



Adatvédelmi szabályzat (GDPR)

ALAP ADATOK:

A jelen adatvédelmi szabályzatot a **Living-room Home Kft** adta ki, és ennek a Vállalkozásnak adatkezelési és adatfeldolgozás műveletei szabályozására szolgál.

Vállalkozás adatai:

Név (cégnév): **Living-room Home Kft** (A www.vestahome.hu oldal jogtulajdonosa)

Székhely: **1134, Budapest Váci út 47/b**

Cégjegyzékszám: **01-09-275962**

Adószám: **25452246-2-41**

Képviseli: **Horváthné Hevesi Katalin Ügyvezető**

A szabályzatot **2018. május 23.** napján a **Living-room Home Kft** igazoltan jóváhagyta, és **2018.05.25.** napjától alkalmazandó.

A jelen szabályzatot- amennyiben az ügymenetben és az adatkezelések módszertanában változás nem történik- **2018.11.03.** napján külön keletkeztető ok nélkül felülvizsgálatra kerül.

A jelen szabályzatot kötelező felülvizsgálni olyan esetekben, amikor új kockázatértékelésre okot adó esemény, avagy az adatkezelés módjában és metodikájában egyéb lényeges változás történik. Az új kockázatértékelés elkészítésére olyan okból, avagy eseményből kerül sor, amikor valószínűsíthető, hogy az adatok kezelése az érintettekre kockázatot jelenthet (így különösen új adatkezelési technológia bevezetése, alkalmazása, a korábbtól eltérő módon történő adatgyűjtés vagy adattovábbítás, stb.)

BEVEZETŐ RENDELKEZÉSEK



A Vállalkozásnak a rendes ügymenetéhez a szokásos üzleti tevékenysége körében elengedhetetlenül szükséges személyes adatokat gyűjtenie és kezelnie. A begyűjtött adatok vonatkozhatnak vevőkre/ügyfelekre, együttműködő partnerekre (beszállítókra), munkavállalókra, és egyéb olyan személyekre, akikkel a vállalkozás az üzleti tevékenysége folytatása során, avagy azon kívül, ámde az üzleti tevékenységgel érintetten (például ajánlások, stb.) kapcsolatba kerül.

A jelen szabályzat célja az, hogy biztosítsa a vállalkozás tevékenysége során a személyes adatok védelméhez fűződő jogok érvényesülését, továbbá, hogy a vállalkozó/vállalkozás által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

A jelen adatvédelmi szabályzatban rögzítésre kerül a személyes adatok gyűjtésének, tárolásának és kezelésének módja, valamint rögzítésre kerülnek a Vállalkozás adatvédelmi elvei. A jelen szabályzat az adatvédelmi szabályoknak való megfelelést szolgálja.

A jelen adatvédelmi szabályzat biztosítja, hogy a Vállalkozás

- megfelel az adatvédelmi jogi követelményeknek, és megfelelő adatvédelmi gyakorlatot és operatív tevékenységet folytat
- védi és figyelembe veszi a munkavállalók, egyéb alkalmazottak, együttműködő partnerek és beszállítók, valamint az ügyfelek/ fogyasztók/megrendelők jogait és jogos érdekeit
- nyilvánvalóvá teszi az egyes adatkezelési műveleteket (gyűjtés, őrzés, tárolás, törlés, továbbítás)
- szabályozza az adatvédelmi incidens megelőzésére vonatkozó teendőket
- szabályozza a teendőket adatvédelmi incidens esetére.

Értelmező rendelkezések:

A jelen szabályzat alkalmazásában:

1. **„személyes adat”**: azonosított vagy azonosítható természetes személyre (a jelen Szabályzatban: „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;
2. **„adatkezelés”**: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;
3. **„az adatkezelés korlátozása”**: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
4. **„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;
5. **„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;
6. **„nyilvántartási rendszer”**: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
7. **„adatkezelő”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az

- adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;
8. **„adatfeldolgozó”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
 9. **„címzett”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;
 10. **„harmadik fél”**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;
 11. **„az érintett hozzájárulása”**: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősített félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;
 12. **„adatvédelmi incidens”**: 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;
 13. **adatbiztonság**: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége; az adatkezelésnek az az állapota, amelyben a kockázati tényezőket – és ezzel a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a legkisebb mértékűre csökkentik;
 14. **hardver eszköz**: valamennyi olyan eszköz, amelynek feladata az informatikai rendszer folyamatos működésének biztosítása, vagy amely biztonsági adatmentésre, avagy másolatok készítésére szolgál,

valamint amely elektronikus vagy egyéb módon a számítógép külső behatás elleni védelmét szolgálja;

15. **hírközlő eszköz:** bármilyen technikai eszköz, technológiai eljárás, amely egy vagy több fogadó személy számára jelzések, adatok és információk továbbítására vagy fogadására alkalmas.
16. **információs önrendelkezési jog:** az Alaptörvény VI. cikkében biztosított személyes adatok védelméhez való jognak az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról;

Az adatvédelem jogi háttere

Az adatvédelemre vonatkozó alapvető szabályokat az Európai Parlament és Tanács (EU) 2016/679

Rendelete (2016. április 27.) szabályozza, mely 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 szól (általános adatvédelmi rendelet, a jelen szabályzatban a továbbiakban: GDPR).

Alapelvek

A vállalkozás/vállalkozó által alkalmazott GDPR az alábbi fontos alapelvet tartalmazza:

1. A Vállalkozás által, illetve a vállalkozási szervezetben a **cél megvalósulásához szükséges mértékben és ideig** csak olyan személyes és különleges adat kezelhető, amely **az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. (adatkezelés célja és ideje)**
2. az adatgyűjtés és kezelés kizárólag pontosan **meghatározott célból és jogcím alapján** történik
3. csak annyi adat kerül gyűjtésre és kezelésre, amennyi a célok eléréséhez feltétlenül szükséges, a vállalkozó/vállalkozás kerüli a felesleges és irreleváns adatok gyűjtését és tárolását **(adattakarékosság)**
4. A Vállalkozás munkavállalói és külső megbízottjai (a továbbiakban: a Vállalkozás alkalmazottai) a feladataik ellátása körében személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezelhetnek. **(jogszabályi megfelelés biztosítása)**

5. A személyes adatok védelméhez való jog a természetes személyek Alaptörvényben biztosított alapjoga, amely garantálja az adatalanyok információs önrendelkezési jogát. Az információs önrendelkezési jog az érintettek beleegyezésének hiányában kizárólag törvényi felhatalmazás alapján korlátozható. Az információs önrendelkezési jog tiszteletben tartása érdekében a Vállalkozás alkalmazottja személyes adatot csak az alábbi esetekben kezelhet:
 - az érintett előzetes, önkéntes és kifejezett hozzájárulása
 - szerződés teljesítése a teljesítéshez szükséges mértékben
 - az érintett vagy a Vállalkozás jogos érdekeinek érvényesítése
 - a Vállalkozás jogi kötelezettségének teljesítése
 - az érintett vagy más természetes személy létfontosságú érdeke
6. Személyes adat kezelésére csak a jelen szabályzat 5. pontjában meghatározott valamely célból, jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. Törvényben elrendelt adatkezelés esetén kizárólag a felhatalmazást adó törvényben meghatározott célból valósulhat meg adatkezelés. A Vállalkozás által kezelt – vagy a Vállalkozás részére más adatkezelő által rendelkezésre bocsátott – személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.
7. A Vállalkozás törekszik arra, hogy az általa kezelt adatok pontosak és naprakészek legyenek.
8. A Vállalkozás csak addig kezeli a személyes adatokat, ameddig az feltétlenül szükséges.
9. A Vállalkozás a szükségtelenné vált adatokat véglegesen és helyre nem állítható módon törli.
10. Az adatok feldolgozására csak az érintett jogainak figyelembe vételével kerül sor.
11. A vállalkozás minden tőle telhető és elvárható lépést megtesz az adatok védelme érdekében.
12. A vállalkozás csak akkor továbbítja az Európai Gazdasági Térségen kívül eső harmadik országnak, szervezetnek, magánszemélynek vagy vállalkozásnak, amennyiben az adott harmadik ország, szervezet, magánszemély vagy vállalkozás igazolhatóan biztosítja az adatok biztonságának kellő mértékét és módját.

