02.HR.SZ.13.

ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZAT

VÁLTOZÁSOK KÖVETÉSE

Változások története			
Változat: **0**	**Módosítás leírása:** A vállalatirányítási dokumentációs rendszer fejlesztése során új szabályzat létrehozása.		
	Készítő	**Jóváhagyó**	**Jóváhagyás dátuma:**
	Brella Zoltán	Korom Anita	2019.03.01.

Tartalom

1. SZABÁLYOZÁS HATÁLYA

A Szabályzat személyi hatálya kiterjed az IBV Hungária Kft-vel, mint adatkezelővel kapcsolatba kerülő természetes személy ügyfelekre, munkaviszonyban álló minden olyan munkavállalóra, vagy más foglalkoztatásra irányuló jogviszonyban foglalkoztatott alkalmazottra, akik a munkájuk során, azzal összefüggésben személyes adatot kezelnek, továbbá azon munkavállalókra, vagy más foglalkoztatásra irányuló jogviszonyban foglalkoztatott alkalmazottra, akiknek az adatait a Vállalat, mint adatkezelő kezeli.

A Szabályzat személyi hatálya tekintetében a pályázó, illetve azon munkavállaló, akinek már megszűnt a munkáltatóval, mint adatkezelővel fennálló munkaviszonya – továbbiakban - munkavállalónak tekintendő.

A Szabályzat tárgya a GDPR és az Infotv. szabályainak való megfelelés érdekében a személyes adatoknak az adatkezelő által vagy az adatkezelő nevében végzett kezelése tekintetében az adatkezelői hatáskörök és felelősség szabályozása, ehhez kapcsolódóan megfelelő és hatékony technikai és szervezési intézkedések rögzítése, mely által igazolható, hogy az adatkezelési tevékenységek jogszerűek, és az alkalmazott intézkedések hatékonysága az előírásoknak megfelelő szintű.

2. SZABÁLYOZÁS CÉLJA

Az Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679 rendelet (a továbbiakban: „GDPR”), a GDPR által nem szabályozott körben az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: „Infotv.”) alapján az IBV Hungária Kft.-vel (a továbbiakban: „Vállalat”) kapcsolatba kerülő természetes személy ügyfelek, illetve munkavállalói, továbbá egyéb személyek személyes adatainak fokozott védelme, illetve ezen személyes adatok jogszerű, tisztességes és átlátható kezelése érdekében alkotja meg a jelen adatvédelmi és adatkezelési szabályzatot (a továbbiakban: „Szabályzat”).

3. TEVÉKENYSÉG LEÍRÁSA

3.1. Szabályzat karbantartása, közzététele

A Szabályzat kidolgozása, karbantartása és közzététele a központi adatvédelmi felelős feladata, végrehajtásáért a szabályzat egyes rendelkezéseinek címzettjei felelősek.

A Szabályzat felülvizsgálata, karbantartása minden naptári év december 31. napjáig esedékes, valamint soron kívül olyan jogszabályváltozás vagy felügyeleti hatóság ellenőrzése esetén, mely a Szabályzatban foglalt rendelkezéseket érinti.

3.2. A személyes adatok kezelésére vonatkozó alapelvek

A GDPR és az Infotv. szabályainak való megfelelés érdekében az alábbi elvek mentén szükséges a Szabályzat egyes rendelkezéseinek értelmezése és végrehajtása:

Jogszerűség, tisztességes eljárás és átláthatóság: a személyes adatok kezelését mindenkor jogszerűen és tisztességesen, valamint az Érintett számára átlátható módon kell végezni.

Az adatkezelés akkor jogszerű, ha az meghatározott, jogszerű célból, megfelelő jogalap megállapítása mellett a szükséges mértékű személyes adattal, a szükségesnél nem hosszabb ideig

történik, az érintett részére átlátható módon, beleértve az adatkezelést megelőző és más kapcsolódó tájékoztatásokat.

Célhoz kötöttség: a személyes adatok kezelését megelőzően mindenkor pontosan meghatározott, egyértelmű és jogszerű cél definiálása szükséges, az adatokat ezekkel a célokkal össze nem egyeztethető módon nem lehet kezelni.

Adattakarékosság: a személyes adatok mindenkor csak meghatározott célból és ezen meghatározott cél eléréséhez szükséges mértékben és ideig kezelendők.

Pontosság: a személyes adatoknak mindenkor pontosnak és naprakésznek kell lenniük. Az adatkezelés célja szempontjából pontatlan személyes adatok törlése és/vagy helyesbítése szükséges.

Korlátozott tárolhatóság: a személyes adatok csak cél eléréséhez szükséges ideig kezelendők. Ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor.

Integritás és bizalmas jelleg: a személyes adatok kezelése mindenkor az adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelem mellett történhet.

Elszámoltathatóság: az adatkezelés jogszerűségével, az adatok védelmével kapcsolatos szabályok betartásáért az adatkezelő felelős, mely kapcsán minden egyes adatkezelési művelet célját, jogalapját, időtartamát köteles meghatározni, dokumentálni, mégpedig oly módon, hogy ezt – szükség esetén - mind az érintett, mind a felügyeleti hatóság rendelkezésére tudja bocsátani.

3.4. Beépített és alapértelmezett adatvédelem vállalati szabályai

A Vállalat a GDPR rendeletben meghatározott tájékoztatások, nyilvántartások és szabályozásokon túl az alábbi technikai és szervezési intézkedéseket rendeli el a beépített és alapértelmezett adatvédelem elvének való megfelelés érdekében:

Adatvédelmi szervezet: Az adatkezelő a GDPR rendeletnek való megfelelés érdekében külön definiált, önálló adatvédelmi szervezetet működtet, mely a központi adatvédelmi felelős, a szakterületi adatvédelmi felelősökből, adatbiztonsági (IT) felelősből áll. Az adatvédelmi szervezet élén az ügyvezető áll.

