RÁVEZETŐ PROJEKT KFT.

BELSŐ SZABÁLYOZÁS A SZEMÉLYES ADATOK KEZELÉSÉNEK RENDJÉRŐL

Hatályos: 2018. április 30. -

Belső szabályozás a személyes adatok kezelésének rendjéről

1. Célok és hatály

1.1. A jelen adatkezelési szabályzat célja a RÁvezető Projekt Kft. (a továbbiakban: Társaság) tevékenységével összefüggésben a személyes adatok kezelésével kapcsolatos belső működés meghatározása.

1.2. A szabályzatban foglaltak értelmezése, alkalmazása és végrehajtása során minden esetben irányadó a vonatkozó szabályozási környezet, így különösen:

- az Európai Parlamentnek és a Tanácsnak 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) szóló 2016/679 (2016. április 27.) számú rendelete (a továbbiakban: GDPR)
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.)
- a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről szóló 1995. évi CXIX. törvény

ismerete. A mindenkor hatályos jogszabályok tartalma a személyes adatokkal kapcsolatos valamennyi tevékenységre vonatkozóan irányadó.

1.3. Személyes adatnak minősül a ténylegesen azonosított vagy azonosítható természetes személyre (a továbbiakban: érintettre) vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy, vagy több tényező alapján azonosítható. Személyes adatnak minősül pl. a név, a telefonszám, a bankszámlaszám, a lakóhelyre vonatkozó adat, az e-mail cím, az IP-cím stb.

1.4. A személyes adatok különleges kategóriáit képezik a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok, valamint a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok. A stresszaudit adatai különleges adatnak tekintendők.

1.5. Amennyiben egy adatról nem eldönthető annak személyes adat, vagy különleges személyes adat jellege, úgy az azzal kapcsolatos belső döntésig azt úgy kell tekinteni mintha ezen minősége fennállna. Az adat személyes adatként vagy különleges személyes adatként való minősítéséről az ügyvezető dönt.

1.6. A személyes adatok kezelése során a jogszabályok, a jelen szabályzat maradéktalan betartása mellett úgy kell eljárni, hogy a tevékenység

a) személyes adatok kezelését csak az adott cél elérésére nézve feltétlenül indokolt mértékben és ideig eredményezze;
b) a személyes adatok biztonságát, az érintett természetes személyek jogait és szabadságait ne veszélyeztesse;
c) kockázatainak számbavétele során az adatvédelem kiemelt prioritást kapjon, az azokkal kapcsolatos hatások vizsgálata során pedig mindenkor a lehető legnagyobb potenciális hatásokat kell figyelembe venni és kerülni kell a kockázatok alulértékelését.

1.7. Jelen szabályzat hatálya kiterjed a Társaság valamennyi munkavállalójára, valamint tevékenységében részt vevő minden személyre – így különösen az alvállalkozókra, és szerződéses partnerekre. Valamennyi releváns szerződés esetében az ügyvezető köteles gondoskodni arról, hogy a Társaság-vel szerződést kötő fél a jelen szabályzatban foglaltakat megismerhesse.

1.8. Nem kell alkalmazni a jelen szabályzatot azon adatkezelések esetében, amelyek nem tartoznak a GDPR hatálya alá (GDPR 2-3. cikk).

2. A személyes adatok kezelhetőségére vonatkozó feltételek

2.1. Személyes adatok kizárólag az alábbi feltételek együttes teljesülése esetén kezelhetőek:

a) az adatkezelés jogalapja a GDPR 6. cikk (1) bekezdésének valamely pontját teljesíti (jellemzően: az adatkezeléshez az érintett hozzájárult vagy az adatkezelés a Társaság-re vonatkozó jogi kötelezettség teljesítéséhez szükséges);
b) a személyes adatkezelésre vonatkozó igény az ügyvezetőnek bejelentésre került;
c) az ügyvezető a személyes adatok kezelésével összefüggésben kijelölte a 2.3. pontban foglalt felelőst, valamint kereteket;
d) az adatkezelésre vonatkozóan adatvédelmi hatásvizsgálat elkészült – illetve amennyiben az adatvédelmi hatásvizsgálat alapján az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában is valószínűsíthetően magas kockázattal jár, úgy a felügyeleti hatósággal (Nemzeti Adatvédelmi és Információszabadság Hatósággal, a továbbiakban: NAIH) történt konzultáció megtörtént, és az adtakezelést a NAIH nem tiltotta meg;
e) az adatkezelés az adatvédelmi nyilvántartásban rögzítésre, valamint
f) a NAIH adatvédelmi nyilvántartásába bejelentésre került.