A szabályzat személyi és tárgyi hatálya

A jelen szabályzat rendelkezései kötelező alkalmazása az alábbi személyi körre tejed ki:

- Vállalkozás vezetősége



- a Vállalkozás valamennyi szervezeti egysége
- a Vállalkozás valamennyi munkavállalója, ide értve a gyakornoki és önkéntes munkát végzőket is
- a Vállalkozás valamennyi beszállítója/ szerződő partnere/ alvállalkozója/ a vállalkozás érdekében vagy képviselőjében a vállalkozás kifejezett írásbeli engedélye szerint eljáró bármely más személy

A jelen szabályzat hatálya az alábbi adatok körére terjed ki:

- valamennyi érintettel összefüggésbe hozható személyes adat, különösen az érintettek:
- neve,
- postai és elektronikus levelezési címe
- telefonszáma

Kockázatok

A jelen szabályzat különösen az alábbi kockázatokkal szembeni védelmet hivatott elősegíteni:

- az adatok jogosulatlan személy vagy személyek általi megszerzése
- érintett adatokkal való rendelkezési jogának megsértése
- adatok biztonsági rendszer megsértésével/ kijátszásával történő megszerzése

Specifikus felelőségek

A Vállalkozás valamennyi vezetőjének, dolgozójának és együttműködő partnerének kötelessége annak biztosítása, hogy az adatok gyűjtése, kezelése és tárolása jogszerűen történjen. Az egyes részfeladatok és felelősségi körök az alábbiak szerint kerülnek meghatározásra:

1. A teljes jogszabályi és jogi megfelelés biztosítása a vezetőség feladata.
2. Az adatvédelmi tisztségviselő (neve: Horváth Norbert László) felelősége az alábbiakra terjed ki:
 - A vezetőség tájékoztatása az adatvédelmi kötelezettségekről, kockázatokról és feladatokról
 - Javaslattevés az adatvédelmi folyamatok és szabályzatok kialakítására, a folyamatok és szabályzatok rendszeres vizsgálata

- Adatvédelmi képzés és oktatás biztosítása a vezetőségnek és a munkavállalóknak, valamint kérésre adatvédelemmel összefüggő tanácsok nyújtása valamennyi vállalati adatkezelési kérdéssel összefüggésben
- Az érintettek megkeresésére tájékoztatás nyújtása arról, hogy a Vállalkozás milyen adatait tárolja és kezeli.
- Intézkedés adatvédelmi incidens esetére.
- Harmadik féllel kötött olyan megállapodások vizsgálata, amely adatkezelési- és továbbítási kérdéseket vet fel.
- Együttműködés a partnerek és beszállítók adatvédelmi tisztségviselőivel.
- Kapcsolattartás az illetékes adatvédelmi hatósággal.
- Amennyiben az illetékes adatvédelmi hatóság előírja, a Hatóság által tartott továbbképzéseken és konferenciákon való részvétel az adatvédelmi ismeretek naprakészen tartása érdekében.
- Ellátja a GDPR és az Infótörvény rendelkezéseiben meghatározott további feladatokat.

c) A rendszergazda/ IT vezető (neve: Horváth Norbert László) felelőssége:

- Valamennyi rendszer, informatikai szolgáltatás és eszköz informatikai biztonsági szempontoknak való megfelelésének biztosítása a rendelkezésre álló vagy ésszerűen elérhető szoftver és hardver megoldások segítségével.
- Rendszeres felülvizsgálat és ellenőrzés lefolytatása a szoftverek és hardverek megfelelő működésének biztosítása érdekében.
- Valamennyi, külső szolgáltató által biztosított és adattárolásra vagy feldolgozásra alkalmas eszköz vállalati alkalmazás megkezdése előtti értékelése, akár szoftver, akár hardver, akár offline, akár online eszközről van szó.

d) A marketinges (neve: Horváth Norbert László) felelőssége:



