A Stég Reklám és Grafikai Kft
1039 Budapest, Mátyás király út 64.
Adószám: 10975026-2-41
Cégjegyzékszám: 01-09-364824
Képviseli: Lőrincz Attila
Adatvédelmi Szabályzata
2018.05.24.

STÉG
REKLÁM ÉS GRAFIKAI KFT.
1039 Budapest, Mátyás király út 64.
Adószám: 10975026 2 41
Bankszámlaszám:
[illegible]

……..……..

Tulajdonos / Ügyvezető igazgató

Tartalomjegyzék

1. A Szabályzat célja és hatálya

Bevezetés

A [Szervezet neve] kinyilvánítja, hogy adatkezelési tevékenységét - a megfelelő belső szabályok, technikai és szervezési intézkedések meghozatalával - úgy végzi, hogy az minden körülmények között feleljen meg az Európai Parlament és Tanács (EU) 2016/679 rendeletének - (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK GDPR hatályon kívül helyezéséről (általános adatvédelmi rendelet, a továbbiakban: **GDPR**) - továbbá az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: **Infotv.**) rendelkezéseinek.

Cél

Jelen Szabályzat célja azon belső szabályok megállapítása és intézkedések megalapozása, amelyek biztosítják, hogy a [Szervezet neve] adatkezelő tevékenysége megfeleljen a GDPR, és az Infotv. rendelkezéseinek. A Szabályzat az **Infotv.** előírásai alapján készült, azonban elkészítése során a [szervezet neve] a **GDPR** által bevezetendő szabályozásra is tekintettel volt.

Jelen Szabályzat célja, hogy meghatározza a [szervezet neve] vezetett nyilvántartások működésének törvényes rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, és megakadályozza a személyes adatokhoz való jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Hatály

E Szabályzat hatálya természetes személyre vonatkozó személyes adatok [Szervezet neve] általi kezelésére terjed ki. Egyéni vállalkozó, egyéni cég, őstermelő ügyfeleket, vevőket, szállítókat e szabályzat alkalmazásában természetes személynek kell tekinteni.

A Szabályzat hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre vonatkozik, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat. (GDPR (14); Infotv. 2. § 1. pont).

2. Alapfogalmak

„Személyes adat":

Azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható (GDPR 4. cikk 1.pont; Infotv. 3. § 2. pont).

„Érintett"

Érintettnek minősül bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy (GDPR 4. cikk 1.pont; Infotv. 3. § 1. pont).

„Adatkezelés":

Az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése (GDPR 4. cikk 2.pont; Infotv. 3. § 10. pont).

„Adatkezelő":

Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja (GDPR 4. cikk 7.pont; Infotv. 3. § 9. pont).

„Adatkezelés korlátozása":

A tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából (GDPR 4. cikk 3.pont; Infotv. 3. § 15. pont).

„Profilalkotás":

Személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előre jelzésére használják (GDPR 4. cikk 4.pont).

„Álnevesítés":

A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni (GDPR 4. cikk 5.pont).

„Nyilvántartási rendszer":

A személyes adatok bármely módon - centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint - tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető (GDPR 4. cikk 6.pont; Infotv. 3. § 21. pont).

***„Adatfeldolgozás"**:*

Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik (GDPR 4. cikk 8.pont; Infotv. 3. § 17. pont).

„Adatfeldolgozó":

Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi (GDPR 4. cikk 8.pont; Infotv. 3. § 18. pont).

„Adatvédelmi incidens":

A személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés (GDPR 4. cikk 12.pont; Infotv. 3. § 26. pont).

„harmadik fél/személy":

Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak (GDPR 4. cikk 12.pont; Infotv. 3. § 22. pont).

