www.dussergroup.hu | professionals@dussergroup.hu | tel: +36204632008
Budapesti iroda | 1094 Budapest, Liliom u. 17.
Szekszárdi iroda | 7100 Szekszárd, Korsófölde u. 3.
Székhely | 7100 Szekszárd, Korsófölde u. 3.

Adatkezelési szabályzat

verzió: 3.0

Budapest, 2025. szeptember 1.

Tartalomjegyzék

1 Bevezetés

Jelen adatvédelmi szabályzatot a 4Sales Systems Kft. adja ki adatkezelési tevékenysége szabályozása céljából. A szabályzat rendszeresen aktualizálásra kerül a hatályos hazai és Európai Uniós jogszabályoknak való folyamatos megfelelés érdekében. Az adatvédelmi szabályzat mindenkor hatályos változata megtekinthető a www.4sales.hu weboldalon, valamint az adatkezelő 7100 Szekszárd, Korsófölde u. 3. szám alatti székhelyén és 1094 Budapest, Liliom u. 17. szám alatti telephelyén nyomtatott formátumban is elérhető.

2 Az adatkezelő adatai

Adatkezelő megnevezése: 4Sales Systems Kft.

Székhely: 7100 Szekszárd, Korsófölde u. 3.

Cégjegyzék szám: 17-09-004173

Telefon: +36204632008

Email: professionals@dussergroup.hu

Honlap: www.4sales.hu

Az adatkezelési tevékenységért felelős személy: Fűkő László ügyvezető

3 A szabályzat célja

Jelen adatkezelési szabályzat célja, hogy meghatározza az Adatkezelő által kezelt személyes adatokkal kapcsolatos legfontosabb szabályokat, az adatkezelésekre vonatkozó információkat és alapelveket.
Az adatkezelési szabályzat célja elsősorban annak biztosítása, hogy az Adatkezelő megfeleljen a hatályos jogszabályok adatvédelemmel kapcsolatos rendelkezéseinek, így különösen, de nem kizárólagosan

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,
- 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 fogyasztókkal szembeni tisztességtelen kereskedelmi gyakorlat tilalmáról szóló 2008. évi XLVII. törvény,
- a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény,
- a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény rendelkezéseinek.

4 A szabályzat hatálya

4.1 Időbeli hatály

Korábbi szabályzat felülvizsgálata megtörtént. Jelen szabályzat 2025. szeptember 1. napjától visszavonásig hatályos.

4.2 Személyi hatály

Jelen szabályzat hatálya kiterjed

- az Adatkezelőre
- az adatkezelő Munkavállalóira és Partnereire; valamint
- minden további természetes személyre, akinek adatait e szabályzat hatálya alá tartozó adatkezelések érintik.

4.3 Tárgyi hatály

Jelen szabályzat hatálya kiterjed az Adatkezelő bármely szervezeti egységében folytatott, személyes adatokat érintő adatkezelésre, függetlenül attól, hogy az elektronikusan és/vagy papíralapon történik.

5 Tájékoztatás az adatkezelésről

Az adatkezelő kötelessége tájékoztatni az érintetteket személyes adataik kezeléséről.
Jelen szabályzat elválaszthatatlan részét képezik a mellékletekben található adatvédelmi tájékoztatók. A tájékoztatók részletesen tartalmazzák az egyes adatkezelésekre vonatkozó fontos információkat, így az adatkezelési tevékenység és a folyamat leírását, az érintettek megnevezését, a kezelt adatok körét, az adatok megőrzésének előre látható időtartamát, az adatkezelések jogalapját és céljait. A tájékoztatók tartalmazzák az adatok biztonsága érdekében alkalmazott szabályokat, az érintettek jogait és jogérvényesítési lehetőségeit.
Jelen adatkezelési szabályzat kizárólag ezekkel az információkkal együtt érvényes.

6 Az adatkezelés alapvető elvei

A személyes adatok:

- kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);
- gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet („célhoz kötöttség”);
- az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”);
- pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);
- tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé („korlátozott tárolhatóság”);
- kezelését oly módon kell végezni, 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”).

Az adatkezelő felelős a fentieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

7 Felelősségek

Az Adatkezelő szervezetén belül a kezelt személyes adatokat – a feladat elvégzéséhez szükséges mértékben és ideig – csak az üggyel érintett szervezeti egység munkavállalói ismerhetik meg és használhatják fel, feltéve, hogy a személyes adatok megismerése nélkül az ügyben érdemben eljárni nem lehet.