Rögzített adatvédelmi feladat- és hatáskörök: Az adatkezelő a GDPR rendeletnek való megfelelés érdekében minden egyes adatvédelemmel kapcsolatos jogszabályi kötelezettség, illetve jelen Szabályzatban rögzített adatvédelemmel kapcsolatos vállalati intézkedés tekintetében meghatározza és dedikálja a feladat- és hatásköröket mind a végrehajtás, mind pedig a végrehajtás ellenőrzése tekintetében.

Adatvédelmi tudatosságot erősítő oktatások: Az adatkezelő a GDPR rendeletnek megfelelés érdekében előre meghatározott rend (időbeli ütemezés, tematika) szerint az adatvédelmi tudatosságot erősítő belső oktatásokat szervez.

Titoktartási klauzulák és titoktartási nyilatkozatok: A Vállalat személyes adatok kezelését végző munkatársai tekintetében a munkaszerződés tartalmazza, hogy a titoktartási kötelezettség munkaviszonyból származó lényeges kötelezettség. A munkaköri leírás rögzíti, hogy a munkavállaló felelős az általa kezelt személyes adatok megfelelő biztonsága érdekében, az adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztésének elkerülése érdekében minden adott helyzetben általában elvárhatót megtenni, az adatokat bizalmasan kezelni.

Adatfeldolgozói nyilvántartás: Az adatkezelő naprakész nyilvántartást vezet azokról az adatkezelőkről, melyek az adatkezelő nevében – szerződés alapján – személyes adatokat kezelnek (adatfeldolgozók).

Álnevesítés: Az adatkezelő álnevesítést nem alkalmaz adatkezelési tevékenysége során.

Adatbiztonsági intézkedések: Információbiztonsági szabályzat (IBSZ) szerint.

Évenkénti felülvizsgálat: A Vállalat évente, külső, a Vállalattól független vállalkozással felülvizsgálja az adatkezelési (jog) és adatbiztonsági (IT) tevékenységét. Ennek időigénye legalább egy nap, formája red flag audit.

Negyedévenkénti dokumentált belső ellenőrzés: A Vállalat negyedévente belső ellenőrzés keretében egy-egy szakterület belső ellenőrzését, dokumentált módon elvégzi.

Belső ellenőrzési terv: A Vállalat az évenkénti felülvizsgálat és a negyedévenkénti szakterületi belső ellenőrzéseket belső ellenőrzési tervben, dokumentált módon ütemezi.

Automatizált tájékoztatások: A Vállalat az érintetti jogok gyakorlásának elősegítése érdekében dedikált, automatizált email fiókokat működtet a kameraszabályzat, álláspályázatok, munkavállalók és a természetes személyű ügyfelek tájékoztatáshoz és hozzáféréshez való joga gyakorlásának elősegítése érdekében.

3.5. Adatvédelmi szervezet

A Vállalat a GDPR rendeletnek való megfelelés érdekében külön definiált, önálló adatvédelmi szervezetet működtet, melyet az alábbiak szerint határoz meg:

- ügyvezető
- HR generalista, mint központi adatvédelmi felelős
- szervezeti egységek vezetői, mint szakterületi adatvédelmi felelősök
- IT vezető, mint adatbiztonsági (IT) felelős
- adatkezeléssel foglalkozó beosztott munkavállalók

3.5.1. Ügyvezető

Az adatvédelmi szervezet élén az ügyvezető áll, aki

- jogosult meghatározni az adatvédelmi feladat és hatásköröket, dönt az adatvédelmi szervezet kialakításáról,
- az adatvédelmi szervezetben meghatározott egyes feladatokat és felelősséget megállapítja, és ezeket hozzáigazítja az általános szervezeti működéshez,
- az adatvédelemmel kapcsolatos belső szabályozásokra tekintettel dönt új munkaköri leírások, munkaköri feladatkatalógusok kiadásáról, ezek aktualizálásáról, módosításáról,
- fegyelmi jogkört gyakorol az adatvédelmi kötelezettségek teljesítése kapcsán,
- megbízást ad külső, független szakértő szolgáltatók részére az adatkezelés rendjének és az adatbiztonság rendjének évenként történő felülvizsgálata kapcsán,
- végső döntést hoz az olyan adatvédelemmel kapcsolatos kérdésekről, mint amilyenek
    - a beépített és alapértelmezett adatvédelemnek való megfelelés és ennek vállalati eszközei,
    - jóváhagyja az adatfeldolgozásra irányuló szerződések tartalmát, formátumát és megköti az adatfeldolgozásra irányuló szerződéseket,
    - vezetői értekezleten beszámoltatja az adatvédelmi szervezet egyes területeiért vagy szintjeiért felelős munkatársakat,

- végső döntést hoz az érdekmérlegelés alapján történő adatkezelés jogalapjáról,
- végső döntést hoz az adatvédelmi hatásvizsgálatokkal kapcsolatos kérdésekről,
- végső döntést hoz az adatvédelmi incidensek hatóság felé történő bejelentéséről, illetve arról, ha ez nem szükséges,
- kinevezi az adatvédelmi tisztviselőt, ha ez indokolttá válik.