3. Az adatkezelések szabályai

Adatkezelési elvek

A [szervezet neve] és szervezeti egységei gondoskodnak arról, hogy a személyes adatok

A. kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon végezzék (***jogszerűség, tisztességes eljárás és átláthatóság elve***);

B. gyűjtését csak meghatározott, egyértelmű és jogszerű célból végezzék, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon (***célhoz kötöttség elve***);

C. az adatkezelés céljai szempontjából megfelelőek és relevánsak legyenek, és a szükségesre korlátozódjanak (**adattakarékosság elve**);

D. pontosak és szükség esetén naprakészek legyenek; továbbá minden ésszerű intézkedést megtegyenek annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatok haladéktalanul törlésre vagy helyesbítésre kerüljenek (***pontosság elve***);

E. tárolása olyan formában történjen, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig tegye lehetővé (***korlátozott tárolhatóság elve***);

F. kezelését oly módon végezzék, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve (***integritás és bizalmas jelleg elve***).

A [szervezet neve]-nek és szervezeti egységeinek meg kell felelniük a fenti elveknek, és képesnek kell lenniük e megfelelés igazolására (***elszámoltathatóság elve, mint „szuper elv"***).

Adatkezelési jogalapok

Személyes adat a [szervezet neve] által akkor kezelhető, ha

- ahhoz az érintett írásban hozzájárult, vagy
- szerződésen alapul, vagy
- jogos érdek alapján, vagy
- jogi kötelezettségen (adó- és számviteli) alapul, vagy
- azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (kötelező adatkezelés).

Az érintettel az adat felvétele előtt közölni kell az adatkezelés célját, valamint azt, hogy az adatkezelés önkéntes hozzájáruláson alapul, szerződéses jogviszonyon vagy jogos érdeken alapul, vagy azt törvény, illetve helyi önkormányzat rendelete közérdeken alapuló célból rendelte-e el.

Kötelező adatkezelés esetén meg kell jelölni az adatkezelést elrendelő jogszabály-helyet.

Az érintettel az adat felvétele előtt közölni kell továbbá a releváns adatkezelés jelen Szabályzat 1. sz. mellékletében meghatározott minden részletét.

4. Adatbiztonsági rendszabályok

A [Szervezet neve] valamennyi célú és jogalapú adatkezelése vonatkozásában a személyes adatok biztonsága érdekében köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR és az Infotv. érvényre juttatásához szükségesek.

Az adatbiztonság megvalósítása érdekében a [szervezet neve] az adatkezelési műveleteket úgy tervezi meg és hajtja végre, hogy a jogszabályok és az adatkezelésre vonatkozó más szabályok alkalmazása során biztosítsa az érintettek magánszférájának védelmét.

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

A [Szervezet neve] a személyes adatokat bizalmas adatként minősíti és kezeli. A személyes adatokhoz való hozzáférést a [Szervezet neve] jogosultsági szintek megadásával korlátozza.

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

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

A [szervezet neve] megteszi továbbá azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek a jogszabályok, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatbiztonság megvalósítása érdekében [szervezet neve] garantálja, hogy illetéktelen személyek fizikailag nem férhetnek hozzá sem a papíralapú, sem pedig az informatikai rendszer egyetlen eleméhez sem.

Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a manuálisan kezelt, mind a számítógépen tárolt és feldolgozott személyes adatok biztonsága érdekében.

Manuális kezelésű adatok

Biztosítani kell az adatok / iratok és az azokat tároló eszközök, megfelelő fizikai védelmét. A manuális kezelésű személyes adatok biztonsága érdekében az alábbi intézkedéseket kell alkalmazni:

Tűz- és vagyonvédelem:
Az irattári kezelésbe vett iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell elhelyezni.

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

Archiválás:
A jelen Szabályzat különös részében említett adatkezelések iratainak archiválását évente egyszer el kell végezni.

Az archivált iratok szétválogatása és irattári kezelésbe vétele egy általános Iratkezelési szabályzatban (2. sz. melléklet) lefektetett elvek mentén kell megvalósuljon.