- Valamennyi külső kommunikációval összefüggő adatvédelmi kérdés jóváhagyása és ellenőrzése, ide értve az elektronikus és papír alapú levelezést is.
- Valamennyi külső marketing/média megkeresés esetén nyilatkozat tétele az adatvédelmi szabályzatnak megfelelően, az adatvédelmi elvek betartásával
- Amennyiben szükséges, a vállalat/vállalkozás többi dolgozója tekintetében biztosítja, hogy a marketing döntések és intézkedések megfelelnek a vonatkozó adatvédelmi jogszabályoknak.
-

Vállalti/Vállalkozási struktúra

a) Vezetőség

A Vállalkozás vezetője: Horváthné Hevesi Katalin

A Vállalkozás vezetője valamennyi, a Vállalkozás rendelkezésére bocsátott adatot megismerhet, felelős a Vállalkozás valamennyi adatkezelő és adatfeldolgozó tevékenységéért.

3. IT

IT vezetők: Horváth Norbert László

Kezelt adatok köre: informatikai háttér biztosítása

A munkavállalók általános felelősségei

Valamennyi munkavállaló (gyakornok, önkéntes), aki a jelen szabályzatban meghatározott adatokhoz hozzá fér a megszerzett adatokat kizárólag a munkavégzése körében és céljából kezelheti, rögzítheti, tarthatja nyilván.

A munkavégzés során megszerzett adatokat a munkavállaló erre vonatkozó külön írásos engedély nélkül nem oszthatja meg arra illetéktelen személyekkel, nem teheti közzé, adatot önkényesen nem kezelhet.



A Vállalat biztosítja, hogy a munkavállalók a munkavállalók képzés/oktatás keretében ismerhessék meg pontos teendőiket és feladatukat, valamint felelősségüket az adatvédelem és az adatkezelés tekintetében.

A munkavállalók kötelesek valamennyi birtokukba jutott adatot biztonságosan kezelni, munkavégzésük során elővigyázatosnak lenni, és a jelen adatvédelmi szabályzatban meghatározott feladatokat végrehajtani.

A munkavállaló köteles a szoftveres hozzáférés esetén erős és titkos jelszavakat alkalmazni, a jelszót megosztani, másnak felfedni szigorúan tilos.

Arra fel nem hatalmazott személyjel vagy személyekkel nem oszthat meg személyes adatokat, sem a vállalkozáson belül, sem azon kívül.

A munkavállaló köteles rendszeresen felülvizsgálni és aktualizálni a rendelkezésekre álló adatokat, annak érdekében, hogy személyes adat szükségtelenül ne kerüljön sem tárolásra, sem egyéb kezelésre. A már szükségtelenné váló adatok törlése a munkavállaló felelőssége.

Amennyiben a munkavállaló bizonytalan a helyes adatkezelés, vagy az adatvédelmi szempontok tekintetében, úgy köteles tanácsért a vezetőjéhez vagy az adatvédelmi tisztségviselőhöz fordulni.

Ha a munkavállaló tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

A Vállalkozás adatkezelést végző alkalmazottja fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a munkavégzése során tudomására jutott személyes adatok jogszerű kezeléséért, a Vállalkozás nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.

Informatikai és fizikai védelem

A Vállalkozó/Vállalkozás az alábbi informatikai védelmi eszközöket és módokat alkalmazza:



a) fizikai védelem

– zárható iroda

- elkülönült ügyféltér
- riasztó

b) IT védelem

- tűzfal
- vírusirtó

Adattárolás

A jelen bekezdés célja annak meghatározása, hogy az adatokat hol és milyen módon szükséges kezelni ahhoz, hogy az adatok biztonsága biztosítható legyen. Az adattárolásra vonatkozó további esetleges kérdésekkel a Rendszergazdához, illetőleg az adatvédelmi tisztségviselőhöz fordulhat a Vállalkozás munkatársa.

a) Papír alapú adatkezelés

A papír alapon kezelt adatokat olyan biztonságos helyen szükséges tárolni, ahol arra jogosulatlan személy azokat nem ismerheti meg.