3.5.2. Központi adatvédelmi felelős

Az adatvédelmi szervezet operatív működtetése a központi adatvédelmi felelős feladata, aki

- naprakészen tartja adatvédelmi szabályzatot, ennek keretében folyamatosan nyomon követi az adatvédelemmel kapcsolatos jogszabályváltozásokat, bírósági és hatósági gyakorlatot, változások esetén intézkedik ezek szabályzatba történő implementálása, ügyvezető által történő elfogadása és kihirdetése felől,
- az adatvédelemmel kapcsolatos változásokról a vezetői értekezleten tájékoztatja az ügyvezetőt és a szakterületi adatvédelmi felelősöket,
- elvégzi az adatvédelmi hatásvizsgálatot a szakterületi adatvédelmi felelősökkel és az adatbiztonsági (IT) felelőssel közösen,
- naprakészen vezeti az adatkezeléssel és adatfeldolgozással kapcsolatos nyilvántartásokat,
- minden új adatkezelési művelet és adat kezelése kapcsán megállapítja az adatkezelés célját, jogalapját (ennek keretében – amennyiben az adatkezelés jogalapja jogos érdek - elvégzi az érdekmérlegelési teszteket), vizsgálja az adatkezelés szükségességére vonatkozó feltételeknek való megfelelést,
- jogszabálykutatással megállapítja a jogi kötelezettség teljesítése alapján történő adatkezelés esetén a vonatkozó jogszabályhelyzet,
- a megkötésre kerülő szerződésekben, amennyiben a szerződés tárgyához kapcsolódóan kerül sor adatkezelésre, felülvizsgálja és javaslatot tesz a szerződés oly módon történő kiegészítésére, hogy abból egyértelműen kiderüljön, ha a szerződés teljesítéséhez személyes adatok kezelése szükséges,
- azon esetek kapcsán, amikor az adatkezelésre nem hozzájárulás, jogi kötelezettség, vagy a szerződés teljesítése okán kerül sor intézkedik az adatkezelő érdekmérlegelése alapján történő adatkezelési jogalap dokumentálása felől, melyet jelen szabályzat szerint elkészít és dokumentál,
- új nyomtatványok alkalmazása esetén azt adatvédelmi szempontból (különös tekintettel az adattakarékosság elvére) felülvizsgálja,
- összeállítja és koordinálja az adatvédelmi oktatásokat,
- intézkedik az adatvédelmi hatásvizsgálat elvégzése kapcsán:
  - elvégzi, dokumentálja azt, intézkedési tervet javasol az ügyvezetőnek,
  - feljegyzést készít az ügyvezető részére, ha adatvédelmi hatásvizsgálat szükségessége felmerül, de azt nem tartja indokoltnak.
- negyedévente egy alkalommal egyeztetést hív össze a szervezeti egységek vezetőivel és közösen áttekintik az egyes területek adatvédelemmel kapcsolatos teendőit, különös tekintettel az új vagy tervezett adatkezelési műveletekre,
- évente felülvizsgálja az interneten közzétett adatkezelési szabályzatot,
- kapcsolatot tart a hatósággal a szakterületi adatvédelmi felelősökkel,
- folyamatosan figyelemmel követi és javasolja, ha adatvédelmi tisztviselő kijelölése válik szükségessé.

3.5.3. Szakterületi adatvédelmi felelősök

Az adatvédelmi szervezet részeként szakterületi adatvédelmi felelősök – az ügyvezető utasítása és a központi adatvédelmi felelős útmutatása alapján - végzik a saját szakterületükhöz tartozó alábbi adatvédelmi teendők operatív irányítását:

- minden új adatkezelési művelet előtt, előzetesen még megfelelő időben köteles a központi adatvédelmi felelőssel egyeztetni és annak útmutatásai szerint eljárni,
- adatvédelmi incidens felmerülése esetén haladéktalanul értesíti a központi adatvédelmi felelőst,
- köteles a területéhez tartozó adatkezelési nyilvántartások vezetésére, ha az adatok kezelése nem szükséges, jogalapja megszűnt az adatok a nyilvántartásokból való törlés, azok azokban szereplő adatok tisztítása,
- beosztott munkavállalóik adatvédelmi tudatosságának fejlesztése, melynek keretében:
    - jó példát mutatnak a személyes adatok kezelése tekintetében,
    - folyamatosan egyeztetnek a beosztottakkal az adatkezelési műveletek jobb, biztonságosabb elvégzése érdekében,
- köteles felszólítani a szervezetéhez tartozó kilépő munkavállalót, hogy a vállalat tulajdonát képező olyan eszközökről, melyeket kizárólagosan használt (telefon, számítógép,stb.) törölje le az összes személyes adatát, magánlevelezését, még abban az esetben is, ha ez a belső szabályok által eleve tilos volt és a jelen szabályzat szerinti nyilatkozatot tegye meg, miszerint az utolsó munkában töltött napján letörölte, elvitte az esetlegesen vele kapcsolatos személyes adatokat,
- köteles a kilépő munkavállaló titoktartási nyilatkozatát bekérni, mely az üzleti titkokon túl a személyes adatokkal kapcsolatos adatokra is vonatkozik.