Számítógépen tárolt adatok

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

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

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében, különösen az alábbi intézkedéseket kell alkalmazni:

Elektronikus levelezés:
A [Szervezet neve] a személyes adatok védelme érdekében gondoskodik az elektronikus úton folytatott bejövő és kimenő kommunikáció ellenőrzéséről.

Tükrözés:
A hálózati kiszolgáló gép személyes adatok elvesztésének elkerülésére folyamatos tükrözéssel biztosítható egy tőle fizikailag különböző adathordozón.

Biztonsági mentés:
A személyes adatokat tartalmazó adatbázisok aktív adataiból rendszeresen kell külön adathordozóra biztonsági mentést készíteni. A biztonsági mentést tartalmazó adathordozót tűzbiztos fémkazettában kell őrizni. A biztonsági mentések során a mentési szabályzatának megfelelően kell eljárni.

Hozzáférés-védelem:
Ennek biztosítása érdekében a személyes ügyfél-adatokat tartalmazó informatikai rendszereket csak megfelelő szintű hozzáférés-jogosultsággal rendelkező személyek használhatják. A hozzáférés-jogosultság magában foglalja azt az elvet is, hogy kizárólag olyan terjedelmű hozzáférést kapnak az informatikai rendszert használók, amely a munka elvégzéséhez elengedhetetlenül szükséges és csak azok a személyek, akiknek az adatok kezelése és feldolgozása munkaköri feladata. Ezen hozzáférés-jogosultságokat és azok szintjeit a [szervezet neve] időközönként felülvizsgálja.
A hálózati források kizárólag érvényes felhasználónév és jelszó használatával érhetők el. A jelszavakat rendszeresen módosítani kell. A rendszer adminisztrátora legalább kéthetente köteles új jelszót megadni, az adminisztratív munkát ellátó felhasználók pedig legalább 30 naponta kötelesek megváltoztatni jelszavukat.

Ártó kódok elleni védelem:
A [Szervezet neve] az informatikai rendszereket tűzfallal védi, és vírusvédelemmel látja el.

Hálózati védelem:
A mindenkor rendelkezésre álló számítástechnikai eszközök felhasználásával meg kell akadályozni, hogy adatokat tároló, hálózaton keresztül elérhető szerverekhez illetéktelen személy hozzáférjen.

5. Adatvédelmi nyilvántartás

A [szervezet neve] adatvédelmi tisztviselője / képviselője útján az adatvédelmi teendőkkel kapcsolatos intézkedések ellenőrzése, valamint az érintett tájékoztatása céljából nyilvántartást vezet, amely tartalmazza:

A. az adatkezelés megnevezését
B. a [szervezet neve] (illetve az adott szervezeti egység) nevét és elérhetőségét, továbbá az adott személyes adatokat kezelő egyéb adatkezelő(k) nevét és elérhetőségét, valamint a [szervezet neve] képviselőjének és adatvédelmi tisztviselőjének nevét és elérhetőségét
C. az adatkezelési célokat
D. az adatkezelés jogalapját
E. az adat forrását
F. az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetését
G. az adatvédelmi incidenssel érintettek körét és számát
H. az adatvédelmi incidens időpontját, körülményeit, hatásait és az elhárítására megtett intézkedéseket; valamint
I. olyan címzettek kategóriáit, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket
J. adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információkat
K. a különböző adatkategóriák megőrzésére, illetve törlésére előirányzott határidőket
L. ha lehetséges, az adatbiztonság garantálása érdekében a [szervezet neve] által tett technikai és szervezési intézkedések általános leírását.

6. Adatvédelmi incidensek kezelése

.

Az adatvédelmi incidens fogalma

A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi; (GDPR 4. cikk 12.)

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

Adatvédelmi incidensek kezelése, orvoslása

Adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása a [Szervezet neve] vezetőjének feladata.
Az informatikai rendszereken naplózni kell a hozzáféréseket és hozzáférési kísérleteket, és ezeket folyamatosan elemezni kell.
Amennyiben a [Szervezet neve] ellenőrzésre jogosult munkavállalói a feladataik ellátása során adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell a [Szervezet neve] vezetőjét. A [Szervezet neve] munkavállalói kötelesek jelenteni a [Szervezet neve]

vezetőjének, vagy a munkáltatói jogok gyakorlójának, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek.

