jogosulatlan továbbításától, azok nyilvánosságra hozatalától, törlésétől vagy megsemmisítésétől, valamint a

véletlen megsemmisülésétől és sérülésétől igyekszik megvédeni, továbbá igyekszik fellépni az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

- Az Adatkezelő Adatfeldolgozó igénybevétele esetén vállalja, hogy csak olyan Adatfeldolgozót vesz igénybe, aki vállalja, hogy a személyes adatok védelme érdekében megteszi a szükséges intézkedéseket, valamint betartja az Adatkezelő szabályzatait és egyedi utasításait. A kiválasztás során az Adatkezelő törekszik arra, hogy csak olyan Adatfeldolgozót vegyen igénybe, amely megfelelő biztosítékokat nyújt arra nézve – különösen szakmai, megbízhatóság és erőforrások vonatkozásában –, hogy az adatvédelmi követelmények teljesülését biztosító technikai és szervezési intézkedéseket végrehajtja, ideértve az adatkezelés biztonságát is.

2.2. Az adatkezelések jogalapja

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

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) 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;
c) az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé.

2.3. A személyes adatok védelmével kapcsolatos eljárás

1. A személyes adatok védelme

(1) Amennyiben olyan adatot kell megszerezni, melyet közokirat tartalmaz, az eredeti okiratot vagy annak közjegyző általhitelesített másolatát be kell mutatni.

(2) Az adatot megszerző szervezeti egység legkésőbb a személyes adatok megszerzésének időpontjában –ha lehetséges még azt megelőzően -az érintettet köteles tájékoztatnia GDPR 13. illetve 14. cikkében és az Info tv.-ben meghatározott adatkezelés részleteiről.

(3) Hozzájáruláson alapuló adatkezelés esetén az adatot megszerző szervezeti egység köteles beszerezni az érintett hozzájárulását a GDPR 7. cikkének figyelembevételével.

2. Társaságon belüli adatátadás

Az adatkezelő szervezeti egység személyes adatot–a szükséges mértékben és ideig – csak olyan adatkezelésre jogosult szervezeti egységhez továbbíthat, amelynek feladata ellátásához a személyes adatok megismerése és kezelése szükséges és az adatkezelésre megfelelő jogalappal rendelkezik.

Amennyiben a két szervezeti egység között a személyes adat átadásával kapcsolatos bármely kérdésben véleményeltérés van, úgy -az adatvédelmi felelős szakmai tanácsának figyelembevételével -közös felettesük dönt.

3. Adattovábbítás harmadik személy részére

(1) A Társaság szervezeti egysége az adattovábbítás feltételeinek meglétét minden egyes személyes adattal összefüggésben köteles ellenőrizni, így különösen azt, hogy az igényelt adatokra vonatkozóan az adatok kezelőjének minősül-e.

(2) Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha a személyes adatot kezelő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) pedig rendelkezik az adat kezeléséhez szükséges jogalappal vagy az érintett írásos – a vonatkozó jogszabályi elvárásoknak megfelelő tartalmú – hozzájárulásával és az adatkérés célja mindezzel összhangban van. Az adattovábbítás feltételeinek megléte és a célhoz kötöttség a jogszerűség együttes követelménye.

(3) Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – törvényben kötelezően előírt adattovábbítás esetét kivéve – a Társaság ügyvezető igazgatójának vagy az általa kijelölt vezetőnek a hatáskörébe tartozik, amellyel kapcsolatban kikérheti az adatvédelmi felelős véleményét. Az adatigénylés abban az esetben teljesíthető, ha az tartalmazza:

a) az adatigénylés célját, jogalapját;

b) a kért adatok körének pontos meghatározását;

c) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

(4) Az adattovábbítás történhet kérelem alapján egyedi adatszolgáltatással, továbbá – törvény ilyen tartalmú rendelkezése vagy erre vonatkozó megállapodás alapján – közvetlen hozzáférés biztosításával.

(5) A személyes adat továbbítására irányuló adattovábbítás törvényben meghatározott feltételek fennállása esetén, ennek hiányában az érintett előzetes és önkéntes hozzájárulása alapján teljesíthető.

(6) Az elsődleges adatkezelő szervek –illetve feladatuk ellátásához szükséges módon és mértékben az elsődleges adatkezelő szervek által felhatalmazott szervezeti egységek –feladata az adattovábbítás végrehajtása. Az adattovábbítás előtt be kell szerezni az adatvédelmi felelős egyetértését.

(7) Közigazgatási szerv, bíróság, ügyészség, rendőrség vagy más nyomozóhatóság, továbbá nemzetbiztonsági szolgálat adatszolgáltatási tárgyú megkeresését a ügyvezető igazgató részére kell felterjeszteni.

Ebben az esetben az ügyvezető igazgató jelöli ki az adatszolgáltatót.

(8) Amennyiben az adatkezelő szerv olyan adatra vonatkozó megkeresést kap, melynek jogszerűségét nem tudja megítélni, köteles azt az adatvédelmi felelős útján a ügyvezető igazgatónak jelenteni. A ügyvezető igazgató az adatvédelmi felelős állásfoglalása ismeretében dönt a megkeresés teljesítéséről.

(9) Személyes adatok továbbítása során, amennyiben az belső vagy külső küldeményként történik, biztosítani kell, hogy zártan kerüljön feladásra.

(10) Személyes adatok elektronikus továbbítása során az Informatikai Biztonsági Szabályzat (IBSZ) szerint szükséges eljárni.

2.4. A Társaság, mint adatfeldolgozó

(1) Azon jogviszonyokban, ahol a Társaság, mint adatfeldolgozó vesz részt, az adatkezelés jogalapját az adatkezelővel megkötött adatfeldolgozási szerződés képezi a GDPR 28. cikkében meghatározottak szerint.

(2) Az adatfeldolgozási szerződés keretein belül végzett személyes adatkezelésre, az érintett általi adatigénylésre a jelen szabályzat rendelkezésétől eltérően az adatkezelővel megkötött adatfeldolgozási szerződés rendelkezéseit kell megfelelően alkalmazni.

2.5. Az adatvédelmi felelős

(1) Az Adatvédelmi felelős a jogszabályban meghatározott feltételeknek megfelelő személy lehet. Az adatvédelmi felelőst a igazgató jelöli ki, közvetlenül a ügyvezető igazgatónak tartozik felelősséggel.

(2) Az adatvédelmi felelős feladatait a GDPR 39. cikke rögzíti.

(3) Az adatvédelmi felelős nevéről és elérhetőségéről a Társaság munkatársait tájékoztatni kell, a társaság honlapján nyilvánosan közzéteszi, valamint a Hatóság nyilvántartásába be kell jelenteni.

(4) A ügyvezető igazgató biztosítja az adatvédelmi felelős számára meghatározott feladata kapcsán eljárva a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat rendelkezésére bocsátja.

(5) A Társasággal foglalkoztatási jogviszonyban álló személyek a személyes adataik kezeléséhez és jogaik gyakorlásához kapcsolódó valamennyi kérdésben a hivatali út betartása nélkül, közvetlenül fordulhatnak az adatvédelmi felelőshöz.

(6) A Társaság valamennyi foglalkoztatottja és szervezeti egysége köteles együttműködni az adatvédelmi felelőssel.

(7) Az adatvédelmi felelős szakmai tanácsát az adatkezelő szervezeti egység az alábbi esetekben köteles kikérni:
a) olyan megállapodás, szerződés, szabályzat esetén, mely érinti az Társaság adatkezelési tevékenységét;
b) adatkezelési tájékoztató tartalmával kapcsolatban az érintetteknek történő átadás előtt.

(8) Amennyiben az adatvédelmi felelős adatvédelmi szempontból egyetért a véleményezésre megküldött dokumentummal, azt **„Adatvédelmi szempontból egyetértek”** szöveggel, dátummal és aláírással látja el. Egyet nem értés esetén a dokumentumot **„Adatvédelmi szempontból nem értek egyet”** szöveggel, dátummal és aláírással látja el.

2.6. Adatkezelési tevékenységek nyilvántartása

(1) A GDPR 30. cikkében meghatározott nyilvántartást az adatvédelmi felelős vezeti.

(2) Az adatkezelő szervezeti egységek saját adatkezelési tevékenységükről naprakész nyilvántartást vezetnek a GDPR 30. cikkében meghatározott adatokról, az érintett tájékoztatására vonatkozó információkról a mellékletben meghatározott formanyomtatványon, amelyet megküldenek az adatvédelmi felelős részére, aki ezek alapján vezeti az (1) bekezdés szerinti nyilvántartást.

(3) Az adatkezelő szervezeti egységek kötelesek haladéktalanul tájékoztatni az adatvédelmi felelőst, ha az általuk végzett adatkezelési tevékenységben – így különösen a kezet adatok körében, az érintettek kategóriájában, az adatkezelés céljában, az adatkezelés időtartamában –változás következik be.

1. ***számú melléklet: Adatvédelmi nyilvántartás***
2. ***számú melléklet: A társaság adatkezelői által nyilvántartott adatok***

2.7. Az adatok védelme

(1) A Társaság minden ésszerű intézkedést megtesz annak érdekében, hogy az általa kezelt adatok illetéktelenek számára ne legyenek hozzáférhetőek.
Az Társaság kiemelt figyelmet fordít az adatok bizalmas kezelésére.

(2) Az elektronikus adatokhoz korlátozott a hozzáférés, jelszavas védelem működik.

(3) A fenti célokérdekében az Társaság a kezelésében lévő elektronikus adatokat kizárólag a saját rendelkezése alatt lévő szervereken tárolja az Informatikai Biztonsági Szabályzatban (IBSZ) foglaltak szerint.

(4) Az Társaságmal minden munkaviszonyban vagy megbízási jogviszonyban álló személy, aki személyes adat birtokába jut, ilyet munkaköre vagy megbízatása alapján kezel, köteles védeni és őrizni a személyes adatokat, és úgy eljárni, hogy azok megfelelő védelmét biztosítsák.

2.8. Adatvédelmi hatásvizsgálat

(1) A GDPR 35. cikke szerinti adatvédelmi hatásvizsgálatot az adatkezelő, illetve adatfeldolgozó szervezeti egységek végzik, melynek során az adatvédelmi felelős szakmai tanácsát ki kell kérni.

(2) Az adatbirtokos abban az esetben végez előzetes hatásvizsgálatot tervezett vagy folyamatban lévő adatkezelésnél, ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, vagy az adatkezelés kockázatának és lényeges körülményének – különösen az adatkezelés technológiájának – megváltoztatása esetén.