3.5.4. Adatbiztonsági (IT) felelős

- Az Információ biztonsági felelős (IBF) éves munkatervének elkészítése, az elfogadott terv szerint a Vállalatnál folyó tevékenységek információbiztonsági szempontból történő irányítása, a meglévő biztonság megtartása, illetve fokozása.
- Együttműködés az informatikai környezet üzemeltetőivel, az informatikai rendszerek védelmére megvalósítandó rendszer biztonsági követelmények kialakításában, az információbiztonság fokozása, a biztonsági incidensek elhárítása érdekében.
- Az informatikai rendszerfejlesztések, bővítések, beszerzések, ezekre vonatkozó szolgáltatási, rendelkezésre állási és más egyéb szerződések egységes rendszer, hálózat és biztonsági szempontból való megfelelőségének ellenőrzése. Gondoskodik arról, hogy csak információbiztonsági szempontból megbízható programok készüljenek, illetve kerüljenek beszerzésre.
- Együttműködés az adatgazdákkal és a létesítmény biztonsági vagy műszaki felelősével az információ biztonsághoz kapcsolódó feladatokban.
- Az információbiztonsági szabályzat (IBSZ) betartatásának ellenőrzése.
- A Vállalat információbiztonsági irányítási rendszerének alapját képző dokumentumok rendszeres karbantartása. Az IBSZ évente egyszeri (szükség esetén azonnali) felülvizsgálata, javaslat előterjesztése annak szükség szerinti módosításáról.
- Az informatikai rendszer biztonsági szolgáltatásainak és a Vállalat információbiztonsági követelményeinek összehangolása.
- Az informatikai rendszer biztonsági szolgáltatásai üzemeltetésének rendszeres ellenőrzése, független felülvizsgálata.
- Annak biztosítása, hogy megtörténjen az információbiztonsági incidensek kezelése, az incidensek kivizsgálása, és az incidensek kapcsán felmerült problémák elhárítása és azok nyilvántartása.
- A Vállalatnál bármilyen módon adatforgalmi, illetve információadási/fogadási kapcsolatban (adathálózat, adathordozók cseréje stb.) álló külső szervekkel történő szerződéskötés esetén az információbiztonság területét érintő részekkel kapcsolatban ellenőrzési, javaslat-tételi joga és kötelezettsége van.
- Az információbiztonsági irányítási rendszer rendszeres felülvizsgálata, a védelmi eszközökkel való ellátottság rendszeres ellenőrzése.

- Az informatikai rendszer változásainak folyamatos nyomon követése, és az annak során tapasztaltaknak megfelelően, módosítási javaslatok elkészítése a Vállalat információbiztonsági dokumentációs rendszerére vonatkozólag.
- A belső szabályozási dokumentum-tervezetek véleményezése az információbiztonságot érintő kérdések vonatkozásában.
- Az általa észlelt, vagy hozzá beérkezett bejelentések alapján, az adatfeldolgozás-, és kezelés biztonságát sértő események, szabálysértések kivizsgálása - az esetleges rossz szándékú hozzáférési kísérletek, illetéktelen adatfelhasználás kiszűrése, a rendszerek eseménynaplóinak kiértékeltetése, intézkedésekre történő javaslattétel.
- Az informatikai rendszerben kialakított, aktuálisan beállított jogosultságok és a jóváhagyott jogosultságok összevetése, ellenőrzése.
- Annak ellenőrzése, hogy megtörtént-e minden informatikai konfigurációs-elem (rendszerelemek) nyilvántartásba vétele és azonosítása az értékek hatásos védelemének kialakításához.
- Annak ellenőrzése, hogy megtörtént-e a leselejtezésre kerülő eszközök adathordozóinak, háttértárainak törlése.
- A Vállalat informatikai adatfeldolgozó tevékenységének és az informatikai kommunikációs hálózat biztonságának folyamatos ellenőrzése. A számítástechnikai munkafolyamat bármely részének előzetes bejelentési kötelezettség nélküli ellenőrzése.
- Az információbiztonság tudatosságának növelése: oktatás(ok) tematikájának meghatározása, szakmai felügyelete, lefolytatása.
- Közreműködik a Vállalat informatikai auditjai során.
- Éves belső IT audit lefolytatásában közreműködik

3.5.5. Adatkezeléssel foglalkozó beosztott munkavállalók

A Vállalat minden olyan munkavállalója, aki adatkezeléssel érintőlegesen is foglalkozik, köteles

- személyes adatok kezelésére vonatkozó szabályokat ismerni és betartani,
- adatvédelmi oktatásokon részt venni, az ott elhangzottak a munkaviszonyra vonatkozó utasításként kezelni, napi ügymenet gyakorlatába beépíteni,
- minden egyes személyes adat felvétele előtt az érintett részére előzetes és számára érthető módon történő tájékoztatására, majd a hozzájárulás – feltéve, hogy az adatkezelés jogalapja hozzájárulás - dokumentált módon, jelen szabályzat, vagy a külön konkretizáló utasítások szerinti beszerzésére az elszámoltatható és átlátható adatkezelés elősegítése végett,
- bármilyen adatvédelemmel kapcsolatos panasz, szóbeli észrevétel vagy megjegyzés esetén köteles azt emailen jelezni a szakterületi és a központi adatvédelmi felelős részére,
- ha a munkaterületen közzétett adatvédelemmel kapcsolatos képi vagy szöveges tájékoztatások hiányosak, azt haladéktalanul köteles jelezni a szakterületi és a központi adatvédelmi felelős felé,
- személyes adatok védelméről köteles szervezetben elfoglalt helyének, feladat és hatáskörének megfelelően eleget tenni, így különösen, de nem kizárólagosan:
    - csak a szükséges és indokolt személyes adatok felvétele,
    - a személyes adatokat tartalmazó iratok, adathordozók védelme,
    - amikor a számítógépén nem dolgozik, elhagyja az irodát a számítógépet lockolni
    - csak olyan iratokat tartani az asztalon, amivel éppen dolgozik
    - minden olyan személyes adatot tartalmazó irat, amivel éppen nem dolgozik biztonságosan elzárni,
    - a rá bízott iratokat záró szekrény a kulcsát az adatbiztonsági elveknek megfelelően elzárva tartani,
    - a jelszavait bizalmas helyen tárolni,
    - a rá bízott laptopot, telefont őrizni, azt tilos őrizetlen helyen (például gépjárműben) felügyelet nélkül hagyni.