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

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

A. az incidens bekövetkezésének időpontját és helyét
B. az incidens leírását, körülményeit, hatásait
C. az incidens során kompromittálódott adatok körét, számosságát
D. a kompromittálódott adatokkal érintett személyek körét
E. az incidens elhárítása érdekében tett intézkedések leírását
F. a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

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

Adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensekről nyilvántartást kell vezetni, amely tartalmazza:

A. az érintett személyes adatok körét
B. az adatvédelmi incidenssel érintettek körét és számát
C. az adatvédelmi incidens időpontját
D. az adatvédelmi incidens körülményeit, hatásait
E. az adatvédelmi incidens orvoslására megtett intézkedéseket
F. az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

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

7. Adatvédelmi tisztviselő / képviselő

Az adatvédelmi tisztviselő / képviselő kinevezése

A [szervezet neve] jelen Szabályzattal adatvédelmi tisztviselőt / képviselőt nevez ki.

A [szervezet neve] adatvédelmi tisztviselője: [megbízott külsős vagy belsős munkatárs neve]

Levelezési cím: [adatvédelmi tisztviselő / képviselő levelezési címe]

Telefonszám: [adatvédelmi tisztviselő / képviselő telefonszáma]

E-mail: [adatvédelmi tisztviselő / képviselő e-mail címe]

Az adatvédelmi tisztviselő / képviselő feladatai

Az adatvédelmi tisztviselő feladatai a következők:

A. tájékoztat és szakmai tanácsot ad a [szervezet neve] és szervezeti egységei vagy az adatfeldolgozók, továbbá a [szervezet neve] adatkezelést végző munkavállalói részére az adatvédelmi jogszabályi kötelezettségeikkel kapcsolatban
B. közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában
C. ellenőrzi a törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő alkalmazottak tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is
D. kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót
E. elkészíti és naprakészen tartja az adatvédelmi és adatbiztonsági szabályzatot
F. vezeti a belső adatvédelmi nyilvántartást
G. gondoskodik az adatvédelmi ismeretek oktatásáról
H. együttműködik a NAIH-al, és az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

8. Adattovábbítás

Adattovábbítás megkeresés alapján

A [szervezet neve]-n kívüli harmadik személytől érkező adatközlésre irányuló megkeresés csak akkor teljesíthető, ha az érintett erre előzetesen írásban felhatalmazza a [szervezet neve]-t, kivéve, ha a mindenkor hatályos jogszabályok ettől eltérően rendelkeznek.

Mind az érintett hozzájárulásán alapuló, mind a [szervezet neve] jogszabályi kötelezettségének teljesítését szolgáló, megkeresés alapján teljesített adatszolgáltatással kapcsolatos tényeket, körülményeket jegyzőkönyv felvételével dokumentálni kell. A jegyzőkönyv az alábbiakat tartalmazza:

A. a megkeresést kezdeményező szerv vagy személy megnevezése, hivatalos levelezési címe, telefonszáma
B. az adatkérés célja, rendeltetése
C. az adatkérés jogszabályi alapja, illetve az érintett nyilatkozata
D. az adatkérés időpontja
E. az adatszolgáltatás alapjául szolgáló adatkezelés megnevezése
F. az adatszolgáltatást teljesítő szervezeti egység megnevezése
G. az érintettek köre
H. a kért adatok köre
I. az adattovábbítás módja.

A megkeresésre történő adattovábbításról szóló jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát pedig a [szervezet neve] releváns osztálya részére kell továbbítani.

A teljesített adattovábbításról az érintettet minden esetben értesíteni kell a jegyzőkönyv harmadik példányának megküldésével.