(3) Az adatbirtokos a kockázatelemzési feladata kapcsán kikérheti a tervezett, illetve megváltozott adatkezelés által érintett személyek véleményét.

(4) Az adatbirtokos a kockázatelemzési feladata kapcsán kikéri a döntés végrehajtásáért felelős szakterület, az Informatikai vezetőnek, mint az elektronikus információs rendszer biztonságáért felelős szervezet vezetőjének vagy az elektronikus biztonságért felelős személynek és a rendszerek üzemeltetésében részt vevő szervezeteknek, valamint az adatvédelmi felelősnek a véleményét.

(5) Ha a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel – az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve – valószínűsíthetően magas kockázatot nem azonosít, vagy megállapítást nyer, hogy az adatkezelés az adatvédelmi hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az adatbirtokos írásban rögzíti.

(6) Az adatbirtokos köteles az előkészített adatkezelés esetén az adatkezelési tevékenységek nyilvántartásáról szóló dokumentumot kitölteni és azt az adatvédelmi felelősnek megküldeni.
Az adatvédelmi felelős a megküldött dokumentumot az adatkezelési tevékenységek nyilvántartásába bejegyzi.

(7) Amennyiben az adatbirtokos az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít, vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn, – a döntése alapjául szolgáló legfontosabb szempontokat írásban megjelölve – adatvédelmi hatásvizsgálat lefolytatását kezdeményezi a ügyvezető igazgatónál.

(8) A ügyvezető igazgató az adatbirtokos javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását, vagy írásban rögzíti mellőzésének okait és az adatvédelmi felelős kapcsolódó álláspontját. Az adatvédelmi hatásvizsgálat lefolytatásáig vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

(9) Az adatbirtokos és az adatkezelés által érintett személyek az adatvédelmi hatásvizsgálat eredményeiről összefoglaló jelentést készítenek, amelyet a ügyvezető igazgató hagy jóvá.

(10) Az adatvédelmi felelős a jelentés alapján az adatkezelést bevezeti az adatkezelési tevékenységek nyilvántartásába.

(11) Ha az adatvédelmi hatásvizsgálat arra az eredményre jut, hogy a tervezett adatkezelés jelentette kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon – vagy azt jogszabály kötelezően előírja –, akkor az adatkezelő szerv előzetes konzultációt kezdeményez a Hatóságnál.

2.9. Az adatfeldolgozás

(1) A Társaság adatfeldolgozót vehet igénybe. Az adatfeldolgozó az adatkezelési műveletekhez kapcsolódó technikai feladatokat végzi, és e minőségében gyakorolja az adatkezelő Társaság által átruházott jogosultságokat, teljesíti kötelezettségeit.

(2) Az adatfeldolgozásra vonatkozó megállapodást írásba kell foglalni. Amennyiben az adatfeldolgozóként igénybe venni kívánt szervre vagy személyre az utasítás hatálya nem terjed ki, akkor a megállapodásban kell érvényesíteni az adatfeldolgozóval szemben e címben foglalt előírásokat.

(3) Adatfeldolgozó igénybevétele esetén az adatkezelés céljának meghatározására, az adatkezelésre vonatkozó érdemi döntések meghozatalára az adatkezelő jogosult.

(4) Az adatfeldolgozó tevékenységi körén belül, illetve az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, továbbá minden olyan jogsértésért, amit az adatkezelő utasításának vagy az adatfeldolgozással összefüggésben kötött megbízási szerződésben foglaltak megszegésével okozott.

Az adatfeldolgozók nyilvántartását az Adatvédelmi felelős vezeti. ***2. számú melléklet: Adatvédelmi nyilvántartás***

2.10. Adatbiztonsági előírások

(1) Az adatkezelő szerv, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról.

Az elektronikusan kezelt adatállományok tekintetében biztosítani kell, hogy a különböző nyilvántartásokban tárolt adatok – törvény eltérő rendelkezése hiányában – közvetlenül ne legyenek összekapcsolhatóak.

Az informatikai adatbiztonsági előírások részletes meghatározását külön szabályzat tartalmazza.

2.11. Az érintett jogai és az érintett jogainak érvényesítésével összefüggő feladatok

1. Az érintettnek joga van írásban tájékoztatást kérni a Társaság által kezelt személyes adatai vonatkozásában
a) a személyes adatok köréről,
b) az adatkezelés jogalapjáról,
c) az adatkezelés céljáról,
d) a címzettek vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják,
e) az adattárolás időtartamáról,
f) az adatok forrására vonatkozó minden elérhető információról, ha az adat nem az érintettől származik.

2. Az érintett írásban kérheti, hogy a Társaság
a) módosítsa valamely kezelt személyes adatát,
b) törölje személyes adatait,
c) a rá vonatkozó, általa az adatkezelő szerv rendelkezésére bocsátott, bármilyen formában rögzített személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja.

3. A Társaság – az adatvédelmi felelős útján – a kérelemnek, ha jogszabály ellentétesen nem rendelkezik, legfeljebb 30 napon belül eleget tesz. A kérelem teljesítéséről vagy annak elutasításáról 30 napon belül köteles tájékoztatni az érintetett.

4. Az érintettet megillető jogok gyakorlására az érintettek adatainak védelmét szolgáló adatbiztonsági követelményeket szem előtt tartva csak a kérelmező megfelelő azonosítása, illetve kérelme tartalmának hitelesítése esetén van lehetőség. Nem biztosítható ezen jogok gyakorlása különösen az elektronikus aláírással nem hitelesített, vagy a kérelmező személyének azonosítását nem biztosító elektronikus levél, valamint telefax útján érkezett kérelmek esetén.

5. A Társaság az érintett részére nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti. A Társaság az információt írásban, elektronikus úton, illetve az érintett kérelmére szóban is megadhatja, amennyiben az érintett személyazonossága igazolt.

6. Az érintett hozzáférési jogának gyakorlása során a tájékoztatást és az adatról kért első másolatot díjmentesen kell biztosítani, kivéve, ha az érintett kérelme – annak ismétlődő jellege vagy jogszabályban, illetve a Hatóság joggyakorlata értelmében – túlzó. Ez esetben – eltérő jogszabályi rendelkezés hiányában – az adatkezelő szerv jogosult észszerű költségtérítést megállapítani a vonatkozó jogszabályok előírásai alapján.

a) Az Érintettet megillető jogok

Az Érintettet az alábbi jogosultságok illetik meg az Adatkezelő adatkezelése esetén:

1. Az Érintett bármikor jogosult tájékoztatást kérni az Adatkezelő által kezelt, rá vonatkozó személyes adatokról. A tájékoztatás az adott adatkezelésről készült tájékoztatóban megjelölt elektronikus e-mail címen, postai levélben, telefonon is kérhető, de utóbbit papír alapon vissza kell igazolni.
2. A tájékoztatás keretében az Adatkezelő köteles az általa kezelt érintetti adatokról tájékoztatást adni – a vonatkozó tájékoztatást elsősorban az Adatkezelőnél az adatkezelésért felelős személy adja.
3. A tájékoztatást az Adatkezelő az Érintett által kért formában adja meg, erre irányuló kifejezett kérés hiányában elsősorban email-en keresztül, másodsorban postai küldeményként, amennyiben az Adatkezelő számára rendelkezésre áll a kommunikációs forma használatához szükséges adat és amennyiben az Érintett személyazonossága kétséget kizáróan megállapítható.
4. Ha az Adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az Érintettet, erről lehetőség szerint őt megfelelő módon tájékoztatja. Ilyen esetekben az Érintett hozzáférési jogát, a helyesbítés és törlés kérésének jogát, az adatkezelés korlátozásához való jogát, az ezekhez kapcsolódó értesítési jogot, valamint adathordozhatósághoz való jogot az Adatkezelő nem biztosítja, kivéve, ha az Érintett abból a célból, hogy az említettek szerinti jogát gyakorolja, az azonosítását lehetővé tevő kiegészítő információkat nyújt.
5. A panaszok kezelésével kapcsolatban az adatvédelemért felelős személy számára tájékoztatást kötelesek adni a személyes adatok kezelésében részt vevő munkavállalók, egyéb személyek.

b) Törlési kérelem kezelése

Az Érintett kérheti az Adatkezelőtől, hogy indokolatlan késedelem nélkül törölje az Adatkezelő által rá vonatkozóan kezelt személyes adatokat, az Adatkezelő pedig köteles ilyen esetben azokat törölni bármely alábbi eset fennállása esetén:

a) a személyes adatokra már **nincs szükség** arra a célra, ami miatt azok gyűjtésre ill. kezelésre kerültek;

b) az Érintett **visszavonja** az adatkezelés jogalapjául szolgáló **hozzájárulását**, és az adatkezelésnek más jogalapja nincs;
c) az Érintett a közérdekű, valamint az Adatkezelő vagy harmadik fél **jogos érdekeinek érvényesítéséhez** szükséges adatkezelés ellen tiltakozik, és nincs más elsőbbséget élvező jogszerű ok az adatkezelésre;
d) a személyes adatokat **jogellenesen** kezelte az Adatkezelő;
e) a személyes adatokat az Adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt **jogi kötelezettség** miatt törölni kell.

Amennyiben az Adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő Adatkezelőket, hogy az Érintett kérelmezte tőlük a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.
A törést nem kell teljesíteni, amennyiben az adatkezelés

a) véleménynyilvánítás szabadságához, vagy a tájékoztatáshoz való jog gyakorlása céljából szükséges,
b) a személyes adatok kezelését előíró, az Adatkezelőre alkalmazandó európai uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;
c) a népegészségügy területét érintő közérdek alapján;
d) jogi igények előterjesztéséhez, érvényesítéséhez és védelméhez szükséges,
e) jogi kötelezettség teljesítése miatt szükséges,
f) közérdekű archiválás, tudományos, vagy történelmi kutatás, statisztikai célból szükséges és az adattörlés lehetetlenné tenné, vagy komolyan veszélyeztetné az adatkezelés céljának teljesítését.
g) az informatikai rendszerek konzisztens, jogszerű működésének fenntartása érdekében szükséges.