A munkavállalók munkaköri leírásában szerepeltetni kell a személyes adatok kezelésével kapcsolatos feladatokat, különös tekintettel az adatkezelési tájékoztatások megadására, a hozzájáruló nyilatkozatok beszerzésére, a nyilvántartások kezelésére, a kezelt adatokra vonatkozó információk naprakészen tartására, valamint az incidensekkel kapcsolatos eljárásra.

Adatkezelő felelős azért, hogy minden adatkezelést végző munkavállalója megismerje jelen szabályzat rendelkezéseit. A szabályzat rendelkezéseinek betartását rendszeresen ellenőrizni kell.

8 Adatbiztonság

Az adatok biztonságával kapcsolatos rendelkezéseket az Adatkezelő információbiztonsági szabályzata tartalmazza.

9 Incidensek kezelése

9.1 Az adatvédelmi incidens fogalma

Adatvédelmi incidens a biztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

9.2 Eljárás adatvédelmi incidens esetén

Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek. Ilyen kár lehet többek között, a személyes adataik feletti rendelkezés elvesztése vagy a jogaik korlátozása, a hátrányos megkülönböztetés, a személyazonosság-lopás vagy a személyazonossággal való visszaélés, a pénzügyi veszteség, a jó hírnév sérelme, stb.

9.2.1 Bejelentés

Az adatkezelő feladata, hogy amint tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órán belül bejelentse a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) felé. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

A bejelentésben legalább

- 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 a további tájékoztatást nyújtó 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.

Amennyiben az incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, a bejelentéstől el lehet tekinteni.

9.2.2 Értesítés

Abban az esetben, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő az érintetteket is indokolatlan késedelem nélkül tájékoztatja, annak érdekében, hogy megtehessék a szükséges óvintézkedéseket. Az érintettnek nyújtott tájékoztatás közérthető formában kell, hogy tartalmazza a NAIH felé teljesítendő bejelentésre vonatkozóan a 9.2.1 pontban leírt információkat.

Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.

Az érintetteket a 3. sz. mellékletben található minta felhasználásával kell tájékoztatni.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

- az adatkezelő 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 értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;
- 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.

9.2.3 Felelősségek

Az adatkezelő bármely munkatársa, aki adatvédelmi incidenst észlel, köteles arról haladéktalanul értesíteni Az adatkezelési tevékenységért felelős személyt.

Az adatkezelési tevékenységért felelős személy gondoskodik a 9.2.1 pontban meghatározott feladatok végrehajtásáról, valamint nyilvántartásba veszi az incidenst (4. sz. melléklet).

Az adatkezelési tevékenységért felelős személy ezek mellett haladéktalanul intézkedik, hogy adatkezelő érintett munkatársai megtegyenek minden lehetséges lépést, amivel az érintett személyes adatok biztonságának és jogszerű kezelésének visszaállítása garantálható.

1. sz. melléklet: Adatkezelési tájékoztatók – a 4Sales Systems Kft.

3. sz. melléklet: Értesítés adatvédelmi incidensről

A 4Sales Systems Kft. (Székhely: 7100 Szekszárd, Korsófölde u. 3., Cégjegyzék szám: 17-09-004173, Képviselője: ... ügyvezető, Telefon: ..., e-mail: ... @dussergroup.hu, Honlap: www.4sales.hu), mint Adatkezelő
a következőkről értesíti:

…….. napon az Ön személyes adatait is érintő incidens történt.

Az események leírása:

Az érintettek kategóriái és hozzávetőleges száma:

Az érintett adatok kategóriái és hozzávetőleges száma:

Az incidensből eredő, valószínűsíthető következmények:

Az incidens orvoslására tett vagy tervezett intézkedések:

Kelt: ……..

……..
aláírás

4. sz. melléklet: Adatvédelmi incidens nyilvántartás

A nyilvántartás vezetéséért felelős személy:

Incidens időpontja	Incidens leírása	Érintettek kategóriái	Az incidens hatásai	Megtett intézkedések	A bejelentés időpontja (NAIH)	Értesítés időpontja (érintettek)

5. sz. melléklet: Érdekmérlegelési teszt

Érintett adatkezelési tevékenység:

A teszt elvégzésének indokai:

A …… (mint adatkezelő) a …….. tevékenysége keretében a …… személyes adatait kezeli.