2.2. Amennyiben a fenti feltételek nem állnak fenn, a személyes adatok kezelése nem kezdhető meg, illetve nem folytatható – a már kezelt, vagy egyébként kezelt adatokat a 3.5 pont szerint törölni szükséges.

2.3. Valamennyi, személyes adat kezelését igénylő tevékenységet haladéktalanul jelezni kell az ügyvezetőnek, aki a jelzés alapján adatkezelésenként:

a) kijelöli az adatkezelés felügyeletéért felelős munkatársat;
b) meghatározza az adatkezelés célját,
c) meghatározza a kezelhető adatok körét,
d) meghatározza az adatvédelmi hatásvizsgálathoz szükséges kockázatelemzés, valamint a hatásvizsgálat elkészítésének határidejét,
e) meghatározza az adathoz való hozzáférés (pl. személyi, időbeli) korlátait, valamint
f) meghatározza az adattovábbítás szabályait (kinek, milyen célból, milyen feltételekkel);
g) amennyiben szükséges, úgy az adatkezeléssel összefüggésben végrehajtandó egyéb technikai és szervezési intézkedéseket rendel el (pl. az adatot tartalmazó file-ok vagy dokumentumok őrzési helyét, az adat tárolására szolgáló eszközök használatával kapcsolatos jelszókezelési szabályokat, vagy a felhasználásnak a Társaság székhelyére való korlátozását rögzíti).

A fenti pontok kapcsán hozott döntéséről tájékoztatja az adatkezelés felügyeletéért kijelölt munkatársat, valamint az irodavezetőt.

2.4. Az adatkezelés céljaként csak olyan ok vagy körülmény jelölhető meg, amely a jogszabályi elvárásokat kielégíti, a Társaság tevékenységével közvetlenül összefügg, ahhoz szükséges vagy arra nézve egyébként célszerű.

2.5. A kezelt adatok köre a minimálisan szükséges, ugyanakkor a tevékenység biztonságos és felelős ellátására nézve indokolt mértékben határozandó meg.

2.6. A 2.3-as pont szerinti adatkezelési kereteket az ügyvezető a 2.9. pont alapján, egyébként pedig indokolt esetben, de legalább minden év decemberében adatkezelésenként felülvizsgálja.

2.7. Az adatvédelmi hatásvizsgálathoz szükséges kockázatelemzést, valamint amennyiben az indokolt (azaz, ha a kockázatelemzés alapján az adatkezelés valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve) az adatvédelmi hatásvizsgálatot az adatkezelés felügyeletéért kijelölt munkatárs köteles az ügyvezető által megjelölt határidőig elvégezni. A kockázatelemzés valamint az adatvédelmi hatásvizsgálat eredményéről az ügyvezető tájékoztatni kell, valamint annak eredményeit a belső elektronikus rendszer e célra létrehozott mappájába is fel kell tölteni.

2.8. A 2.7. pont szerinti kockázatelemezés, valamint hatásvizsgálat információihoz csak az azt készítő munkatárs (vagy a munkakörét átvett személy) illetve az ügyvezető és az irodavezető számára biztosítható hozzáférés.

2.9. A kockázatelemzés, valamint a hatásvizsgálat (illetve a 2.10. pont szerint a NAIH-al folytatandó konzultáció) eredményei alapján az ügyvezető a 2.3-as pont szerint meghatározott adatkezelési kereteket – akár a kapcsolódó adatkezelésekre kiterjedően is – felülvizsgálja oly módon, hogy a módosított keretek jelöléséből (pl. verziószám, dátum stb.) megállapítható legyen a módosítással érintett korábbi utasítás, valamint a változás ténye.