Adatkezelő törli vagy anonimizálja az Érintettre vonatkozó, az informatikai rendszereiben, valamint papír alapú dokumentációiban szereplő személyes adatokat, ha jogszabály máshogy nem rendelkezik és a személyes adat kezeléséhez fűződő cél megszűnt. Amennyiben a személyes adat törlése nem valósítható meg az azt tartalmazó irat sérelme nélkül:

a) amennyiben az irat megőrzéséhez az Adatkezelő, vagy harmadik személy jogos érdeke fűződik, az iratot az Adatkezelő az iratkezelési szabályok szerinti időtartamig megőrzi, törlési kérelem esetén az iratot zártan kezeli és erről az Érintettet értesíti, és az iratot a személyes adattal együtt az iratkezelési szabályban meghatározott időtartam lejártát követően megsemmisíti,
b) amennyiben az irat megőrzéséhez az Adatkezelőnek és harmadik személynek sem fűződik jogos érdeke, az iratot a személyes adattal együtt megsemmisíti.
c) Az adatok törlése iránt minden esetben az adatvédelemért felelős személy a személyes adat kezelésével kapcsolatban Érintett szervezeti egységgel, informatikai rendszer rendszergazdájával együttműködésben intézkedik.

Az Adatkezelő informatikai rendszereiből a személyes adatot – az adott informatikai rendszer adottságai szerint - az élő rendszerből visszaállíthatatlanul törli, vagy anonimizálja, továbbá az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket, és gondoskodik arról, hogy az informatikai rendszer archivált változatában is – a technológiai, technikai lehetőségek függvényében – átvezetésre kerüljön a személyes adat törlése. A törlésért az informatikai rendszerért felelős személy felel.

Amennyiben a helyreállíthatatlan törlés informatikai rendszer sajátosságából következő okból nem kivitelezhető, Adatkezelő az adat logikai törlését hajtja végre.

Az anonimizálás keretében a személyes adatot olyan azonosítóra kell lecserélni, amely megakadályozza, hogy a személyes adathoz tartozó további adatok a későbbiekben kapcsolatba hozhatók legyenek az Érintettel.

A papír alapú dokumentációk esetében, azok jegyzőkönyvvel rögzített megsemmisítéséről kell gondoskodni. A jegyzőkönyvben rögzíteni kell: a megsemmisített iratok típusát, a megsemmisített iratok beazonosíthatóságához szükséges információkat, a megsemmisítés időpontját és a megsemmisítést végző személy nevét, beosztását, külső partner esetén a külső partner nevét.

Amennyiben az adatok törlése jogszabályi előírás miatt szükséges, de az az Érintett jogos érdeke miatt nem lehetséges, a személyes adatot, illetve a személyes adatot tartalmazó elektronikus, vagy papír alapú dokumentációt zárolni kell. Ebben az esetben az informatikai rendszerben tárolt adathoz, illetve dokumentumhoz csak az informatikai rendszer rendszergazdája vagy az adatvédelemért felelős személy rendelkezhet hozzáféréssel. Papír alapú dokumentumok esetén a dokumentum őrzését zárható szekrényében kell megvalósítani.

A papír alapú dokumentációk belső rendszerbe feltöltött elektronikus példányához az Adatkezelő a felhasználók hozzáférését megszünteti.

c) Az adatkezelés elleni tiltakozás kezelése
Az Érintett az Adatkezelőhöz intézett írásbeli nyilatkozatával tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja

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

Tiltakozási jog gyakorlása esetén Adatkezelő nem kezelheti tovább a személyes adatokat, 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. Annak megállapítása kapcsán, hogy az adatkezelést kényszerítő erejű jogos okok indokolják, Adatkezelő dönt. Az ezzel kapcsolatos álláspontjáról véleményben kötelező tájékoztatnia az Érintettet.

Az Adatkezelő csak abban az esetben teljesíti az adatkezelés elleni tiltakozás miatti kérelmet, ha a kérelem írásban került benyújtásra.

Az adatvédelemért felelős személy a legrövidebb időn belül köteles beazonosítani az Érintettet, és köteles a tiltakozást a kérelem benyújtásától számított legrövidebb időn belül megvizsgálni, annak megalapozottsága kérdésében az Adatkezelővel együtt döntést hozni, és döntéséről a kérelmezőt tájékoztatni.

d) Helyesbítési kérelem kezelése
Az Érintett bármikor jogosult a helytelenül rögzített adatainak helyesbítését kérni.

Amennyiben az Érintett jelzi, hogy az Adatkezelő által kezelt bármely adata nem felel meg a valóságnak, az adatvédelemért felelős személy azonosítja az Érintettet, valamint az általa helyesbítésre kért adat nyilvántartás helyét, és gondoskodik az adat helyesbítéséről, ezen eljárása keretében az adat helyesbítésére vonatkozó igényt az Adatkezelő

Érintett informatikai rendszerének rendszergazdája felé jelzi, a szükséges azonosító adatok, a hibás és a helyes adat megadásával. Amennyiben a helyes adat nem áll rendelkezésre, az Adatkezelő az Érintettől kér felvilágosítást a helyes adatról. Ha a helyes adat nem állapítható meg, az adatvédelemért felelős személy gondoskodik a helytelen adat zárolásáról. A zárolás az adat passzív állapotba helyezését jelenti, valamint értesíti az érintetett, hogy az adat helyesbítésére a helyes adat hiányában nincs mód, de az adat zárolásra került. Adatkezelő minden olyan címzettet tájékoztat a helyesbítésről, kiegészítésről, akivel a személyes adatot közölte, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintettet e címzettek adatairól tájékoztatja, ha ezt írásban kérelmezi.

e) Személyes adat korlátozása iránti kérelem kezelése

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

- az Érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az Adatkezelő ellenőrizze a személyes adatok pontosságát;
- az adatkezelés jogellenes, és az Adatkezelő ellenzi az adatok törlését, és e helyett kéri azok felhasználásának korlátozását;
- Adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az Érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy
- az Érintett tiltakozott az adatkezelés ellen, de az Adatkezelő jogos érdeke is megalapozhatja az adatkezelést, ez esetben amíg megállapításra nem kerül, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az Érintett jogos indokaival szemben, az adatkezelést korlátozni kell.

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

Adatkezelő az Érintettet, akinek a kérésére az adatkezelést korlátozta, az adatkezelés korlátozásának feloldásáról előzetesen tájékoztatja.

f) Adathordozhatósághoz való hozzájárulás iránti kérelem kezelése

Ha az adatkezelés szerződés teljesítéséhez szükséges, vagy az adatkezelés az Érintett önkéntes hozzájárulásán alapul, akkor az Érintett kérheti az Adatkezelőtől, hogy a neki megadott adatait gépileg értelmezhető formában részére átadja. Ha az technikailag megvalósítható, akkor azt is kérheti az Adatkezelőtől, hogy az az adatokat más adatkezelő számára továbbítsa.

Ez az érintetti jog kizárólag az Érintett által átadott adatokra korlátozódik, egyéb adatok hordozhatóságára nem vonatkozik (pl. statisztika stb.)

Az Érintettnek joga van arra, hogy a rá vonatkozó, Adatkezelő rendszerében megtalálható személyes adatokat:

- tagolt, széles körben használt, géppel olvasható formátumban megkapja,
- jogosult más adatkezelőhöz továbbítani,
- kérheti az adatok közvetlen továbbítását a másik adatkezelőhöz – ha ez technikailag megvalósítható Adatkezelő rendszerében.

Az Adatkezelő csak abban az esetben teljesíti az adathordozhatóságra vonatkozó kérelmet, ha a kérelem írásban vagy e-mail útján került benyújtásra. A kérelem teljesítéséhez szükséges, hogy Adatkezelő meggyőződjön arról, hogy valóban az arra jogosult Érintett kíván élni e jogával. Az Érintett e jog keretében azon adatok hordozhatóságát igényelheti,

melyet saját maga adott meg Adatkezelő részére. A jog gyakorlása nem jár automatikusan az adatnak Adatkezelő rendszereiből való törlésével, ezért az Érintett e jogának gyakorlását követően is Adatkezelő rendszereiben nyilvántartásra kerül, kivéve, ha kéri adatainak törlését is.

g) Az elhunyt Érintettet megillető jogok más által történő érvényesítése

Az Érintett halálát követő öt éven belül az elhunytat életében megillető jogokat – mint a hozzáféréshez, helyesbítéshez, törléshez, az adatkezelés korlátozásához, adathordozhatósághoz és tiltakozáshoz való jogot – az elhunyt által arra ügyintézési rendelkezéssel, közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az Adatkezelőnél tett nyilatkozattal meghatalmazott személy jogosult érvényesíteni. Ha az elhunyt az Adatkezelőnél több ilyen nyilatkozatot tett, a későbbi időpontban tett nyilatkozatban megnevezett személy érvényesítheti e jogokat.

Ha az elhunyt nem tett ilyen tartalmú nyilatkozatot, akkor az elhunyt életében megillető és előző bekezdésben meghatározott jogait az Érintett - Polgári Törvénykönyv szerinti - közeli hozzátartozója érvényesítheti az Érintett halálát követő öt éven belül (több közeli hozzátartozó esetén az a közeli hozzátartozó, aki ezen jogosultságát elsőként gyakorolja). Közeli hozzátartozónak a Ptk. 8:1. § (1) 1. pontja szerint a házastárs, az egyenesági rokon, az örökbefogadott, a mostoha- és a nevelt gyermek, az örökbefogadó-, a mostoha- és a nevelőszülő és a testvér minősül. Az elhunyt közeli hozzátartozója az alábbi tényeket köteles igazolni:

- az elhunyt Érintett halálának tényét és idejét – halotti anyakönyvi kivonattal vagy bírósági határozattal, valamint
- saját személyazonosságát – valamint amennyiben szükséges közeli hozzátartozói minőségét – közokirattal igazolja.

Az elhunyt jogait érvényesítő személyt e jogok érvényesítése során az elhunytat életében megillető jogok illetik meg és kötelezettségek terhelik.

Adatkezelő írásbeli kérelemre köteles tájékoztatni a közeli hozzátartozót a megtett intézkedésről, kivéve, ha azt az elhunyt nyilatkozatában ezt kifejezetten megtiltotta.

h) Kérelem teljesítésének határideje, módja

Adatkezelő indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az Érintettet az intézkedéseiről. A kérelem összetettségére és a kérelmek számára tekintettel ez a határidő további két hónappal meghosszabbítható, de ebben az esetben az Adatkezelő köteles az Érintettet egy hónapon belül tájékoztatni a határidő-hosszabbításról és annak okairól. Emellett Adatkezelő köteles az Érintettet tájékoztatni arról, hogy panaszt nyújthat be a felügyeleti hatóságnál, és élhet a bírósági jogorvoslati jogával.

Ha az Érintett kérelme egyértelműen megalapozatlan vagy túlzó (különösen, ha az ismétlődő), akkor az Adatkezelő a kérelem teljesítéséért észszerű mértékű díjat számíthat fel vagy megtagadhatja a kérés teljesítését. Ennek bizonyítása Adatkezelőt terheli.