3.6. Adatvédelmi tisztviselő

A Vállalat adatvédelmi szervezetet, ennek keretében belül központi adatvédelmi felelőst, szakterületi adatvédelmi felelősöket és adatbiztonsági (IT) felelőst jelöl ki, ugyanakkor a GDPR szerinti adatvédelmi tisztviselő kijelölése nem indokolt.

3.7. A Vállalat főbb adatkezelési műveleteinek nyilvántartásai

A Vállalat naprakész részletes nyilvántartást vezet az adatkezelési tevékenységeiről, mely rögzíti az

- adatkezelés célját,
- az érintettek kategóriáit,
- a személyes adatok kategóriát,
- az adatkategóriák törlésére előirányzott határidőket,
- technikai és szervezési intézkedések leírását,
- címzettek kategóriáit, akikkel – esetlegesen - személyes adatot közöl vagy továbbít.

A Vállalat adatkezelési műveleteit az alábbi szakterületi bontás szerint tartja nyilván:

- Operáció szervezeti egység adatkezelési műveletei
- Gazdasági osztály szervezeti egység adatkezelési műveletei
- HR (és munkaügyi) osztály adatkezelési műveletei
- Ipari üzletág – Műszaki szervezeti egység adatkezelési műveletei
- Ipari üzletág – Kereskedelem szervezeti egység adatkezelési műveletei
- Lámpa üzletág – Műszaki szervezeti egység adatkezelési műveletei
- Lámpa üzletág – Kereskedelem szervezeti egység adatkezelési műveletei

A Vállalat adatkezelési műveleteiről vezetett adatkezelési tevékenységek nyilvántartását minden szakterületi adatvédelmi felelős maga köteles naprakészen tartani, melyet a központi adatvédelmi felelős folyamatosan felügyel és a belső ellenőrzési terv szerint dokumentált módon is ellenőriz.

3.8. Adatkezelés célja és jogalapja

A személyes adatok kezelése csak jogszerűen, tisztességesen és az érintett számára is átlátható módon történhet, ennek keretében meghatározott, egyértelmű és jogszerű cél rögzítése, megfelelő jogalap azonosítása és dokumentálása, az előre meghatározott törlési idő szerint a szükséges mértékű adatot érintő, az adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztése, megsemmisítése vagy károsodása elleni védelem biztosítása szükséges.

3.9. Adatkezelés jogalapjának megállapítási rendje

3.9.1. Lehetséges adatkezelési jogalapok

Az adatkezelés céljához igazodó jogalapok – a Vállalatnál - az alábbiak lehetnek:

- hozzájárulás [GDPR 6. cikk (1) a)],
- jogi kötelezettség teljesítése [GDPR 6. cikk (1) c)],
- szerződés megkötése [GDPR 6. cikk (1) b)],
- szerződés teljesítése [GDPR 6. cikk (1) b)],
- hozzájárulás [GDPR 6. cikk (1) a)],
- jogos érdek/érdekmérlegelés [GDPR 6. cikk (1) f)],
- az érintett vagy más természetes személy létfontosságú érdekének védelme [GDPR 6. cikk (1) d)]

3.9.2. Lehetséges adatkezelési jogalapok azonosítása

Az adatkezelés céljához igazodó jogalap megállapítása a központi adatvédelmi felelős útmutatása alapján a szakterületi adatvédelmi felelős feladata, mely kapcsán az alábbi teendők elvégzése szükséges:

- lehetséges jogalapok azonosítása,
- a kiválasztott jogalapokkal kapcsolatos adminisztráció elvégzése,
    - adatkezelés jogalapjának dokumentuma,
    - adatkezelési tevékenységek nyilvántartásában való rögzítés,
    - érintetti tájékoztatások felől történő intézkedés.

3.9.3. Lehetséges adatkezelési jogalapok azonosítása

Az elszámoltathatóság elvének való megfelelés érdekében az adatkezelés jogalapját minden esetben írásban szükséges meghatározni az alábbiak szerint:

- Jogi kötelezettség teljesítéséhez kapcsolódó adatkezelés esetén szükséges annak a jogszabálynak a meghatározása, melynek teljesítése érdekében történik az adatkezelés. Külön dokumentum nem szükséges, adatkezelési tevékenységek nyilvántartásában történő rögzítés elegendő.

- Szerződés megkötésére irányuló (ajánlat) adatkezelés esetén szükséges a szerződés típusának, tárgyának a meghatározása. Külön dokumentum nem szükséges, adatkezelési tevékenységek nyilvántartásában történő rögzítés elegendő.

- Szerződés teljesítésével összefüggő adatkezelés esetén szükséges a szerződés típusának, tárgyának a meghatározása. Külön dokumentum nem szükséges, adatkezelési tevékenységek nyilvántartásában történő rögzítés elegendő.

- Hozzájárulás alapján történő adatkezelés esetén a hozzájárulás tényét igazoló dokumentum beszerzése (hozzájáruló nyilatkozat), továbbá az adatkezelés adatkezelési tevékenységek nyilvántartásában történő rögzítése szükséges.

- Jogos érdek alapján történő adatkezelés esetén külön érdekmérlegelés elvégzése szükséges. Az érdekmérlegelést a szükségesség arányosság elve alapján (érdekmérlegelés tesztje) végez el a Vállalat, feltéve, hogy az adatkezeléssel elérendő cél más jogalappal nem megvalósítható és az érintett magánszférájának korlátozása arányban áll az elérendő céllal. Dokumentuma az érdekmérlegelés, továbbá az adatkezelést szükséges rögzíteni az adatkezelési tevékenységek nyilvántartásában.