Azokat az elektronikus úton érkezett vagy kezelt adatokat, melyek valamely okból nyomtatásra kerülnek elzárt irattárolóban, illetőleg elkülönítetten szükséges kezelni. A Vállalat munkatársai kötelesek gondoskodni arról, hogy a kinyomtatott iratokhoz arra jogosulatlan személyek ne férjenek hozzá. A kinyomtatott adatokat tartalmazó iratokat azonnal szükséges megsemmisíteni akkor, amikor a kinyomtatás oka megszűnik.

b) Elektronikus adatkezelés

1. Az elektronikusan tárolt adatokat védeni szükséges a jogosulatlan eléréstől, véletlen törléstől, és kémprogramokkal/vírusokkal/illetéktelen rendszerfeltörésekkel és rendszertámadásokkal szemben.
2. Az adatokat erős jelszavakkal szükséges védeni, melyek cseréjére rendszeresen, de legalább fél évente sor kerül. A jelszavaknak titkosnak, hozzáférhetetlennek kell lenniük, a munkavállalók/vezetők nem oszthatják meg azt sem egymás között, sem más személyekkel.
3. Amennyiben az adat hordozható adattárolón (CD, DVD, pendrive, egyéb külső adattároló) kerül rögzítésre, ezek az adattároló eszközöket a használatot követően biztonságos helyen, jogosulatlan személyek számára hozzáférhetetlenül szükséges tárolni.
4. Adatokat csak az arra kijelölt szervereken és hardver eszközökön szabad tárolni. Felhő alapú szolgáltatás igénybevételével adat csak a kijelölt és meghatározott szolgáltatóval kötött szerződés alapján és szerint tárolható. A Vállalkozó/Vállalkozás vezetője az adattárolás megkezdése előtt meggyőződik arról, hogy a felhő alapú szolgáltatást biztosító partner megfelel az adatvédelem jogszabályi és technikai követelményeknek.
5. Valamennyi adattárolásra szolgáló szerveret és számítógépet szükséges tűzfallal és vírusirtóval védeni.
6. A tárolt adatokat rendszeresen szükséges felülvizsgálni.
7. A személyes adatokat tartalmazó szervereket a nyitott irodahelységen kívüli elkülönített helyen szükséges tárolni.
8. Az adattárolásra alkalmazott szoftvereket rendszeresen frissíteni szükséges. A frissítés megkezdése előtt a szoftverfrissítési módszert az adatvesztés elkerülése érdekében tesztelni szükséges.
9. A személyes adatokat tilos közvetlenül a laptopra vagy egyéb mobil eszközre menteni (például tablet, okostelefon)

c) Postai küldeményekre vonatkozó speciális szabályok

A postai küldemények átvételére a Vállalkozás vezetője jogosult. Átvételre jogosult lehet más, a vezető által meghatározott személy is, azzal, hogy a küldemények bontására továbbra is a Vezető jogosult.

Az adatok felhasználása



A Vállalkozás az adatkezelés eltérő célja alapján ügyviteli és nyilvántartási célú adatkezeléseket végez. Az ügyvitelhez kapcsolódó adatkezelés a szerződés/megállapodás nyilvántartásához (iktatásához), feldolgozásához kapcsolódik. Alapvető célja az adott szerződéshez/megállapodáshoz tartozó feladatok elvégzéséhez (szerződések teljesítése), az adatkezelés szereplőinek azonosításához és a szerződés lezárásához szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott szerződés irataiban és az ügyviteli segédletekben szerepelnek; kezelésük ebből a célból csak az alapul szolgáló irat selejtezéséig lehetséges.