Külföldre történő adattovábbítás

Az EGT-államba irányuló adattovábbítást úgy kell tekinteni, mintha Magyarország területén belüli adattovábbításra kerülne sor.

Olyan adatkezelés esetén, amelynél számolni kell az EGT-államokon kívülre irányuló adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni. Az érintett írásbeli hozzájárulása nélkül személyes adat EGT-államokon kívülre nem továbbítható, kivéve ha a törvény ezt lehetővé teszi.

Az EGT-államokon kívülre irányuló adattovábbítással kapcsolatos tényeket, körülményeket jegyzőkönyv felvételével dokumentálni kell. A jegyzőkönyv az alábbiakat tartalmazza:

A. az adattovábbítás címzettje (megnevezés, hivatalos levelezési cím, telefonszám)
B. az adattovábbítás célja, rendeltetése
C. az adattovábbítás jogszabályi alapja, illetve az érintett nyilatkozata
D. az adattovábbítás időpontja
E. az adatszolgáltatást teljesítő szervezeti egység megnevezése
F. az érintettek köre
G. a továbbított adatok köre
H. az adattovábbítás módja.

Az EGT-államokon kívülre irányuló adattovábbításról szóló jegyzőkönyv első példányát az adatkezelés helyén kell őrizni, második példányát pedig a [szervezet neve] munkaügyi osztálya részére kell továbbítani.

A teljesített adattovábbításról az érintettet minden esetben értesíteni kell a jegyzőkönyv harmadik példányának megküldésével egyidejűleg.

Személyes adatok nyilvánosságra hozatala

A [szervezet neve], illetve szervezeti egységei által kezelt személyes adatok nyilvánosságra hozatala tilos, kivéve, ha törvény rendeli el. A [szervezet neve] működését bemutató - személyes adatokon is alapuló - statisztikai adatok házon belül és megfelelő jogosultsági szintek megléte esetén közölhetők.

9. Az érintett jogai és jogérvényesítési lehetőségei

Az érintett jogai

Az érintett a [szervezet neve], annak szervezeti egységei, vagy a jelen Szabályzat 1. sz. mellékletében az adott adatkezelésnél meghatározott egyéb adatkezelők elérhetőségein keresztüli jogai:

A. előzetes tájékozódáshoz való jog
B. érintett hozzáférési joga
C. helyesbítéshez való jog
D. törléshez (elfeledtetéshez) való jog
E. adatkezelés korlátozásához való jog
F. adathordozhatósághoz való jog
G. tiltakozáshoz való jog
H. automatikus döntéshozatal elleni tiltakozás joga

i. Előzetes tájékozódáshoz (tájékoztatás kérése) való jog

Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon (GDPR 13-14. cikk; Infotv. 15. § 1 bekezdés)

A [szervezet neve], illetve szervezeti egységei az érintett erre vonatkozó kérelme esetén 25 (huszonöt) naptári napon belül írásban adják meg az érintettnek a tájékoztatást.

ii. Érintett hozzáférési joga

Az érintett jogosult arra, hogy az Adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a Rendeletben meghatározott kapcsolódó információkhoz hozzáférést kapjon. (GDPR 15. cikk).

iii. Helyesbítéshez való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok - egyebek mellett kiegészítő nyilatkozat útján történő - kiegészítését. (GDPR 16. cikk; Infotv. 17. § 1 bekezdés).

A személyes adatok helyesbítésével kapcsolatos tényeket jegyzőkönyvbe kell venni.

iv. Törléshez (elfeledtetéshez) való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az Adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje, ha a Rendeltben meghatározott indokok valamelyike fennáll. (GDPR 17. cikk; Infotv. 17. § 2 bekezdés).

v. Adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést ha a rendeletben meghatározott feltételek teljesülnek. (GDPR 18. cikk; Infotv. 18. § 1 bekezdés).

vi. Adathordozhatósághoz való jog

A Rendeletben írt feltételekkel az érintett jogosult arra, hogy a rá vonatkozó, általa egy Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt,

géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik Adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az Adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta. (GDPR 20. cikk).

vii. Tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a GDPR 6. cikk (1) bekezdésének e) pontján (az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges) vagy f) pontján (az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükség) (GDPR 21. cikk; Infotv. 21. § 1 pont).