2.10. Amennyiben az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően továbbra is magas kockázattal jár az érintettekre nézve, a személyes adatok kezelését megelőzően az ügyvezető köteles konzultációt kezdeményezni a NAIH-al. A konzultációba az adatkezelés felügyeletéért felelős munkatársat be kell vonni, aki annak, valamint a konzultáció megállapításai alapján végrehajtott intézkedések eredményei alapján a kockázatelemzést, valamint az adatvédelmi hatásvizsgálatot felülvizsgálja.

2.11. Az adatkezelésnek az adatvédelmi nyilvántartásba történő átvezetését az adatkezelés felügyeletéért felelős munkatárs készíti elő, és az ügyvezető hagyja jóvá.

2.12. Az adatvédelmi nyilvántartás adatait az irodavezető viszi fel az adatbázisba a 2.3. pont szerinti ügyvezetői döntés, valamint a kockázatelemzése és hatásvizsgálati dokumentumok alapján – amelyet az ügyvezető szükség szerint, de legalább évente egyszer, decemberben ellenőriz.

2.13. Ha a személyes adatok nem az érintettől kerülnek megszerzésre, az adatkezelés felügyeletéért felelős munkatárs előkészíti a GDPR 14. cikke szerinti tájékoztatást az érintett felé, amelyet az ügyvezető hagy jóvá.

3. A személyes adatok kezelésének gyakorlati szabályai

3.1. Személyes adatok kizárólag az ügyvezető által meghatározott belső szabályok és jogszabályi előírások maradéktalan betartása mellett kezelhetőek.

3.2. Amennyiben az adatkezelési szabályok megsértését észleli, azt valamennyi munkatárs, valamint szerződéses viszonyban álló személy köteles haladéktalanul jelezni az ügyvezető részére. A jelzések alapján az ügyvezető a kérdéses adatkezelési gyakorlatokat kivizsgálja vagy kivizsgáltatja, majd annak eredményei alapján megteszi a szükséges intézkedéseket a biztonságos, az érintettek jogait és szabadságait biztosító adatkezelés megteremtése érdekében.

3.3. Az érintettnek a személyes adatainak kezelésére vonatkozó kéréseit (így különösen a GDPR III. fejezetének 3. szakasza szerint megfogalmazott nyilatkozatait) az irodavezető továbbítja az adatkezelés felügyeletéért felelős munkatársnak, valamint tájékoztatásul az ügyvezetőnek. A nyilatkozatokat az adatkezelés felügyeletéért felelős munkatárs haladéktalanul, de legfeljebb 3 munkanapon belül köteles

a) amennyiben a kérés nem teljesíthető, úgy azt indoklással együtt az ügyvezető válaszaként kiküldhető levéltervezetként előkészíteni;
b) a nyilatkozatban foglaltakat – az ügyvezető értesítése mellett – végrehajtani és az érintettet a GDPR 19. cikkelye alapján tájékoztató választ előkészíteni.

3.4. A személyes adatokat törölni kell, ha

a) az adatkezelésre meghatározott időtartam eltelt, vagy az adatkezelés egyébként céltalanná, illetve indokolatlanná vált,
b) az érintett a GDPR 17. cikke alapján kéri,
c) arra a Társaságot jogszabály, bírósági vagy hatósági határozat kötelezi.

Nem törölhető olyan adat, amely a Társaság kötelezettségeinek teljesítése érdekében szükséges lehet. Az adatok törlését minden esetben az ügyvezető hagyja jóvá – ide nem értve azon automatizált adattörléseket, amelyek elektronikus adatbázisokat vagy dokumentumokat érintenek, és amelyekkel kapcsolatosan a törlési rutinokat az ügyvezető előzetesen jóváhagyott.

3.5. A személyes adatok törlése során úgy kell eljárni, hogy az a törölt adat megismerhetőségét kizárja. Így:

a) a személyes adatot tartalmazó papír alapú dokumentum
   - teljes egészében megsemmisítendő (pl. iratmegsemmisítővel),
   - ha a dokumentum teljes megsemmisítése nem indokolt, úgy a személyes adatok olvashatatlanná tételével biztosítandó a törlés

oly módon, hogy a papír alapú dokumentumról készített elektronikus másolat is törlendő, vagy az olvashatatlanná tett változattal váltandó fel;

b) a személyes adatot tartalmazó elektronikus dokumentum
   - teljes egészében törlendő, vagy
   - amennyiben annak teljes törlése nem indokolt, úgy abból a törlendő adatok távolítandóak el

oly módon, hogy az elektronikus dokumentum személyes adatot tartalmazó változata ne legyen helyreállítható.