A nyilvántartási célú adatkezelés az egyes adatfajtákból álló adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, lekérdezhetőségét. Az adatok jogszerű és célhoz kötött használata során az alábbi intézkedések megtétele kötelező annak érdekében, hogy:

1. az adatkezelővel munkavégzésre irányuló jogviszonyban álló személyek adatait tartalmazza;
2. a foglalkozás-egészségügyi ellátásban kezelt személy betegségére, egészségi állapotára vonatkozó személyes adatokat tartalmaz, gyógykezelés, vagy az egészség megőrzése, társadalombiztosítási igény érvényesítése céljából;
3. az érintett anyagi és egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik;
4. a Vállalkozással szerződéses kapcsolatba került személyek személyes adataira, vagy azzal összefüggésben kezelt személyes adatokra vonatkozik (ügyviteli célú adatkezelés);
5. a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve, hogy – törvényben meghatározottak szerint – az adatok érintettel való kapcsolatának megállapítását véglegesen lehetetlenné teszik;
6. tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra;
7. levéltári őrzésre átadott iratokkal összefüggésben valósul meg.



A személyes adatok kezelésének célja a vállalkozás üzletviteli tevékenysége során történő felhasználása, ennek megfelelően az alábbi feladatok azonosíthatók:

- a személyes adatokkal dolgozó munkavállalók a munkaterület elhagyása során kötelesek a felhasznált eszközt képernyőzárral védeni, melyhez egyedi belépési azonosító, illetőleg kód kapcsolódik
- személyes adat csak olyan levelezőrendszeren küldhető tovább, melynek biztonsága és zárt jellege garantált, továbbá olyan címzett számára, aki megfelelő és biztos módon beazonosítható olyan személyként, aki a fogadott személyes adatokat jogszerűen megismerheti
- a személyes adatokat tartalmazó fájlokat, üzeneteket kóddal, vagy egyéb módon titkosítani szükséges
- a személyes adatok Európai Gazdasági Térségen túli továbbítása fő szabály szerint tilos; amennyiben annak továbbítása mégis szükségessé válik, úgy azt csak olyan fogadó részére szabad továbbítani, aki igazoltan megfelel a GDPR-ban foglalt valamennyi adatvédelmi követelménynek.
- a Vállalkozás napi operatív tevékenysége során tilos a saját gépre személyes adatokat menteniük, valamennyi adatot kötelező a Vállalkozás saját belső rendszerére menteni.
- a Vállalkozás működése során nem vihető ki személyes adatokat tartalmazó iratok a Vállalkozás székhelyéről vagy telephelyéről. Amennyiben ez mégis szükségessé válna, úgy e tekintetben a munkavállalók kötelesek azt bejelenteni, és egyedi jóváhagyást kérni a felettesüktől.

A kezelt adatok pontossága

A Vállalkozásnak jogszabályi kötelezettsége az általa kezelt személyes adatok naprakész és pontos nyilvántartása.

A Vállalkozás kiemelt figyelmet fordít az esetlegesen (és szükségesen) nyilvántartott különleges adatok naprakészségére és pontosságára.

A fentiek okán a Vállalkozás valamennyi munkavállalójának kiemelt feladata, hogy a tőle telhető legjobb módon az adatokat naprakészen és pontosan tartsa nyilván.



Az adatokat a lehető legkevesebb adattároló helyen szükséges tartani, a Vállalkozás munkavállalói feleslegesen és engedély nélkül semmilyen egyéb nyilvántartást, vagy személyes adatokat tartalmazó egyéb forrást nem készíthetnek.

A Vállalkozás valamennyi munkatársa köteles azon lenni, hogy a személyes adatok naprakészek legyenek, és kötelesek az adatokat az ügyfél- és egyéb kapcsolatok során folyamatosan egyeztetni.

A Vállalkozás az érintettek számára folyamatosan biztosítja az adatpontosítás lehetőségét.

Amennyiben a kezelt adatok körében pontatlan adatok kerülnek elő, azt haladéktalanul pontosítani szükséges, így különösen, ha az ügyfél az általa megadott telefonszámon vagy elektronikus levelezési címen már nem érhető el. Az elektronikus levelezés mindaddig elérhetőnek tekinthető, ameddig az ügyfél a cím megváltozását nem jelenti be, vagy onnan a kézbesítés sikertelenségére vonatkozó rendszerüzenet vissza nem érkezik. Az érintett jelzésének hiányában is pontatlannak bizonyult adatot valamennyi rendszerből és adattárolóról a pontatlanság megállapítását követően haladéktalanul törölni szükséges.