Ha az Érintett elektronikus úton nyújtotta be a kérelmét, akkor az Adatkezelő a tájékoztatását köteles elektronikus úton megadni, kivéve, ha ezt az Érintett kifejezetten más formában kéri.

Az Adatkezelő minden olyan címzettet köteles tájékoztatni az általa elvégzett helyesbítésekről, törlésekről vagy adatkezelés-korlátozásokról, aki számára a helyesbített adatot elérhetővé tett, kivéve, ha ez lehetetlennek bizonyul vagy ez aránytalanul nagy erőfeszítést igényel.

i) Jogorvoslathoz való jog

Az Érintett jogait emailben vagy postai úton küldött írásbeli kérelemben gyakorolhatja.

Az Érintett nem érvényesítheti a jogai, ha Adatkezelő bizonyítja, hogy nincs abban a helyzetben, hogy azonosítsa az Érintettet. Ha az Érintett kérelme egyértelműen megalapozatlan vagy túlzó (különösen az ismétlődő jellegre figyelemmel) Adatkezelő a kérelem teljesítéséért észszerű mértékű díjat számíthat fel vagy megtagadhatja az intézkedést. Ennek bizonyítása az Adatkezelőt terheli. Ha Adatkezelő részéről kétség merül fel a kérelmet benyújtó természetes személy kilétével kapcsolatban, további, a kérelmező személyazonosságának megerősítéséhez szükséges információk nyújtását kérheti.

Az Érintett az Info.tv., a Rendelet, valamint a Polgári Törvénykönyv (2013. évi V. törvény) alapján

a. Nemzeti Adatvédelmi és Információszabadság Hatósághoz (1125 Budapest, Szilágyi Erzsébet fasor 22/c.; www.naih.hu) fordulhat vagy

b. Bíróság előtt érvényesítheti jogait. A per – az Érintett választása szerint – a lakóhelye szerinti törvényszék előtt is megindítható (a törvényszékek felsorolását és elérhetőségét az alábbi linken keresztül tekintheti meg: **http://birosag.hu/torvenyszekek).**

2.12. Adatkezelés során alkalmazandó intézkedések

Az Adatkezelő által működtetett informatikai rendszerek felhasználói, a személyes adatokkal egyéb módon kapcsolatba kerülő személyek a személyes adatok védelme érdekében kötelesek betartani a jelen pontban meghatározásra kerülő előírásokat.

A munkavégzés/feladatellátás során keletkezett személyes adatot is tartalmazó elektronikus dokumentumok csak a munkavégzés céljára szolgáló számítástechnikai eszközökön nyithatók meg.

A munkavégzés/feladatellátás céljára szolgáló eszközök és szoftverek hozzáférési kódjait a munkavállalók bizalmasan kötelesek kezelni.

A munkavégzés/feladatellátás céljára szolgáló mobiltelefonokon a személyes adatot is tartalmazó dokumentumot is tartalmazó leveleket nem szabad megnyitni, a dokumentumot lehetőség szerint csak asztali számítógépen, vagy notebook-on lehet megnyitni. Amennyiben mégis mobiltelefonon keresztüli megnyitás szükséges, akkor a mobiltelefonról a helyi másolatot minden esetben törölni kell.

A munkavégzés/feladatellátásra használt mobiltelefont, amelyen az Adatkezelő által kezelt, vagy feldolgozott személyes adat is megtalálható, minden esetben a mobiltelefonba épített ábrás, vagy kódos védelemmel kell használni.

A munkavállalók kötelesek az Adatkezelő mint munkáltató által biztosított készüléken képernyőzárat – ábrát, vagy kódot - megadni, létrehozni, továbbá a készüléket a munkaviszonyuk fennállása alatt folyamatosan ábrás, vagy kódos védelemmel ellátva használni, melyet kizárólag az adott munkavállaló ismerhet. A munkavállalók kötelesek a kódot a mobiltelefon visszaadásának napján az Adatkezelő (munkáltató) számára megadni, vagy a mobiltelefont kóddal nem védett állapotban visszaszolgáltatni.

A munkavégzés/feladatellátás céljára átadott notebook-ok és egyéb munkaállomások esetében az eszközöket csak a felhasználók használhatják, hozzátartozóik, vagy más személyek számára nem engedélyezett a használat. A munkavégzés/feladatellátásra használt notebook-ot, amelyen az Adatkezelő által kezelt, vagy feldolgozott személyes

adatok is megtalálhatók, minden esetben jelszavas védelemmel kell használni. A munkavállalók kötelesek az Adatkezelő (munkáltató) által biztosított készüléken jelszót létrehozni, továbbá a készüléket a munkaviszonyuk fennállása alatt folyamatosan jelszavas védelemmel ellátva használni, melyet kizárólag az adott munkavállaló ismerhet. A munkavégzéshez biztosított fizikai eszközök és szoftveres megoldások visszaadásának napján a munkavállalók kötelesek a jelszót az Adatkezelő (munkáltató) számára megadni, vagy az eszközt jelszóval nem védett állapotban visszaszolgáltatni.
A papír alapú személyes adatokat tartalmazó munkadokumentumokat olyan módon kell kezelni, tárolni, hogy azokhoz csak az a munkavállaló rendelkezhessen hozzáféréssel, akinek a feladatkörébe tartozik a vonatkozó adatok kezelése. Ez a munkavállaló köteles a vonatkozó dokumentumokat mások által elhatárolt, zárt helyen tartani, és ha azok használatára már nincs szükség, akkor olyan módon kell megsemmisíteni (pl: irat ledarálásával), hogy a megsemmisítést követően ne lehessen azok tartalmát megállapítani.

A munkavállaló munkaviszonya, megbízása, egyéb feladatellátásra szolgáló jogviszonya megszűnése esetén minden személyes adatot is tartalmazó papír alapú és elektronikus iratot, adatot köteles a foglalkoztatásának utolsó napját megelőzően az Adatkezelő részére visszaszolgáltatni, azokról másolatot nem tarthat magánál, amiről átadás-átvételi jegyzőkönyvet kell készíteni.

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

Minden munkavállaló köteles az általa használt munkaterületet olyan módon használni, hogy azon az Adatkezelő kezelésében vagy feldolgozásában lévő, személyes adatot is tartalmazó dokumentumok lehetőség szerint szabadon ne legyenek hozzáférhetők. Ilyen intézkedésnek minősül különösen: számítástechnikai eszközök jelszavas védelme, az irodahelyiség zárása, az iratok elhelyezése védett helyre. Minden munkavállaló köteles biztosítani azt, és a megfelelő intézkedéseket megtenni annak érdekében, hogy az Adatkezelő valamennyi irodai területére a nem az Adatkezelővel munkaviszonyban, vagy egyéb munkavégzésre irányuló egyéb jogviszonyban álló személy csak az Adatkezelő munkavállalójának, vagy megbízottjának kíséretében léphessen be. Az Adatkezelő területére belépni jogosult személyek az Adatkezelő által kezelt személyes adatok megismerésére nem jogosultak, és az Adatkezelő kezelésében álló személyes adatok biztonságának megsértésével az Adatkezelőt ért kárért az adatvédelmi incidenst előidéző személy teljes felelősséggel tartozik.

Személyes adatok csak biztonságos kommunikációs csatorna alkalmazásával, vagy megfelelő titkosítási megoldással adhatók át más személynek. Ellenkező jelzésig az Adatkezelő belső levelezési rendszerén belüli adatáramlás biztonságos kézbesítési csatornának tekintendő. Külső adatátadás során gondoskodni kell a személyes adatok titkosításáról SSL kapcsolat, vagy egyedi titkosítás használatával, a jelszó elkülönített csatornán (pl.: SMS) keresztüli küldésével, papír alapon pedig zárt borítékon keresztüli átadással.

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

Titoktartási nyilatkozat hiányában nem adható át külső személynek személyes adat!

2.13. Adatkezelés tervezésével, informatikai rendszer fejlesztésével kapcsolatos rendelkezések

1. Adatkezelés tervezése

Személyes adatok kezelésével járó új tevékenységek bevezetésekor az alábbi feladatokat kell elvégeznie az adatvédelemért felelős személynek:

a) meg kell határoznia
   1. a kezelendő személyes adatok körét,
   2. az adatok kezelésének célját,
   3. az adatkezelés jogalapját,
   4. az adatkezelés időtartamát,

b) fel kell mérnie, hogy az adatok milyen informatikai rendszerben lesznek kezelve, az adatok milyen informatikai rendszerben jelennek meg,

c) meg kell határoznia, hogy előreláthatóan az adatokhoz kinek szükséges hozzáférnie az Adatkezelő-en belül, illetve kívül,

d) be kell mutatni, hogy az adatokat szükséges-e továbbítani más személy számára,

e) be kell mutatni, hogy az adatkezeléshez igénybe kell-e venni Adatfeldolgozót, amennyiben igen, az Adatfeldolgozó feladata mi lesz, várhatóan ki lesz az Adatfeldolgozó,

f) meg kell határozni az adatkezelés megkezdésének tervezett időpontját, az adatok felvételének módját és pontos helyét (pl.: erre szolgáló internetes felület vagy papír alapú adatfelvétel).

g) A kialakított adatkezelési terv alapján az adatkezelésről szóló tájékoztatót és a végleges adatfeldolgozási szerződést az adatvédelemért felelős személy készíti el.

2. Az adatvédelmi szervezet

a) Az ügyvezető igazgató

- gondoskodik az adatkezelés személyi és tárgyi feltételeinek biztosításáról,
- jogosult az Adatkezelő adatkezeléseire vonatkozó döntések meghozatalára;
- kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről;
- szükség esetén részt vesz az Adatkezelő adatvédelmi incidenseket kivizsgáló munkacsoport munkájában.

b) Az Informatikai Biztonsági Felelős (IBF)

Az Informatikai Biztonsági Szabályzatban meghatározott feladatai teljesítése során kiemelt figyelmet szentel a személyes adatokat érintő biztonsági intézkedések megvalósításának.
Az adatvédelmi felelős bevonásával gondoskodik az informatikai megoldások kialakítása során az adatvédelem és adatbiztonság szempontjainak érvényesüléséről. Adatvédelmi incidens esetén jelen szabályzatban meghatározottak szerint részt vesz az adatvédelmi felelős által létrehozott adatvédelmi munkacsoport munkájában, az incidens megoldásában.