Ebben az esetben a [szervezet neve], illetve szervezeti egységei a kérelem benyújtásától számított 15 (tizenöt) naptári napon belül megvizsgálják a tiltakozást, és a vizsgálat eredményéről az érintettet írásban tájékoztatják.

Ha az érintett a [szervezet neve]-nek, illetve szervezeti egységének a döntésével nem ért egyet, illetve, ha a [szervezet neve], illetve szervezeti egysége a határidőt elmulasztja, az érintett - a döntés közlésétől, illetve a határidő utolsó napjától számított 30 (harminc) naptári napon belül - bírósághoz fordulhat.

viii. Automatikus döntéshozatal elleni tiltakozás joga

Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen - ideértve a profilalkotást is - alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené (GDPR 22. cikk).

Az érintett jogérvényesítési lehetőségei

i. NAIH vizsgálatának kezdeményezése

Az érintett a GDPR 77. cikk (Infotv. 52. § (1) bekezdése) alapján a NAIH-nál bejelentéssel vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatai kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.

A NAIH vizsgálatára vonatkozó részletes szabályokat a GDPR VIII. fejezete (Infotv. 52-58. §-ai) tartalmazza.

A bejelentés a NAIH alábbi elérhetőségein tehető meg:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Postacím: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
E-mail: ugyfelszolgalat@naih.hu
Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410
Honlap: www.naih.hu

ii. Bírósági eljárás kezdeményezése

Az érintett jogainak megsértése esetén a GDPR 79. cikke (Infotv. 22. § (1) bekezdése) alapján bírósághoz fordulhat, a bíróság ezen ügyben soron kívül jár el.

A per elbírálása a törvényszék hatáskörébe tartozik.

A per az érintett választása szerint az érintett lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindítható.

A törvényszékek felsorolása és elérhetősége az alábbi linken keresztül tekinthető meg: www.birosag.hu/torvenyszekek

10. Ellenőrzés

Az adatvédelemmel kapcsolatos előírások, így különösen jelen Szabályzat rendelkezéseinek betartását az adatkezelést végző szervezeti egységek vezetői folyamatosan ellenőrzik.
A [szervezet neve] jelen Szabályzat 7. pontjában kinevezett Adatvédelmi tisztviselő / képviselő, valamint a releváns osztály vezetője az irat- és adatkezeléssel kapcsolatos szabályzatok, jegyzőkönyvek és a belső adatvédelmi nyilvántartás áttekintésével gondoskodik az adatkezelés törvényes rendjének megtartásáról. Törvénysértés esetén a [szervezet neve] képviselője ennek megszüntetésére szólítja fel a [szervezet neve]-t, illetve érintett szervezeti egységét.

Az adatbiztonsági rendszabályok és intézkedések megtartását a [szervezet neve] képviselője által kinevezett belső ellenőr és egy informatikus munkatárs ellenőrzi.

Az egyes adatkezelések ellenőrzését szükség szerint, de legalább évente egyszer el kell végezni.

10. Záró rendelkezések

A jelen Szabályzatban foglaltakra a GDPR (Infotv.) rendelkezései az irányadók.

A Szabályzat megállapítása és módosítása

A Szabályzat megállapítására és módosítására a [Szervezet neve] ügyvezetője jogosult.

A szabályzat publikálása

Jelen Szabályzat mindenkor aktuális példánya elektronikusan elérhető a [szervezet weboldal címe] weboldalon.

11. Mellékletek

1. sz. melléklet: Adatkezelési tájékoztató(k)
2. sz. melléklet: Iratkezelési szabályzat