A Vállalkozás marketingért felelős munkatársának / megbízottjának a feladata a marketing levelezési-és adatrendszerek naprakészen tartása, azzal, hogy annak teljes felülvizsgálata legalább félévente különösebb ok nélkül is ütemezetten kötelező.

Az érintettek jogai

Valamennyi érintett, akinek a Vállalkozás a személyes adatait kezeli jogosult:

- tájékoztatást kérni arról, hogy milyen okból és mely adatait kezeli a Vállalkozás
- tájékoztatást kérni azon címzettekről vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölni fogják, ideértve különösen a harmadik országbeli címzetteket, nemzetközi szervezeteket
- adott esetben a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, az időtartam meghatározásának szempontjai



- kérheti az adatok helyesbítését, törlését vagy kezelésének korlátozását, tiltakozhat a személyes adatok kezelése ellen
- ha az adatokat a Vállalkozás nem az érintettől gyűjtötte, a forrásukra vonatkozó valamennyi fellelhető információ
- a Hatósághoz fordulás lehetőségéről
- tájékoztatást kérni arról, hogy hogyan érheti el a Vállalkozás által kezelt adatokat
- tájékoztatást kérni arról, hogy a Vállalkozás naprakészen tartja-e az adatait, és milyen intézkedéseket hozott a naprakészen tartás érdekében
- tájékoztatást kérni arról, hogy a Vállalkozás hogyan teljesíti az adatvédelmi kötelezettségeit.

Amennyiben valamely érintett a fenti tájékoztatások egyikét kéri, azt az „érintett hozzáférési jogának” hívjuk.

Az érintett hozzáférési joga e-mailen érkezhetsz, a Vállalkozás (info@vestahome.hu) elektronikus levelezési címére. A Vállalkozás az ilyen igények bejelentésére űrlapot alkalmazhat, melyet az érintetteknek azonban nem kötelező alkalmazni, az elektronikus levélben történő bejelentés is érvényes bejelentésnek minősül.

A Vállalkozás az érintett hozzáférési kérelmének 6 héten belüli *megismételt teljesítéséért* 12.000.- Ft., azaz tizenkettőezer forint adminisztrációs díjat kérhet kéreseként. A Vállalkozás az érintett kérelmét 14 (tizennégy) napon belül köteles teljesíteni.

Az érintettnek joga van továbbá:

- hozzájáruláson alapuló adatkezelés esetén a hozzájárulását visszavonni
- tiltakozni a személyes adatai kezelése ellen
- kérni az adatai más szerv/személy részére történő hiánytalan továbbítását (adathordozhatóság)

A Vállalkozás minden esetben pontosan azonosítja az adatkérő személyét a kért információ kiadását megelőzően.



A Vállalkozás vezetője- az adatvédelmi tisztségviselővel való egyeztetést követően- jogosult dönteni az érintett kérelméről. Ha munkavállalóhoz érkezik a megkeresés, azt haladéktalanul köteles a Vállalkozás vezetője részére továbbítani.

Az adatok egyéb okból történő hozzáférhetővé tétele

Meghatározott feltételek mellett a GDPR Rendelet megengedhetővé teszi azt, hogy jogérvényesítési okokból az érintett hozzájárulása nélkül is más számára megismerhetővé tegye az egyes személyes adatokat.

A Vállalkozás jogosult a személyes adatokat másokkal megosztani, azzal, hogy a megosztás kizárólag az igényérvényesítéshez szükséges terjedelemben és okból, illetőleg kizárólag jogszerű megkeresés alapján, szüksége esetén ügyvéd tanácsának kikérése mellett történik.