Az ACE Kft ügyvezető igazgatója által kijelölt Informatikai Biztonsági Felelős (IBF) az IT vezető.
Nyilvános e-mail elérhetősége: GDPR@aeroplex.com

c) **Az adatgazdák**

- a szervezeti egységek vezetői, akik felelősek az irányításuk alá tartozó szervezeti egységek adatkezelésének jogszerűségéért, jelen utasításban foglaltak végrehajtásáért és betartásáért.
- jogosulatlan hozzáférés vagy az adatvédelmi előírások egyéb megsértésének észlelése esetén az adatvédelemért felelős munkavállaló egyidejű tájékoztatása mellett intézkedést tesznek annak megszüntetésére, indokolt esetben kezdeményezik a felelősségre vonási eljárás lefolytatását.
- adatvédelmi incidens bekövetkezése esetén részt vesznek az adatvédelmi felelős által összehívott munkacsoport munkájában.

AEROPLEX Közép-Európai Légijármű Műszaki Központ Kft. elsődleges adatgazdái (Adatkezelő szervezeti egységei) és azok elérhetősége:

1. Munkavállalók személyes adatainak nyilvántartása
Név: Ügyvezető igazgatói Titkárság
Email: [AceItitkarsag@aeroplex.com]

2. Humán adatok nyilvántartása
Név: Humán Erőforrás szervezet
Email: [AceHuman@aeroplex.com]

3. Társadalombiztosítási adatok nyilvántartása
Név: Pénzügyi igazgató
Email: [ACEPenzugy@aeroplex.com]

d) **Az adatkezelést végző munkatárs**

Köteles

- az általa kezelt, feldolgozott adatokat az IBSZ-ben meghatározottak szerinti biztonsági osztályba sorolásuk kategóriája szerint kezelni;
- az általa végzett adatfeldolgozást jogszerűen végezni;
- a tudomására jutott személyes adatokat kizárólag az Adatkezelő rendelkezései szerint feldolgozni, továbbá a személyes és egyéb bizalmas adatokat az Adatkezelő rendelkezései szerint tárolni és megőrizni;
- adatvédelmi incidens gyanúja esetén köteles az adatvédelmi felelős rendelkezései szerint eljárni.

Az adatkezelést végző munkatárs az adatkezelést érintő érdemi döntést nem hozhat, saját célra adatfeldolgozást nem végezhet.

2.14. Adatbiztonság

1. Adatbiztonság elve

Adatkezelő az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok észszerűen elvárható legmagasabb szintű biztonságáról (adatbiztonság elve).

Az informatikai rendszerekben megvalósuló adatkezelések során felmerülő adatbiztonsági kérdésben az adatgazdák vagyis az adott szervezeti egység által kezelt személyes adatok tekintetében kötelesek:

- az adatkezelés időtartama alatt az adatok biztonságos tárolása, az időtartam lejártával az adatállomány törlése, fizikai megsemmisítése érdekében a szükséges intézkedéseket megtenni;
- az adatokat megfelelő intézkedésekkel védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés a véletlen megsemmisítés és sérülés, Adatkezelő által alkalmazott technika megváltoztatásából fakadó hozzáférhetetlenné válás ellen.
- gondoskodni arról, hogy a jelen Szabályzatot, valamint a feladatkörükben kiadott külön, a személyes adatok kezeléséről szóló rendelkezéseket az irányításuk alatt dolgozók megismerjék és betartsák, illetve azt folyamatosan ellenőrizni;
- ellenőrizni, hogy a szervezeti egységében kezelt adatok továbbításukat követően is olyan adatkezelőhöz, adatfeldolgozóhoz kerülnek, aki vagy amely az adatok biztonságos kezeléséről megfelelően gondoskodni tud, ezzel összefüggő kérdésekben jogosult kérni az adatvédelmi felelős. állásfoglalását;
- Adatkezelő valamennyi munkavállalója köteles a személyes adatokat tartalmazó iratokat és a munkavégzéshez szükséges segédleteket a munkavégzés befejezését követően – ahol biztosított – zárható lemez- vagy páncélszekrényben, biztonsági zárral ellátott fiókban, szekrényben tárolni. Ahol ezek a feltételek nem biztosítottak ott is törekedni kell az adatok legalább zárral ellátott fiókban, szekrényben történő biztonságos tárolására. Az íróasztalokon a munkavégzés befejezését követően személyes adatokat tartalmazó iratok tárolása tilos.
- a munkatársak irodai helyiségüket és az irat és adattárolásra használt berendezéseket munkaidőben fokozott gondossággal kötelesek őrizni. A munkatárs köteles a számítógépét és az ahhoz alkalmazott adathordozókat úgy kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. Köteles továbbá a munkaidő végeztével a számítógépet kikapcsolni, az irodahelység ajtaját – közös iroda esetén az utolsóként távozó munkatársa – bezárni.

További adatbiztonsági előírások:

- A személyes adatokat tartalmazó iratot vagy adathordozót az Adatkezelő területéről kivinni csak különösen indokolt esetben az adott szervezeti egység vezetőjének kifejezett engedélyével szabad. Ebben az esetben az iratot vagy adathordozót magánál tartó munkavállaló felel annak megőrzéséért, sértetlenségéért, illetve, hogy annak tartalmáról illetéktelen személy ne szerezhessen tudomást.
- Adatkezelési tevékenységet az egyes munkatársak csak feladatkörük ellátásához szükséges mértékben folytathatnak. Az adatkezelési tevékenységet ellátó munkatárs köteles gondoskodni az általa kezelt adatok és iratok megőrzéséről.

Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban leírtak követendők!

2. Informatikai nyilvántartások védelme

Adatkezelő az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

- a jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver és hardver eszközök védelméről, illetve a fizikai védelemről;
- az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről;

- az adatállományok vírusok elleni védelméről;
- az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról.

Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban leírtak az irányadóak követendők!

3. Papíralapú nyilvántartások védelme

Adatkezelő a papíralapú nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság, illetve tűzvédelem tekintetében.

A munkavállalók, és egyéb, az Adatkezelő érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

4. Számítógépes infrastruktúra használatának szabályai

A munkatársak Adatkezelő számítógépes infrastruktúráját csak rendeltetésszerűen használhatják. Az eszközöket csak a munkaköri leírásban részletezett tevékenységekre használhatják.

A munkatársak fokozottan kötelesek ügyelni arra, hogy az Adatkezelő által biztosított rendszerekbe belépést biztosító jelszavukat illetéktelen személy ne ismerje meg. Ennek keretében

- a jelszavakat úgy kell megválasztani, hogy azokat ne lehessen kitalálni;
- a jelszavakat tilos mások tudomására hozni;
- a jelszavakat ajánlott legalább háromhavonta cserélni, kivéve a számítógépes bejelentkezéshez és webes levelezéshez használt jelszót, melyet 45 naponta kell megváltoztatni;
- bármely rendszer, amely jelszóval védett belépést igényel tilos kilépés nélkül elhagyni, nem elegendő pl. egy böngésző bezárása;
- a munkatársaknak tilos más munkatársak informatikai eszközét illetéktelenül használni,
- tilos a hálózati erőforrásokat védő technikai korlátozások feltörése, más felhasználók jelszavainak megszerzése, illetve
- tilos a munkatárs rendes munkavégzésén kívül a rendszer, és más felhasználók adatait, fájljait – engedély nélkül – másolni, törölni vagy módosítani.

Az informatikai rendszert tűzfal, és rendszeresen frissülő vírusellenőrző szoftver védi, amelyek működtetéséről, frissítéséről az IT vezető gondoskodik és/vagy az informatikai szabályzat szabályozza.

Az elektronikus adattároló berendezések fizikai védelméről megfelelően gondoskodni kell, így

- azokat zárt védett helyen kell tartani,
- a számítástechnikai eszközök közelében enni vagy inni tilos,
- Adatkezelő területéről csak jelszóval védett számítógép vihető ki, Adatkezelő előzetes engedélyével.

Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban (IBSZ) leírtak a követendők!

5. Személyes adatok automatizált feldolgozása

A személyes adatok automatizált feldolgozása során biztosítani kell

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

Az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amelyik a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban (IBSZ) leírtak a követendők!

2.15. Az Adatfeldolgozók

Adatkezelő fenntartja magának a jogot, hogy tevékenysége során Adatfeldolgozót vegyen igénybe, állandó vagy eseti megbízás alapján. Állandó jellegű adatfeldolgozásra elsősorban az ügyfélkapcsolattal, a szolgáltatások nyújtásával összefüggő adminisztráció ellátása, valamint az informatikai rendszer fenntartása érdekében kerülhet sor. Az Adatfeldolgozó igénybevétele során a vonatkozó jogszabályok, elsősorban a rendelet rendelkezései az irányadók.

Adatfeldolgozó igénybevételére kizárólag írásbeli szerződés alapján kerülhet sor. Az Adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit a vonatkozó jogszabályok keretei között az Adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az Adatkezelő felel. Az Adatkezelő garanciákat nyújtó szerződési feltételek kialakításával és megfelelő szervezeti, technikai intézkedésekkel biztosítja, hogy az Adatfeldolgozó tevékenysége során az érintettek jogai ne sérülhessenek, és az Adatfeldolgozó személyes adatokat csak akkor ismerhessen meg, ha a feladata ellátásához elengedhetetlenül szükséges.

Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban (IBSZ) leírtak követendők!