- Létfontosságú érdek alapján történő adatkezelés esetén külön dokumentum elkészítése szükséges, melyben az érintett, az adatkezelő vagy harmadik személy létfontosságú érdeke meghatározásra és igazolásra kerül. Külön dokumentum elkészítésén túl, az adatkezelést szükséges rögzíteni az adatkezelési tevékenységek nyilvántartásában.

A Vállalat a GDPR 6. cikk (1) e) pontja alapján közérdekű vagy átruházott közhatalmi jogosítványt nem gyakorol így az adatkezelések során nincs ilyen adatkezelési jogalap.

3.10. Korlátozott tárolhatóság

A Vállalat központi adatvédelmi felelőse az adatkezelési tevékenységek nyilvántartásában adatkezelési műveletekhez igazodóan figyelemmel azok céljára, jogalapjára törlési időket határoz meg és ennek megfelelően intézkedik a törlések végrehajtásának ellenőrzése felől.

Azon adatok törlése, melyek kezelése nem szükséges az adatot közvetlen módon kezelő szakterületi adatvédelmi felelős feladata.

3.11. Adatbiztonság

A Vállalat jelen Szabályzatban meghatározott technikai és szervezési intézkedéseken túl külön információbiztonsági szabályozást alakított ki, amely rögzíti az adatbiztonsági alapelvek alkalmazásának módjait és feltételeit. A Vállalat által meghatározott jogosultsági szintek korlátozzák az adatokhoz való hozzáférést mind adatkezelő, mind adatfeldolgozó oldalon. Az informatikai rendszerek biztonsága érdekében a Vállalat tűzfalat működtet, valamint víruskereső és vírusirtó programot, a külső- és belső adatvesztések megelőzése érdekében.

További irányított információbiztonsági intézkedések:
- üzemeltetés- és fejlesztésbiztonság,
- az adatszivárgás megelőzése,
- az üzletfolytonosság fenntartása,
- a kártékony kódok elleni védelem,
- az adatok biztonságos tárolása, továbbítása, feldolgozása,
- behatolás védelem és felderítés,
- a jogosulatlan hozzáférés megelőzése,
- a sérülékenység- és incidenskezelés,
- a munkavállalók biztonsági képzése.

A részletes információbiztonsági szabályzat nem nyilvános, annak megismerésére csak az IT osztály munkatársai, a Gazdasági vezető és az Ügyvezető jogosultak.

3.12. Érintettek tájékoztatása

Az érintetteket a Vállalat az adatkezelés során – külön kérés nélkül – az alábbiakról tájékoztatja:
- adatkezelő személye, elérhetőségei
- adatkezelés célja
- adatkezelés jogalapja
- kezelt adatok köre
- címzettek, adattovábbítás
- címzettek, adatfeldolgozás
- érintettek köre
- adatkezelési időtartama
- személyes adatok forrása (ha azt a Vállalat harmadik féltől kapta)
- adatkezelés módja (manuális vagy automatizált)
- technikai és szervezési intézkedések
- érintetti jogok és joggyakorlás

Az érintettek tájékoztatásának hozzáférhetősége érdekében a Vállalat az alábbiakat határozza meg:
- Álláskeresők részére az allas@ibv.hu e-mail címen érdeklődők számára automatikus válaszüzenetben. Személyes érdeklődés esetén szóban történik az adatkezelési tájékoztatás
- Látogatók esetében a kamera rendszer használata kapcsán figyelemfelhívó jelzéseket alkalmaz a Vállalat, illetve biztosítja a Kamera szabályzat elérhetőségét fizikálisan a teher- és személyportán, valamint a recepción, továbbá elektronikusan a kamera@ibv.hu a-mail címen érhető el.
- A honlapon az Adatkezelési szabályzat elérhetősége biztosított.

3.13. Érintteti jogok gyakorlásának elősegítése

Az érintettet az alábbi jogok illetik meg a személyes adataival kapcsolatban:

3.13.1. Tájékoztatáshoz való jog

Az érintettnek joga van a Vállalattól tájékoztatást kérni az adatkezeléssel kapcsolatos körülményekről, melynek a Vállalat az alábbi adatkezelési tájékoztatások által tesz eleget az adatkezelésekkel egyidejűleg:

- Tájékoztató az álláspályázattal kapcsolatos adatkezelésről
- Tájékoztató a munkaviszonnyal kapcsolatos adatkezelésről
- Tájékoztató a kamerarendszer alkalmazásáról

Az érintett adatkezeléssel kapcsolatos egyéb kérdései tekintetében a Vállalat központi adatvédelmi felelőse illetékes.

3.13.2. Hozzáféréshez való jog

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 az adatkezeléssel kapcsolatos információkról hozzáférést kapjon.

3.13.3. Törléshez való jog

Az érintett jogosult arra, hogy kérésére a Vállalat indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat. A Vállalat az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törli, amennyiben a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték, illetve, ha a személyes adatokat jogellenesen kezelték.

Az érintett ilyen irányú kérését minden esetben a Vállalat központi adatvédelmi felelőse felé is továbbítani szükséges.

3.13.4. Az adatkezelés korlátozásához való jog

Az érintett jogosult arra, hogy a Vállalat korlátozza az adatkezelést, az alábbi feltételek fennállása esetén:

- jogellenes adatkezelés esetén, ha az érintett ellenzi az adatok törlését és ehelyett kéri azok felhasználásának korlátozását,
- a Vállalatnak már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett tiltakozott az adatkezelés ellen, ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

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

Az érintett ilyen irányú kérését minden esetben a Vállalat központi adatvédelmi felelőse felé is továbbítani szükséges.

3.13.5. Tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a Vállalat érdekmérlegelésén alapuló kezelése ellen. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelés olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

Az érintett ilyen irányú kérését minden esetben a Vállalat központi adatvédelmi felelőse felé is továbbítani szükséges.