Az elektronikus dokumentumokat, adatbázisokat a biztonsági mentésekből is törölni szükséges, vagy olyan visszaállítási protokoll biztosítandó, amely a kérdéses file-okat nem állítja vissza, és a biztonsági másolatok tartalmához nem (akár harmadik személyek, mint pl. rendszergazdai feladatokat ellátók irányában sem) teszi lehetővé.

3.6. Az adatok törléséért az adatkezelés felügyeletéért kijelölt munkatárs felelős. Az azokkal kapcsolatos informatikai támogatás érdekében az ügyvezető az adatkezelés felügyeletéért kijelölt munkatárs kérésére megfelelően intézkedik.

3.7. Az adatvédelmi incidenseket valamennyi munkatárs vagy szerződéses jogviszonyban álló személy köteles haladéktalanul jelezni az ügyvezetőnek. Az adatvédelmi incidens a biztonság olyan sérülése, amely a személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Ilyen incidensként értékelendő a személyes adatokat tartalmazó e-mail szándékolt címzettjétől eltérő személynek való megküldése, a személyes adatot tartalmazó információs és kommunikációs technológia eszköz elvesztése, vagy az informatikai rendszer feltörése például, de ilyennek tekintendő minden olyan esemény is, amely illetéktelen (arra a 2.3-as pontban foglalt döntés szerinti jogosultsággal nem rendelkező) személynek tette lehetővé a személyes adatok megismerését.

3.8. Az adatvédelmi incidenst az adatkezelés felügyeletéért kijelölt munkatárs köteles haladéktalanul kivizsgálni, és az azzal kapcsolatos kockázatokat értékelni. A kockázatértékelés eredményéről az ügyvezetőt tájékoztatni kell.

3.9. Amennyiben az incidens nem, vagy valószínűsíthetően nem járt kockázattal az érintett jogaira és szabadságaira, úgy az ügyvezető – akár a 2.3-as pont szerinti keretek felülvizsgálatával – megteszi a szükséges intézkedéseket a további incidensek elkerülése érdekében.

Az intézkedéseket az adatkezelés felügyeletéért kijelölt munkatárssal, az irodavezetővel, valamint szükség esetén a többi munkatárssal vagy szerződéses személlyel is közölni kell. Mellőzendő a többi munkatárs vagy szerződéses személy értesítése, ha a közlés feltehetően újabb adatvédelmi incidenseket alapozna meg.

3.10. Az érintett jogaira és szabadságaira kockázatot jelentő incidenseket az ügyvezető köteles jelezni a NAIH felé a GDPR 33. cikke alapján, amely adatszolgáltatás tartalmát az adatkezelés felügyeletéért kijelölt munkatárs készíti el. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelés felügyeletéért kijelölt munkatárs haladéktalanul elkészíti az érintettet az adatvédelmi incidensről tájékoztató felhívást, amelyet az ügyvezető hagy jóvá.

3.11. Az adatvédelmi incidensekről szóló nyilvántartást az irodavezető vezeti.

4. Különleges adatok kezelése

4.1. Különleges adatnak tekinthető a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adat, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

4.2. Különleges adatok kizárólag a GDPR 9. cikk (2) bekezdésében foglalt esetek, valamint a jelen szabályzat 2.1-es pontjában (ide nem értve utóbbi a) pontját) meghatározott feltételek teljesülése esetén kezelhetőek.

4.3. A különleges adatokhoz hozzáférés kizárólag az ügyvezetőnek, valamint az az adatkezelés felügyeletéért felelős munkatársnak, illetve a munkakörét helyettesítő munkatársnak adható. Más munkatársnak jogosultság, vagy külső, más szerződéses személynek hozzáférés csak különösen indokolt esetben adható.

4.4. Különleges adatok esetében az adatkezeléssel kapcsolatos kockázatok sem az adatvédelmi hatásvizsgálat, sem az adatvédelmi incidensek keretében nem zárhatóak ki, és nem értékelhetőek az azokkal kapcsolatos tevékenységek valószínűsíthetően kockázatmentesnek.