Az adatok adatfeldolgozó részére történő átadása

A Vállalkozás szervezetén kívül az alábbi okból és személyekkel (a jelen szabályzatban a továbbiakban: Partner) osztja meg az érintettre vonatkozó személyes adatokat:

- könyvelő, az adózási kötelezettségek teljesítése végett
- rendszergazda, az adat- és információbiztonság teljesítése végett
- üzemorvos, a munkavállalók foglalkozás egészségügyi felmérése végett
- tárhelyszolgáltató, mint adatfeldolgozó, a webes felület biztosítása végett
- elektronikus levelezési szolgáltató, a kapcsolattartás biztosítása végett

A vállalkozó minden esetben, valamennyi együttműködő partner tekintetében az adatok továbbításának megkezdése előtt meggyőződik arról, hogy az adott partner az Európai

Uniós és magyarországi adatvédelmi szabályoknak megfelelően jár el. A Vállalkozás valamennyi

Partnerrel írásbeli szerződést köt, melyben rögzítésre kerül:



- az adatkezelés módja
- az adatkezelés időtartama

Tájékoztatási kötelezettség teljesítése

A Vállalkozás biztosítja, hogy az érintettek tisztában legyenek azzal, hogy a személyes adataik feldolgozásra kerülnek, és felvilágosítást kapjanak arról, hogy:

- hogyan használják/dolgozzák fel az adataikat
- hogyan érvényesíthetik a jogaikat.

A fenti okból a Vállalkozás adatvédelmi tájékoztatót készít, és könnyen hozzáférhetővé teszi a magánszemélyek számára, még az adatkezelés megkezdését megelőzően. Az adatvédelmi tájékoztató minden adatkezelési művelet vagy műveletsorozat tekintetében külön- külön meghatározza az érintettek jogait, továbbá rögzíti az adatkezelés célját, módját, idejét.

Az adatkezelési tájékoztatót a Vállalkozás az érintett kérésére bármikor megküldi, azzal, hogy az adatvédelmi tájékoztató a Vállalkozás weblapján is megtalálható.

A személyes adatok törlése

A Vállalkozás törli a személyes adatokat, ha

- a személyes adatra nincsen szükség abból a célból, amelyből gyűjtötték vagy más módon kezelték
- az érintett a hozzájárulását visszavonja, és az adatkezelésnek más jogalapja nincsen
- a személyes adatok kezelése valamely okból jogellenesen történt – a személyes adatokat jogi kötelezettség teljesítése érdekében törölni kell
- a személyes adat gyermekekre vonatkozik.

A törlés szükségességének felismerése a munkavállaló feladata, aki azt- amennyiben a törlés szükségessége tekintetében bizonytalan- köteles a vezetőjének, illetőleg az adatvédelmi tisztségviselőnek jelezni.



A Vállalkozás nem töröl olyan adatot, mely a jogi kötelezettsége teljesítéséhez, illetőleg a jogai érvényesítéséhez szükséges.

A személyes adatok törlése végleges, és helyreállíthatatlan módon valósul meg.

Intézkedések adatvédelmi incidens esetén

A Vállalkozás munkavállalója, együttműködő Partnere adatvédelmi incidens esetén azonnal köteles értesíteni a Vállalkozás vezetőjét, illetőleg adatvédelmi tisztségviselőjét, akiknek haladéktalanul vizsgálatot kell indítaniuk az incidens kockázatának felmérésére. Amennyiben az szükségesnek látszik, a Vállalkozás rendszergazdáját/IT vezetőjét is haladéktalanul értesíteni kell.

Amennyiben az adatvédelmi incidens kockázatot jelent az érintett jogaira nézve, úgy a Vállalkozás legkésőbb 72 (hetvenkét) órán belül köteles azt bejelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóság incidens- bejelentési nyilvántartási rendszerébe.

A bejelentésben

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát
- közölni kell az adatvédelmi tisztviselő 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



- 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.

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

A Vállalkozó/Vállalkozás nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a Vállalkozás indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell:

- az adatvédelmi tisztségviselő neve és elérhetősége
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket
- a Vállalkozás által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

A Vállalkozás mellőzi az érintett tájékoztatását, ha a következő feltételek bármelyike teljesül:

- a Vállalkozás megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetlenné teszik az adatokat



- a Vállalkozás 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. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

EGYÉB RENDELKEZÉSEK

A Vállalkozó/Vállalkozás az adatvédelmi szabályzat megváltoztatására vonatkozó jogát fenntartja.

Budapest , 2018.05.23.