Adatfeldolgozói szerződések kötelező tartalmi elemei

A szabályzat hatálybalépését követően kötött adatfeldolgozói szerződésekben legalább az alábbiakról rendelkezni kell:

- szerződés tárgya,
- az Adatkezelő és az Adatfeldolgozó adatai
- a feldolgozott adatok körének megjelölése,
- az adatfeldolgozás céljai,
- az adatfeldolgozás időtartama,
- a feldolgozandó személyes adatok becsült mennyisége,
- az Adatfeldolgozó által elvégzett technikai műveletek megnevezése és alapvető elemei;
- az érintettek köre,

- Adatfeldolgozó által ellátandó feladatok pontos leírása,
- az utasításhoz kötöttség ténye,
- a tájékoztatási kötelezettséget,
- azt, hogy az Adatfeldolgozó a Rendeletben alkalmazott biztonsági eljárásokra (álnevesítés, titkosítás) felkészül, azokat legkésőbb a Rendelet alkalmazásának megkezdésétől bevezeti;
- Adatkezelő rendszergazdájának, információbiztonsági felelősének és adatvédelemért felelős személyének elérhetősége,
- Adatfeldolgozó titoktartási kötelezettsége,
- az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedések meghatározása, az adatbiztonsági előírások meghatározása;
- annak meghatározása, hogy az Adatfeldolgozónak az Adatkezelő mely szabályzatainak kell megfelelnie,
- további Adatfeldolgozó igénybevételének lehetőségét, amennyiben ez ismert, a további Adatfeldolgozó személyének megjelölésével, amennyiben nem ismert a bevonás menetére vonatkozó rendelkezéseket és az Adatkezelő ellenvetési jogát,
- a további Adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen a Rendelet követelményeinek,
- az adatfeldolgozás befejezését követően eljárásokat (minden személyes adatot törölni kell vagy vissza kell juttatni az Adatkezelő számára és törölni kell a meglévő másolatokat, kivéve, ha az európai uniós vagy a tagállami jog az személyes adatok tárolását írja elő,
- a további Adatfeldolgozóval az Adatfeldolgozónak az eredeti szerződésének megfelelő tartalmú szerződést kell kötnie,
- az együttműködés elvét azaz, hogy az Adatfeldolgozónak kötelessége az Adatkezelővel együttműködni az alanyi jogok teljesítési során,
- az Adatkezelő és az Adatfeldolgozó közötti utasításadás, illetve kapcsolattartás módja,
- a felelősség elvét, azaz annak tényét, hogy az Adatkezelő az Adatfeldolgozó rendelkezésére bocsát minden olyan információt, amely az Adatkezelő Rendeletben megfogalmazott kötelezettségeinek teljesítéséhez szükséges,
- az audit jog kikötését, azaz, hogy az Adatfeldolgozó köteles elősegíteni az Adatkezelő által vagy az általa megbízott más természetes vagy jogi személy által végzett auditokat, beleértve a helyszíni ellenőrzéseket,
- a felelősség egyes kérdései a felek között,
- jogérvényesítési lehetőségek a felek között.

Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban (IBSZ) leírtak az irányadó követendők!

2.16. Adatvédelmi incidensekkel kapcsolatos kötelezettségek

1. Az adatvédelmi incidens

Az adatvédelmi incidens alatt a Rendelet értelmében a biztonság olyan sérülését értjük, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

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.

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

A bejelentést elsősorban munkaidőben, telefonon keresztül kell megtenni, és azt követően az adatvédelemért felelős személy számára küldött elektronikus levél formájában is meg kell erősíteni.

Kérdéses esetben a mindenkori nformatikai Biztonsági Szabályzatban (IBSZ) leírtak az irányadókövetendők!

2. Adatvédelmi incidens során alkalmazandó eljárásrend

Az adatvédelemért felelős személy és az egyéb érintett személyek a számukra jelzett, vagy saját hatáskörükben megállapított adatvédelmi incidens felderítése és súlyosságának megállapítása érdekében a jelen fejezetben foglaltak szerint kötelesek eljárni.

Az Adatkezelő minden szükséges intézkedést megtesz az adatvédelmi incidensek elkerülése érdekében. Amennyiben mégis adatvédelmi incidens következik be:

1. Az adatvédelemi felelős felveszi a kapcsolatot az adatvédelmi incidenssel érintett informatikai rendszer rendszergazdájával, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával, és ha azonosítható ilyen, az incidenst előidéző személlyel.

2. Az adatvédelemért felelős személynek a felderítés során az alábbi kategóriák valamelyikébe kell az adatvédelmi incidenst sorolni:

   A. Alacsony szintű adatvédelmi incidens: a személyes adatok elhanyagolható körének jogosulatlan továbbítása, megváltoztatása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset.

   B. Közepes szintű adatvédelmi incidens: a személyes adatok csekély körének megváltoztatása, jogosulatlan továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset.

   C. Magas szintű adatvédelmi incidens:

      - a személyes adatok széles körének jogosulatlan megváltoztatása, továbbítása, nyilvánosságra hozatala, szándékolt, vagy véletlen törlése vagy megsemmisítése, vagy más jogellenes adatkezelési eset, illetve
      - az adatok körétől függetlenül minden olyan eset, amikor valószínűsíthető, hogy az incidensnek az érintettre hátrányos hatása van, vagy biztosra vehető, hogy az incidensnek az érintettre hátrányos hatása van.

3. Alacsony szintű adatvédelmi incidens esetén az adatvédelemi felelős :

   - legkésőbb a tudomásszerzéstől számított 1 napon belül az érintett rendszer rendszergazdájával és az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdájával meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
   - rögzíti az adatvédelmi incidenst az incidensek nyilvántartásába.

4. Közepes szintű adatvédelmi incidens esetén:

   - az adatvédeleméi felelős haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személyen kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és Adatkezelő vezetője,
   - a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére,
   - az adatvédelemi felelős rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,
   - az adatvédeleméi felelős értesíti a felügyeleti hatóságot 72 órán belül az adatvédelmi incidensről, ha az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintett vagy más érintettek jogaira és szabadságaira nézve.

5. Magas szintű adatvédelmi incidens esetén:

   - az adatvédelemért felelős személy haladéktalanul, de legkésőbb a tudomásszerzéstől számított 24 órán belül munkacsoportot hív össze, amelyben részt vesz az adatvédelemért felelős személyen kívül a rendszergazda, az adatvédelmi incidenssel érintett adatkezelési folyamat adatgazdája és Adatkezelő vezetője,
   - a munkacsoport meghatározza az adatvédelmi incidens kezelésének módját és felhívja az intézkedésre jogosult személyt az incidens kezelésére, továbbá meghatározza az érintettek értesítésének módját, az értesítés tartalmát, és gondoskodik az érintettek haladéktalan értesítéséről.
   - az adatvédelemért felelős személy rögzíti az adatvédelmi incidenst az incidensek nyilvántartásában,
   - az adatvédelemért felelős személy értesíti a felügyeleti hatóságot a tudomásszerzéstől számított 72 órán belül az adatvédelmi incidensről.

Az Adatkezelő az adatvédelemért felelős személy útján az adatvédelmi incidenssel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából az adatvédelmi incidensekről nyilvántartást vezet, amely tartalmazza az adatvédelmi incidenssel érintett személyes adatok körét, az adatvédelmi incidenssel érintettek körét és számát, az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket, valamint az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

Amennyiben az érintett ezt kéri, az adatvédelemért felelős személy tájékoztatást ad az érintett személyes adatára is kiterjedő adatvédelmi incidensekkel kapcsolatban.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő indokolatlan késedelem nélkül köteles írásban, vagy ha rendelkezésre áll email cím, akkor emailben tájékoztatni az érintettet az adatvédelmi incidensről.

A tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat:

- adatvédelemért felelős személy vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Adatkezelő nem köteles tájékoztatni az érintettet az adatvédelmi incidensről, ha

- Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazta (különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat).
- Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg.
- A tájékoztatás aránytalan erőfeszítést tenne szükségessé az Adatkezelő részéről. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását. Pl. sajtóközlemény kiadása.

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

Adatvédelmi incidens nem csak Adatkezelőnél merülhet fel, hanem a vele szerződéses kapcsolatban álló Adatfeldolgozónál is. Ha az Adatfeldolgozó rendszerében észlel adatvédelmi incidenst, indokolatlan késedelem nélkül köteles bejelenteni azt Adatkezelőnek, illetve amennyiben nem lehetséges az információkat egyidejűleg közölni, azokat köteles további indokolatlan késedelem nélkül akár részletekben is közölni.

Amennyiben Adatkezelő észlel adatvédelmi incidenst valamely Adatfeldolgozójánál, vagy adatvédelmi incidens gyanúja merül fel, akkor Adatkezelő az Adatfeldolgozó egyidejű értesítésével lefolytatja az adatvédelmi incidens azonosításával és kezelésével kapcsolatos, jelen pont szerinti eljárását.
Kérdéses esetben a mindenkori Informatikai Biztonsági Szabályzatban (IBSZ) leírtak az irányadó követendők!

2.17. Adatvagyon nyilvántartás vezetése

Az adatvédelemi felelős az adatkezelések átláthatóságának biztosítása érdekében nem nyilvános adatvagyon nyilvántartást vezet, amely tartalmazza legalább:

- az adatkezelési eset megnevezését,
- az Adatkezelő kezelésében lévő adatok felsorolását,
- azt, hogy adott adat milyen informatikai rendszerben kerül kezelésre,
- az adatkezelés célját,
- az adatkezelés időtartamát,
- az Adatfeldolgozók személyét
- az adat forrását,
- az adatkezelési folyamat adatgazdája szervezeti egységét, személyét.

2.18. Adatkezelési tájékoztatás

Az újonnan megkezdett adatkezelés esetében amennyiben az Érintettre vonatkozó személyes adatokat az Adatkezelő az Érintettől gyűjti, a személyes adatok megszerzésének időpontjában, amennyiben az Érintett utólag kér tájékoztatást, úgy ezen tájékoztatás megadásakor is az Érintett rendelkezésére kell bocsátani a következő információkat:

a) az Adatkezelő ill. képviselőjének kiléte és elérhetőségei;
b) az adatvédelemi felelős elérhetőségei;
c) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja (ideértve különösen az Adatkezelő és harmadik fél jogos érdekeinek kifejtését is);
d) a személyes adatok címzettjei, amennyiben van ilyen, a címzettek kategóriái;
e) adott esetben annak a ténye, ha az Adatkezelő harmadik országba, vagy nemzetközi szervezet részére kívánja az adatokat továbbítani, a vonatkozó megfelelőségi határozat léte vagy hiánya, vagy ilyen adattovábbítás esetén s megfelelő és alkalmas garanciák megjelölése, valamint azok másolatának megszerzésére szolgáló módokra vagy azok elérhetőségére való hivatkozás;
f) a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
g) az Érintett azon jogáról történő tájékoztatása, hogy kérelmezheti az Adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését, vagy kezelésének korlátozását (zárolás), és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az Érintett adathordozhatósághoz való jogát;
h) amennyiben az adatkezelés az Érintett hozzájárulásán alapul, az arról való tájékoztatást, hogy hozzájárulását bármely időpontban visszavonhatja, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
i) az Érintettnek joga van felügyeleti hatósághoz címzett panasz benyújtására;
j) azt, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint, hogy az Érintett köteles-e a vonatkozó személyes adatokat megadni, továbbá, hogy milyen lehetséges következményekkel jár az adatszolgáltatás elmaradása;
k) az automatizált döntéshozatal ténye – amennyiben az adatkezelés során ez felmerül, beleértve, hogy megjelölendő, hogy az ilyen adatkezelés milyen jelentőséggel és az Érintette nézve milyen várható következményekkel bír.