Erre az adatkezelésre

az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (info tv.),

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, GDPR) következő rendelkezései alapján kerül sor:

GDPR 6. cikk (1) bekezdés f) pontja: 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, különösen, ha az érintett gyermek.

Info tv. 6. § (1) bekezdés b) az adatkezelő vagy harmadik személy *jogos érdekének érvényesítése céljából szükséges*, és ezen érdek érvényesítése a személyes adatok védelméhez fűződő jog korlátozásával arányban áll.

Az érdekmérlegelési tesztet annak megállapítása érdekében végezzük, hogy az adatkezelésre alapot adó jogos érdekünk arányban áll-e az adatkezeléssel érintett személy jogainak korlátozásával.

A tesztet a WP29 06/2014. számú véleményében (WP217), a NAIH 2015/515/H. számú határozatában, valamint a NAIH az előzetes tájékoztatás adatvédelmi követelményeiről szóló ajánlásában foglalt szempontok alapján végeztük el.

1. Az adatkezelő jogos érdeke

A jogos érdek leírása:

A **jogos érdek** jelentőségének értékelése:

☐ 1 - csekély jelentőségű

☐ 2 - közepesen jelentős

☐ 3 - nagyon jelentős

2. Az érintettekre gyakorolt hatás

Lehetséges hatások felsorolása	Bekövetkezés **valószínűsége** (alacsony/magas)	Következmények **súlyossága** (alacsony/magas)

A súlyosság megállapításához értékelendő szempontok:

Az érintettek száma:

Az adatok jellege (szenzitív adatokról van-e szó):

Nyilvánosan elérhetők-e az adatok:

Az adatfeldolgozás módja:

Az adatkezeléssel kapcsolatban az érintettnek ezek lehetnek az ésszerű elvárásai:

Az adatkezelő státusza:

Az érintett státusza:

A fenti szempontok alapján az **érintettekre gyakorolt hatás** jelentőségének értékelése:

☐ 1 - csekély jelentőségű

☐ 2 - közepesen jelentős

☐ 3 - nagyon jelentős

3. Biztosítékok

Az érintettre gyakorolt lehetséges negatív hatások csökkentése, illetve kiküszöbölése érdekében a következő intézkedéseket tesszük/biztosítékokat nyújtjuk:

4. Az érdekmérlegelés eredménye

Kelt:

SEGÉDLET A TESZT ELVÉGZÉSÉHEZ

A „jogos érdek”, mint jogalap akkor támaszthatja alá az adatkezelés jogszerűségét, ha az adatkezelő igazolni tudja, hogy ez a jogos érdek (akár az övé, akár más harmadik félé) fontosabb, mint az érintett személy(ek) adatkezelés által veszélyeztetett/sértett jogai, érdekei.

Ez a teszt arra szolgál, hogy az adatkezelő előzetesen fel tudja mérni, hogy a jogos érdek jogalap alkalmazható-e az adott esetben, megalapozott döntést hozzon az adatkezeléssel kapcsolatban, és dokumentált formában az érintettek rendelkezésére bocsáthassa az ezzel kapcsolatos információkat.

1 Jogos érdek

3 **kritérium**, amit vizsgálni kell, mielőtt ezt a jogalapot alkalmazzuk:

- Jogszerűnek kell lennie, tehát nem állhat szemben semmilyen jogszabályi rendelkezéssel.
- kellően egyértelműnek, pontosnak kell lennie (tehát ebben a pontban le kell írni részletesen, érthetően a jogos érdeket! Nem elég az pl. hogy a „vagyon védelme”.)
- valós és fennálló érdeknek kell lennie (nem lehet beléptető rendszert, vagy kamerás megfigyelést alkalmazni azért, mert mindenki más is így csinálja, meg kell tudni magyarázni, hogy nekünk konkrétan milyen érdekünk fűződik hozzá.)

Jogos érdek lehet például: közvetlen üzletszerzés, csalás megelőzése, dolgozók biztonsági vagy vezetési célú ellenőrzése, stb.