3.13.6. Jogorvoslathoz való jog

Az érintett megilleti a jogorvoslat joga. Amennyiben az érintett panasszal kíván élni személyes adatainak kezelésével kapcsolatban jogosult mind az adatkezelőhöz, mind a felügyeleti hatósághoz panaszt benyújtani, valamint bírósági jogérvényesítéssel élni. Bírósági jogérvényesítés esetén az érintett a pert választása szerint a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt indíthatja meg.

3.13.7. Helyesbítéshez, elfeledtetéshez, valamint adathordozhatósághoz való jog

Az érintettet személyes adatainak kezelésével kapcsolatban megilleti a helyesbítéshez, elfeledtetéshez, valamint az adathordozhatósághoz való jog.

Az érintett ilyen irányú kérését minden esetben a Vállalat központi adatvédelmi felelőse felé is továbbítani szükséges.

3.14. Adatvédelmi tudatosságot erősítő oktatások

3.14.1. Új belépők oktatása

A Vállalattal újonnan munkaviszonyt (vagy más foglalkoztatásra irányuló jogviszonyt) létesítő munkavállalók adatvédelmi oktatáson vesznek részt, amely az új munkavállaló betanítási programjának részét képezi.

3.14.2. Éves rendes oktatás

A központi adatvédelmi felelős évente legalább egy alkalommal oktatást tart az adatvédelmi tudatosság emelése érdekében, amelyen kötelesek részt venni a Vállalat kijelölt munkatársai. Az adatvédelmi oktatás legalább az alábbi témákra kiterjed:

- az előző oktatás óta eltelt időszak tapasztalatai az adatvédelem területén,
- amennyiben az előző oktatás óta módosult a Szabályzat, a módosítással kapcsolatos legfontosabb tudnivalók,
- az esetlegesen megtörtént adatvédelmi incidens bemutatása, értékelése, a helyesbítő-megelőző intézkedések ismertetése,
- az adatvédelem területén érintő jogszabály módosítások, Magyarországon és az Európai Unióban, különös tekintettel a magyar és más EU-s hatóságok bírságolási gyakorlatára.

3.14.3. Rendkívüli oktatás

A központi adatvédelmi felelős rendkívüli oktatást tart – amennyiben az indokolt - az alábbi esetekben:

- adatvédelmi incidens megtörténte,
- marasztalással záruló felügyeleti hatósági eljárás lefolytatása a Vállalattal szemben,
- adatvédelmi bírság kiszabása a Vállalat versenytársaival szemben
- adatvédelmi bírság kiszabása a Vállalat székhelye szerinti településen működő adatkezelővel szemben

A rendkívüli adatvédelmi oktatásról jelenléti ívet szükséges készíteni és az oktatás tematikáját, az oktató nevét, beosztását hozzá kell tűzni.

A rendkívüli adatvédelmi oktatásról jelenléti ívet szükséges készíteni és az oktatás tematikáját, az oktató nevét, beosztását hozzá kell tűzni.

3.15. Adatvédelmi hatásvizsgálatok elvégzésének rendje

Az adatvédelmi hatásvizsgálat célja az adatkezelés szabályosságának, szükségességének és arányosságának vizsgálata. A hatásvizsgálat a GDPR előírásainak teljesítését, a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelését segíti elő a kezelésükre szolgáló szabályok, intézkedések pontos meghatározásával.

Az adatvédelmi hatásvizsgálat rendeltetése annak felderítése és értékelése, hogy az adott adatkezelés milyen kockázatokat hordoz az érintettek magánszférájára nézve, illetve ezek a kockázatok milyen intézkedésekkel csökkenthetők és szüntethetők meg.

Az adatvédelmi hatásvizsgálat kiterjed:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, (beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket);
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett természetes személyek jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására.

Adatvédelmi hatásvizsgálatot kötelezően el kell végezni, amennyiben az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Elvégzése a központi adatvédelmi felelős és az ügyvezető közös feladata.

3.16. Adatfeldolgozókkal történő együttműködésre vonatkozó szabályok

Adatfeldolgozó az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel [GDPR 4. cikk 8. pont].

3.16.1. Adatfeldolgozókkal kapcsolatos feladat- és hatáskörök

A szakterületi adatvédelmi felelősök kötelesek minden olyan új szerződéskötést megelőzően egyeztetést kezdeményezni a központi adatvédelmi felelőssel, amikor az adatkezelést az adatkezelő nevében más végzi (adatfeldolgozó).

A központi adatvédelmi felelős – adatfeldolgozásra és az együttműködésre irányuló szerződés(ek) megkötését megelőzően – köteles az adatkezelőktől megfelelő garanciákat kérni, hogy az adatkezelés a GDPR követelményeinek megfelelően, az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtása mellett történik.

Az adatfeldolgozásra irányuló szerződések megkötésre történő előkészítése, ellenőrzése a központi adatvédelmi felelős feladata. Az adatfeldolgozókról az adatkezelő nyilvántartást vezet. A nyilvántartás vezetése a központi adatvédelmi felelős feladata.