A társaság által kezelt személyes adatokat feldolgozó rendszereket **a 6.számú melléklet tartalamazza**. (A társaság adatkezelői által használt rendszerek) A kitöltött melléklet adattartalma nem nyilvános, abból információt kapni csak előzetes Ügyvezető Igazgatói és Adatvédelmi Biztosi engedéllyel lehetséges.

Amennyiben az Adatkezelő a személyes adatokat az eredeti adatkezelési céltól eltérő további célra is fel kívánja használni és ezen adatkezelésre jogosult is, úgy az Adatkezelő köteles a GDPR vonatkozó szabályainak megfelelően az Érintettet az eltérő célról és minden, a fenti pontokban megfogalmazott információkról a további adatkezelést megelőzően tájékoztatni.

Az újonnan megkezdett adatkezelés esetében amennyiben erre lehetőség van, továbbá, ha az Érintettre vonatkozó személyes adatokat az Adatkezelő nem az Érintettől gyűjti, a személyes adatok megszerzésének időpontjában, illetőleg a tájékoztató elkészítésekor az Érintett rendelkezésére bocsátja a fenti információkat, valamint a személyes adatok forrását és adott esetben azt, hogy az adatok nyilvánosan hozzáférhető forrásból származnak-e.

3. ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat rendelkezései 2021. január 01-től hatályosak.

4. MELLÉKLETEK

1. *számú melléklet: Adatvédelmi tájékoztató a társaság munkavállalói részére*
2. *számú melléklet: Adatvédelmi nyilvántartás*
3. *számú melléklet: A társaság adatkezelői által nyilvántartott adatok*
4. *számú melléklet: Bejelentő lap az adatkezelő részére adatvédelmi incidens esetén*
5. *számú melléklet: Az érintett tájékoztatása az adatvédelmi incidensről*
6. *számú melléklet: A társaság adatkezelői által használt rendszerek*

1. számú melléklet: Adatvédelmi tájékoztató a társaság munkavállalói részére

ADATVÉDELMI TÁJÉKOZTATÓ AZ AEROPLEX KÖZÉP-EURÓPAI KFT. MUNKAVÁLLALÓI RÉSZÉRE

Az **AEROPLEX Közép-Európai Légijármű Műszaki Központ Korlátolt Felelősségű Társaság** (székhelye: 1185 Budapest, Liszt Ferenc Nemzetközi Repülőtér; cégjegyzékszáma: 01-09-164863; adószáma: 10751116-2-43) mint munkáltató és adatkezelő (a továbbiakban: a „**Munkáltató**") ezúton tájékoztatja munkavállalóit (a továbbiakban: a „**Munkavállaló**" vagy a „**Munkavállalók**") személyes adataik kezeléséről.

1. A személyes adatok kezelésének oka

2016. május 24-én az Európai Unió rendeletet tett közzé a személyes adatok védelme érdekében. A szabályozás közvetlenül érvényes minden olyan szervezetre, amely személyes adatot kezel. (EU 2016/679 rendelete (GDPR)) Magyarországon 2018 május 25-től kötelező a betartása.

2. Az adatkezelés célja

A Munkáltató a Munkavállalók személyes adatait a munkaviszony létesítése, teljesítése, fenntartása és megszüntetése érdekében kezeli.

3. A kezelt adatok köre, az adatkezelés jogalapja

A Munkáltató törvényi felhatalmazás alapján kezeli a Munkavállaló következő személyes adatait: a Munkavállaló neve; születési neve; születési helye; születési ideje; anyja születési neve; lakóhely; tartózkodási hely (amennyiben eltérő a lakóhelytől); adóazonosító jele; társadalombiztosítási azonosító jele (TAJ szám); arra vonatkozó információ, hogy a Munkavállaló pályakezdőnek vagy nyugdíjasnak minősül-e; nyugdíjas törzsszám (nyugdíjas munkavállaló esetén); személyi igazolvány száma; lakcímet igazoló hatósági igazolvány száma; bankszámla száma; életkora; családi állapota; házastársa adószáma és munkahelye; gyermekei száma és születési ideje valamint azok adóazonosító jele és társadalombiztosítási azonosító jele; családi adókedvezményt igénybe vesz-e; van-e másik munkaviszonya (másodállás); rehabilitációs kártyával rendelkezik-e; a Munkavállaló iskolai végzettsége; szakképzettsége; állampolgársága; munkaköre; munkabére; munkaegészségügyi alkalmassági igazolása; munkaruha készíttetéséhez szükséges adatok: magasság, testsúly, cipőméret; előző munkahely kilépő papírja; a Munkavállaló jövedelmét terhelő, bíróság által meghatározott levonással kapcsolatos adatok; saját e-mail címe az elektronikus munkabérjegyzék megküldéséhez; telefonszáma; törvény által meghatározott egyéb adatok.

A Munkáltató a „Beutalás munkaköri orvosi alkalmassági vizsgálatra" című üzemorvosnak átadásra kerülő dokumentumon is szerepelteti a fenti adatok közül releváns adatokat.

A jelen bekezdésben felsorolt személyes adatok kezelésének jogalapja a Munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: az „Mt.") 10. § (1) és (3) bekezdése, valamint a mindenkor hatályos egyéb adózási, társadalombiztosítási, munkaegészségügyi és munkavédelmi, valamint egyéb vonatkozó jogszabályok – többek között, de nem kizárólagosan az Adózás rendjéről szóló 2017. évi CL. törvény, a Számvitelről szóló 2000. évi C. törvény, a Személyi jövedelemadóról szóló 1995. évi CXVII. törvény, a Munkavédelemről szóló 1993. évi XCIII. törvény.

A Munkáltató másolatot készít a Munkavállaló következő, a fent felsorolt személyes adatokat tartalmazó iratairól: lakcímet igazoló hatósági igazolvány, adóazonosító kártya, TAJ-kártya, iskolai végzettséget, nyelvvizsgát igazoló bizonyítvány(ok), képesítést igazoló dokumentumok (pl. OKJ-s bizonyítványok), TB kiskönyv, NAV igazolás 25 év alatti pályakezdők esetén SZOCHO-kedvezményhez, az előző munkahelyről kapott kilépő papírok és külföldi állampolgár esetén a jogszerű magyarországi tartózkodást és munkavállalást igazoló okiratok, meghatározott munkakörök esetén járművezetői jogosítvány.

A Munkáltató, mint adatkezelő jogos érdekeinek érvényesítéséhez szükséges okból tartja nyilván a Munkáltató székhelyéül szolgáló terület üzemeltetője, a Budapest Airport Zrt. (székhelye: 1185 Budapest, BUD Nemzetközi Repülőtér; cégjegyzékszáma: 01-10-044665) által vagyonvédelmi célból működtetett beléptető rendszerek használatához szükséges, Munkavállalók használatába adott belépőkártyák számát. Munkáltató tájékoztatja a Munkavállalókat, hogy a

munkavállalók névjegyzéke a Budapest Airport Zrt. mint a székhelyül szolgáló terület üzemeltetője részére átadásra került. A beléptető rendszerekkel kapcsolatos adatkezelésre vonatkozóban bővebb tájékoztatás a Budapest Airport Zrt-től kérhető.
A Munkáltató tájékoztatja a Munkavállalókat arról is, hogy a Munkáltató helyiségeiben kamerák kerültek elhelyezésre. A kamerafelvételekre vonatkozó adatkezelésről a Munkáltató külön tájékoztatóban tájékoztatja az érintetteket.
A Munkáltató informatikai és egyéb eszközöket (elsősorban számítógép, e-mail fiók, internet hozzáférés, telefon, személygépkocsi) bocsáthat a Munkavállaló rendelkezésére munkavégzés céljából. Ennek feltételeiről és a használat megengedett módjáról bővebb információ a Munkáltató vonatkozó szabályzataiban található. A Munkáltató ezen informatikai és egyéb eszközei Munkavállaló általi használatának ellenőrzésére kizárólag az adatvédelmi jogszabályokkal, valamint az Mt. 11. § (1)-(2) bekezdéseivel összhangban, a Munkáltató jogos érdeke alapján jogosult. Amennyiben a Munkáltató élni kíván az ellenőrzés lehetőségével, úgy az ellenőrzés részleteiről és az azzal kapcsolatos adatkezelésről külön szabályzatban tájékoztatja a Munkavállalókat.
A Munkavállalók önkéntes hozzájárulása alapján kapcsolattartás céljából, a kezelheti Munkáltató a Munkavállalók következő adatait: magán telefonszám, magán e-mail cím és levelezési cím.

4. Az adatkezelés időtartama

Amennyiben az adatkezelés a Munkáltatóra, mint adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges, úgy a Munkáltató a vonatkozó jogi kötelezettség teljesítésére előírt időtartamig kezeli a Munkavállalók személyes adatait. A Munkáltató a munkavállaló biztosítási jogviszonyával összefüggő, a nyugellátás megállapítása során figyelembevételre kerülő keresetről, jövedelemről adatot tartalmazó munkaügyi iratokat a munkavállalóra irányadó öregségi nyugdíjkorhatár betöltését követő öt évig őrzi meg.
Nem selejtezhető dokumentumok esetén az adatkezelés időtartama megegyezik az őrzési idővel, azaz 50 év.
A Munkáltató, mint adatkezelő jogos érdekeinek érvényesítéséhez szükséges adatkezelések esetén az adatkezelés időtartama a munkaviszonyból eredő jogok és kötelezettségek érvényesíthetőségének elévülési idejéig, illetőleg az adott adatkezelésre vonatkozó külön tájékoztatóban vagy szabályzatban megjelölt határidőig tart.
A kizárólag a munkavállaló önkéntes hozzájárulásán alapuló adatkezeléssel érintett személyes adatok a hozzájárulás érintett általi visszavonásával ill. a munkaviszony megszűnését követően 1 hónappal törlésre kerülnek.

5. A személyes adatok megismerése, adatfeldolgozó

A munkaviszonnyal összefüggésben kezelt, jelen tájékoztatóban megjelölt személyes adatokat a Munkáltató szervezetén belül kizárólag a Humán központ azon munkatársai ismerhetik meg – és ők is csak a szükséges mértékben –, akiknek a feladatuk elvégzéséhez a Munkavállaló személyes adatainak ismerete szükséges.

A Munkáltató tájékoztatja a Munkavállalókat, hogy a Munkavállalók bizonyos személyes adatainak kezelésére adatfeldolgozókat vesz/vehet igénybe. Az adatfeldolgozók és az általuk végzett tevékenységek listáját jelen tájékoztató tartalmazza.