Fontos a jogos érdek **jellege**. Egybe eshet például közérdekkel, szélesebb közösség érdekével, ezek az elbírálásnál pozitív irányba billentik a mérleget. Ugyanilyen tényező lehet az érdek jogszerűségének széles körű jogi (pl. nem kötelező érvényű aktusok, iránymutatások), vagy társadalmi/kulturális elismerése.

Szükségesség megállapítása: Mérlegelni kell, hogy vannak-e más, kevésbé invazív eszközök.

2 Az érintettekre gyakorolt hatás

Meg kell állapítani, hogy az adatkezeléssel érintett személyek milyen alapvető, személyhez fűződő jogait és szabadságait, illetve milyen érdekeit veszélyezteti az adatkezelés, ezekre nézve milyen lehetséges hatásokkal kell számolni. Védendő érintetti jogok/érdekek pl.: információs önrendelkezési jog, személyhez fűződő jogok, magánszféra tiszteletben tartása, stb. Az ezeket érintő lehetséges hatásokat kell felsorolni, majd értékelni.
Az értékelésnél figyelembe kell venni:

- a hatás bekövetkezésének valószínűségét
- a bekövetkezett kockázatok következményeinek súlyosságát

A súlyosság megállapításához szempont pl.:

- az érintettek száma
- az adatok jellege (szenzitív adatokról van-e szó)
- nyilvánosan elérhetők-e jelenleg az adatok (ez nem zárja ki a hatást, de figyelembe kell venni!)
- adatfeldolgozás módja:
    - széles körben nyilvánosságra hozták
    - nagy mennyiségű adat feldolgozása, összekeverése
    - profilozás (ez sokszor váratlan és pontatlan következtetésekhez vezethet)
- az érintett ésszerű elvárásait (mire számíthat, mi történik az adataival?)

- az adatkezelő (munkáltató, multinacionális vállalat, piacvezető, stb.) és az érintett státuszát (gyermek, munkavállaló, diák, beteg, stb.).

A pozitív és a negatív hatásokat egyaránt figyelembe kell venni, valamint azt is, hogy milyen negatív hatásokkal járhat (másokra nézve) az adatkezelés elmaradása.

A lehetséges negatív hatások köre tág. *Pl.: az érintett kizárása, megkülönböztetése, hírnevének sérelme, tárgyalási pozíciójának romlása, de akár az irritáció, szorongás is ide tartozhat.*

Nem cél az összes negatív hatás kiküszöbölése! Az aránytalanságot kell megszüntetni.

A 3-as skálán való értékeléshez:

- Ha a leírtak alapján a veszélyeztetett érintetti jogokat magasabb számmal értékeltük, mint a saját jogos érdekünket, akkor a jogalap nem áll meg, illetve megfelelő számú és minőségű biztosíték alkalmazása szükséges ahhoz, hogy az aránytalanság kiküszöbölhető legyen. Nagyobb eltérés esetén a tesztet nem is kell folytatni, a jogalap nem alkalmazható.
- Ha a két érték egyforma, a teszt folytatható.
- Ha az érdekeink jelentősebbnek értékelhetők, a tesztet akkor is végig le kell folytatni.
- Csekély jelentőségű érdek alapján is lehetséges adatkezelést végezni, de csak akkor, ha a veszélyeztetett jogok is csekély jelentőségűek. A tesztet ilyen esetben is el kell végezni.

3 Biztosítékok

Biztosítékok nyújtásával módosítható az aránytalanság mértéke.

Ilyen biztosíték lehet pl.:

- az összegyűjtött adatok mennyiségére vonatkozó szigorú korlátozások
- az adatok azonnali törlése felhasználásuk után
- a funkcionális szétválasztás biztosítására irányuló technikai és szervezeti intézkedések
- az anonimizálási technikák megfelelő használata
- az adatok összesítése
- a magánélet védelmét erősítő technológiák
- a megnövelt átláthatóság, elszámoltathatóság, kiegészítő tájékoztatás nyújtása
- az adatfeldolgozás letiltásának lehetősége
- az adatok hordozhatósága, megismerhetősége érdekében tett lépések.

4 Az érdekmérlegelés eredménye

Végül a fentiek alapján meghozott döntést egyértelműen le kell írni. Össze kell foglalni a figyelembe vett tényezőket, és nyilatkozni arról, hogy a jogalap a teszt eredményeképpen alkalmazható-e, vagy sem.