4.5. Különleges adatok esetében az azok jellegére és formájára, valamint az adatkezelés kockázataira nézve figyelemmel indokolt technikai és szervezési intézkedések elrendelése nem mellőzhető a 2.3. g) pontja során hozott ügyvezetői döntés esetében.

5. Az adatkezelések technikai háttere

5.1. Személyes adatot tartalmazó papír alapú dokumentumok kizárólag az iratkezelési szabályzatban meghatározott tárolási rendben, illetve eszközökben őrizhetők, és azok a Társaság székhelyéről kizárólag az ügyvezető engedélyével vihetőek ki.

5.2. Elektronikus formában tárolt személyes adatok, vagy személyes adatokat tartalmazó dokumentumok kizárólag jelszóval védett számítógépeken kezelhetőek, összhangban a Társaság mindenkori érvényes Információbiztonsági Szabályzatában foglalt rendelkezésekkel. Ilyen dokumentumok vagy adatbázisok külső tárhelyre vagy levelezőrendszerre történő továbbítása, illetve más, harmadik személy által potenciálisan hozzáférhető eszközökön való használata, megnyitása, tárolása tilos.

5.3. Az 5.2-es pontban foglalt számítógépekre olyan biztonsági megoldások telepítendőek fel, amelyek az informatikai biztonsági igényeket az adatkezelés tárgyával, valamint a kezelés jellegével összefüggésben biztosítják. A konkrét igények az adatvédelmi hatásvizsgálat eredményei alapján határozandóak meg.

5.4. Különleges személyes adatokat tartalmazó elektronikus dokumentumok vagy adatbázisok kizárólag a Társaság saját eszközein tárolhatók, illetve kezelhetők. Ezen eszközökre az 5.2-es pontban foglaltak megfelelően irányadók.

5.5. Személyes adatokat tartalmazó dokumentumokról vagy adatbázisokról készített biztonsági mentések (vagy ilyen dokumentumokat, illetve adatbázisokat is tartalmazó biztonsági mentések) megfelelő titkosítás mellett is kizárólag olyan környezetben tárolhatók, amelyek magas szinten támogatják az adatkezeléssel kapcsolatos garanciák megtartását, valamint nem jelentenek kockázatot az adatok biztonságára vonatkozóan.

6. További rendelkezések

6.1. Az adatkezeléssel kapcsolatos nyilatkozatokat és utasításokat írásban kell megtenni. Amennyiben az eset összes körülménye sürgős szóbeli közlést indokol, úgy az azzal kapcsolatosan tett nyilatkozatok és utasítások a szóbeli közlésre okot adó körülmény elmúltát követően haladéktalanul írásba foglalandóak. A belső működésben az írásbeliség igényének az e-mailben történő rögzítés minden esetben megfelelőnek és elégségesnek tekinthető.

6.2. Az adatvédelemmel kapcsolatos működés során mindenkor a legteljesebb mértékben törekedni kell rá, hogy a jelen szabályzatnak, valamint a jogszabályi elvárásoknak való megfelelés igazolható legyen, különösen:

a) az érintettnek az adatkezeléshez történő hozzájárulására,
b) az érintettnek a különleges adatok kezelésére tett kifejezett hozzájárulására,
c) az érintett által az egyes adatok törlésére, helyesbítésére, az adatkorlátozás teljesítéséről szóló teljesítés igazolására,
d) az adatvédelmi incidensekről szóló érintetti értesítésre vonatkozóan.

Ezen fenti esetekben az igazolhatóságot biztosító írásbeli (vagy annak minősülő) forma sürgős esetekben sem mellőzhető. Az online rendszerekkel kapcsolatos működési háttér úgy alakítandó ki hogy ezen igények teljesítését biztosítsa – így pl. abban az adatkezeléshez történő, az azonosított érintett által tett hozzájárulás egyértelműen megállapítható legyen.

6.3. Harmadik személyektől nem fogadható el olyan teljesítés, amely olyan személyes adatot tartalmaz, melynek jogszerű kezelhetősége a Társaság által a teljesítő által nem biztosított. Ezen rendelkezést a harmadik személyekkel kötött valamennyi szerződéses megállapodásban rögzíteni kell.

6.4. Jelen szabályzat szükség esetén, de legalább kétévente az ügyvezető által felülvizsgálandó.