6. Adatbiztonság

A személyes adatok kezelésével összefüggésben a Munkáltató gondoskodik az adatok biztonságáról, továbbá megteszi mindazon elvárható technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek a vonatkozó jogszabályokban foglalt előírások érvényre juttatásához szükségesek. Ennek megfelelően az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

7. A Munkavállalók jogai, jogorvoslat

A Munkavállalók bármikor kérelmezhetik a Munkáltatótól, mint adatkezelőtől a rájuk vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, valamint - a kötelező adatkezelés kivételével – azok törlését vagy kezelésük korlátozását.

Önkéntes hozzájáruláson alapuló adatkezelés esetén vagy ha az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben a munkavállaló az egyik fél, vagy ha az a szerződés megkötését megelőzően a munkavállaló kérésére történő lépések megtételéhez szükséges, és ha az adatkezelés automatizált módon történik, úgy az érintett munkavállaló kérheti, hogy a rá vonatkozó, általa a Munkáltató mint adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, valamint, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa. Ezen adatok hordozhatóságához való jog gyakorlása során a Munkavállaló jogosult arra, hogy - ha ez technikailag megvalósítható - kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű (vagy esetlegesen az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett) feladat végrehajtásához szükséges, és nem érintheti hátrányosan mások jogait és szabadságait.
Önkéntes hozzájáruláson alapuló adatkezelés esetén az érintett bármely időpontban visszavonhatja hozzájárulását az adatkezeléshez, ez azonban nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét.
A jelen pontban meghatározott jogok érvényesítésére vonatkozó kérelmet írásban, az AEROPLEX Közép-Európai Légijármű Műszaki Központ Korlátolt Felelősségű Társaság (székhelye: 1185 Budapest, Liszt Ferenc Nemzetközi Repülőtér; e-mail cím: acehuman@aeroplex.com részére kérjük megküldeni.
Amennyiben az adatkezelés jogalapja a Munkáltató vagy egy harmadik fél jogos érdekeinek érvényesítése, úgy a Munkavállalók jogellenes adatkezelés esetén tiltakozhatnak az adatkezelés ellen postai úton vagy e-mailben a következő elérhetőségeken: AEROPLEX Közép-Európai Légijármű Műszaki Központ Korlátolt Felelősségű Társaság (székhelye: 1185 Budapest, Liszt Ferenc Nemzetközi Repülőtér; e-mail cím: acehuman@aeroplex.com.
A munkavállalók egyebekben Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (a GDPR-rendelet) és a vonatkozó egyéb adatvédelmi jogszabályok megsértése miatt panaszt tehetnek a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (postacím: 1537 Budapest, Pf. 834.; cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c; e-mail: ugyfelszolgalat@naih.hu; telefon: +36 (1) 391-1400; honlap: http://www.naih.hu).

A jelen tájékoztatóban és annak mellékletében foglalt rendelkezések a mindenkor hatályos munkaügyi és adatvédelmi jogszabályok rendelkezéseinek megfelelően módosulhatnak, illetve a Munkáltató jogosult azokat egyoldalúan módosítani.

Budapest, 2021. január 01.

2. számú melléklet: Adatvédelmi nyilvántartás

Nyilvántartási időszak:

1. A társaság adatkezelőinek nyilvántartása

Sorszám	Adatkezelő szervezeti egység	Adatkezelő személy és munkakör	Kezelt adatok	Érintett személyek /munkavállalók	Adatkezelés időtartama	
					kezdete	vége

2. A társaság adatfeldolgozóinak nyilvántartása

Sorszám	Adatfeldolgozó szervezet	Adatfeldolgozó szervezeti egység (ha ismert)	Feldolgozott adatok	Adatkezelés időtartama	
				kezdete	vége

3. Adatfeldolgozók

Sorszám	Adatvédelmi incidens bejelentésének időpontja	Adatvédelmi incidenst bejelentő	Adatvédelmi incidens adatai	Adatvédelmi incidenssel érintett adatok köre	Az érintettek jellege	Következmények	Incidens orvoslására megtett intézkedések	Egyéb bejelentések

3. számú melléklet: A társaság adatkezelői által nyilvántartott adatok

Sorszám	Adatkezelő szervezeti egység	Adatkezelő személy és munkakör	Kezelt adatok	Érintett személyek /munkavállalók	Adatkezelés időtartama	
					kezdete	vége

4. számú melléklet: Bejelentő lap az adatvédelmi felelős részére adatvédelmi incidens esetén

1. Az adatvédelmi incidenst bejelentő Tájékoztató adatai:
Név:
E-mail-cím:
Cím:
Telefonszám:
Kapcsolattartó megnevezése, elérhetősége (telefonszám, e-mail):

1.1. Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban:
1.2. Részt vesz-e az adatkezelőn kívül más az adatvédelmi incidenssel érintett szolgáltatásban:
1.3. Az adatkezelőn kívüli fél megnevezése és minősége:

2. Az adatvédelmi incidenssel kapcsolatos időpontok:

Kezdő időpont:
Záró időpont:
Az adatvédelmi incidens továbbra is fennáll:
Az incidensről való tudomásszerzés időpontja:
Az incidens észlelésének módja:
Az adatfeldolgozó általi értesítés időpontja:
A késedelmes tájékoztatás indokai:
Egyéb megjegyzések az incidens időpontját illetően:

3. Az adatvédelmi incidens adatai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

3.1. Sérülés jellege:
– bizalmas jelleg:
– integritás:
– rendelkezésre állás:

3.2. Az adatvédelmi incidens jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– eszköz elvesztése vagy ellopása:
– informatikai rendszer feltörése (hackelés):
– papíralapú dokumentum nem megfelelő módon történő megsemmisítése:
– papíralapú dokumentum elvesztése, ellopása vagy olyan helyen hagyása, amely nem minősül biztonságosnak:
– rosszindulatú számítógépes programok (pl. zsarolóprogram):

– elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön):
– személyes adatok téves címzett részére történő küldése:
– levél elvesztése vagy jogosulatlan felnyitása: – adathalászat:
– személyes adatok nagy nyilvánosság előtti jogellenes közzététele:
– személyes adatok jogosulatlan szóbeli közlése:
– egyéb:

4. Az adatvédelmi incidens okai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény (belső szabályzat megsértése által):
– szervezeten belüli, rosszhiszemű cselekmény:
– külső, rosszhiszeműnek nem minősülő cselekmény:
– külső, rosszhiszemű cselekmény:
– egyéb:

5. Az adatvédelmi incidenssel érintett személyes adatok köre:

5.1. Személyes adatok (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– személyazonossághoz kapcsolódó adatok:
– elérhetőségi adatok:
– azonosító adatok:
– személyi szám:
– hivatalos okmányok:
– helymeghatározó adatok:
– gazdasági, pénzügyi adatok:
– büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok:
– különleges adatok:

5.2. Különleges adatok (legalább egy kiválasztása kötelező):
– faji eredetre, nemzetiséghez tartozásra vonatkozó adatok:
– politikai véleményre vonatkozó adatok:
– vallásos vagy más világnézeti meggyőződésre vonatkozó adatok:
– érdekképviseleti szervezeti tagságra vonatkozó adatok:
– szexuális életre vonatkozó adatok:
– egészségügyi adatok:
– genetikai adatok:
– biometrikus adatok:
– még nem ismert:
– egyéb:

5.3. Az adatvédelmi incidenssel érintett személyes adatok becsült száma:

6. Az érintettek jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– alkalmazottak:
– felhasználók:
– ügyfelek (jelenlegi és potenciális):
– kiskorúak:
– kiszolgáltatott személyek:
– hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek:
– még nem ismert:
– egyéb:

6.1. Az incidenssel érintett adatalanyok részletes leírása (pl. adatbázisokban szereplő foglalkoztatottak leírása):

6.2. Az adatvédelmi incidenssel érintettek becsült száma:

7. Az incidens bekövetkezését megelőző események leírása:

---

8. Következmények:

8.1. Bizalmas jelleg sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult:
– az adat összekapcsolhatóvá vált az érintett egyéb adatával:
– az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges:
– egyéb:

8.2. Integritás sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– az adat módosíthatóvá vált annak ellenére, hogy archivált vagy elavult volt:
– az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták:
– egyéb:

8.3. Rendelkezésre állás sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása:
– egyéb:

8.4. Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk vagy egyéb jelentős következmények:

8.5. Az incidens valószínűsíthető hatásai az érintettekre (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– személyes adatok feletti rendelkezés elvesztése:
– érintett jogainak korlátozása:
– hátrányos megkülönböztetés:
– személyazonosság-lopás:
– személyazonossággal való visszaélés:
– pénzügyi veszteség:
– álnevesítés engedély nélküli feloldása:
– jó hírnév sérelme:
– szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése:
– egyéb:

8.6. A valószínűsíthető következmények súlyossága (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
– elhanyagolható:
– korlátozott:
– jelentős:
– maximális:

9. Az incidens orvoslására megtett intézkedések:
9.1. Megtett intézkedések (az adatvédelmi felelős vagy a bizottság tölti ki):
A megtett védelmi intézkedések leírása:

9.2. Az érintettek tájékoztatása (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
A tájékoztatás tervezett időpontja:
– még nincsen eldöntve:
– a tájékoztatás hiányának indokai:
– tényleges ideje, tartalma:
– érintetteknek javasolt intézkedések:
– intézkedések leírása, amelyek alapján az érintettek tájékoztatására nem került sor:
– tájékoztatott érintettek száma:
– az érintett tájékoztatásának formája:
– az érintetteknek szóló tájékoztatás tartalma:
– nyilvánosan közzétett információk vagy hasonló intézkedés:

10. Egyéb:

11. Egyéb bejelentések:
Más hatóságoknak (EU-tagállami) vagy tagállamnak bejelentette-e az adatvédelmi incidenst?:
Más hatóságoknak vagy 3. országnak bejelentette-e az adatvédelmi incidenst?:

5. számú melléklet: Az érintett tájékoztatása az adatvédelmi incidensről

1. Az adatvédelmi incidens időpontja:

2. Jellege:

3. Az adatvédelmi felelős/kapcsolattartó neve:

Elérhetősége:

4. Az adatvédelmi incidensből eredő valószínűsíthető következmény(ek):

5. Az adatvédelmi incidens kezelésével kapcsolatban tervezett, illetve megtett intézkedések (ideértve a hátrányos következmények enyhítését célzó intézkedéseket):

6. számú melléklet: A társaság adatkezelői által használt rendszerek

Sorszám	Adatkezelő szervezeti egység	Adatkezelő személy és munkakör	Kezelt adatok	Az adatkezeléshez használt rendszerek neve	Az adatkezeléshez használt rendszerek stáusza	
					dátum	állapot