3.16.2. Előzetes adatfeldolgozói nyilatkozat és adatfeldolgozásra irányuló szerződés

Az adatfeldolgozókkal az általuk történő adatkezelést megelőzően – az együttműködésre vonatkozó szerződés részeként, vagy amellett – adatfeldolgozásra irányuló szerződést szükséges kötni. Az adatfeldolgozásra irányuló szerződés megkötésének feltétele az adatfeldolgozó által előzetesen adott nyilatkozat, melyben az adatfeldolgozó kijelenti, hogy

- rendelkezik információbiztonsági szabályozással, amely leírja az adatbiztonsági alapelvek alkalmazásának módjait és feltételeit;
- a meghatározottak a jogosultsági szintek, melyek korlátozzák az adatokhoz való jogosulatlan hozzáférést
- tűzfalat működtet, az informatikai rendszerek biztonsága érdekében;
- rendelkezik víruskereső és vírusírtó programmal, a külső- és belső adatvesztések megelőzése érdekében;
- irányított információbiztonsági intézkedéseket hajt végre:
    - üzemeltetés- és fejlesztésbiztonság,
    - adatszivárgás megelőzése,
    - az üzletfolytonosság fenntartása,
    - kártékony kódok elleni védelem,
    - az adatok biztonságos tárolása, továbbítása, feldolgozása,
    - behatolás védelem és felderítés,
    - a jogosulatlan hozzáférés megelőzése,
    - a sérülékenység- és incidenskezelés,
    - a munkavállalók biztonsági képzése kapcsán.

Az adatfeldolgozásra irányuló szerződést írásban kell megkötni, és egyúttal meg kell határozni:

- az adatkezelés tárgyát (szerződés tárgya),
- az adatkezelés célját,
- a feldolgozott személyes adatok körét,
- az adatfeldolgozás időtartamát,
- az érintettek körét,
- az utasítások rendjét (az adatfeldolgozó személyes adatokat csak az adatkezelő írásbeli utasításai alapján kezel),
- az adatfeldolgozó tájékoztatási kötelezettségét adatvédelmi incidens esetére,
- adatfeldolgozás bizalmasságát (adatfeldolgozó biztosítja azt, hogy a személyes adatok, kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt álljanak),
- adatbiztonsággal kapcsolatos intézkedéseket,
- további adatfeldolgozókkal kapcsolatos rendelkezések.

Az előzetes adatfeldolgozói nyilatkozatot és adatfeldolgozásra irányuló szerződést az együttműködésre vonatkozó nevesített (pl. megbízási, vállalkozási szerződés) vagy nevesítetlen szerződéssel együtt szükséges kezelni, tárolni és később archiválni.

3.16.3. Adatfeldolgozói nyilvántartás

A Vállalat naprakész nyilvántartást vezet azokról az adatkezelőkről, melyek a Vállalat nevében – szerződés alapján – adatfeldolgozóként személyes adatokat kezelnek.

Az adatfeldolgozói nyilvántartás vezetése a központi adatvédelmi felelős feladata.

3.17. Adatvédelmi incidensek kezelésének és bejelentésének rendje

A Vállalat minden munkatársa köteles a tudomására jutott adatvédelmi incidenst haladéktalanul jelenteni a központi adatvédelmi felelősnek.

3.17.1. Központi adatvédelmi felelős értesítése az adatvédelmi incidensről

Az értesítésnek az alábbi adatokat tartalmaznia kell:
- az adatvédelmi incidenst észlelő személy nevét,
- amennyiben az adatvédelmi incidens észlelő és jelentő személy nem azonos, úgy az adatvédelmi incidenst jelentő személy nevét,
- az adatvédelmi incidens rövid leírását,
- annak tényét, hogy az észlelt adatvédelmi incidens érinti-e a Vállalat informatikai rendszerét vagy sem,
- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

Az észlelésről szóló értesítést abban az esetben is haladéktalanul meg kell tenni, ha az fenti adatok teljes körűen nem állnak rendelkezésre a bejelentés pillanatában. A hiányzó adatokat annak felmerülésekor haladéktalanul meg kell küldeni a központi adatvédelmi felelős részére.

Az adatvédelmi incidensről szóló értesítést bizonyítható módon, írásban, aláírással és dátummal ellátott módon kitöltve kell megküldeni a központi adatvédelmi felelős részére. Amennyiben – elháríthatatlan okból - az adatvédelmi incidenst észlelő vagy jelentő személy nem tudja írásban megtenni a jelentést, ezért ez szóban történik, úgy a központi adatvédelmi felelős köteles erről jegyzőkönyvet felvenni, amelynek tartalmaznia kell legalább az előző pont szerinti információkat. Az adatvédelmi incidenst észlelő vagy jelentő személy az akadály megszűnését követően haladéktalanul köteles írásban is megerősíteni az általa előadottakat és jegyzőkönyvbe foglaltakat.

Amennyiben az adatvédelmi incidens érinti a Vállalat informatikai rendszerét is, akkor a központ adatvédelmi felelős az adatvédelmi incidens kivizsgálásába bevonja a Vállalat adatbiztonsági (IT) felelősét is.

Az értesítés érkezését követően a központi adatvédelmi felelős – az érintett szervezeti egységek bevonásával - haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését.

A Vállalat területei kötelesek a központi adatvédelmi felelőssel együttműködni, valamint az incidensre vonatkozó adatokat, információkat, a megelőzés és kiküszöbölésre vonatkozó érdemi javaslatokat a központi adatvédelmi felelős részére megadni.

3.17.2. Az adatvédelmi incidensek kategorizálása

A Vállalat az adatvédelmi incidenseket három kategóriába sorolja:
1. kategória: valószínűsíthetően kockázattal nem járó incidens,
2. kategória: valószínűsíthetően alacsony kockázattal járó incidens,
3. kategória: valószínűsíthetően magas kockázattal járó incidens.

A Vállalat az adatvédelmi incidenst az alábbi szempontok szerint értékeli:
- az incidens típusa (bizalmassági, integritási vagy elérhetőségi),
- a személyes adatok jellege (személyes adat / különleges kategória),
- a személyes adatok száma,

- az érintett személyek száma,
- az érintett természetes személyek kategóriái,
- az érintett természetes személyek azonosíthatósága,
- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- az érintett adatkezelés jogalapja.

A Vállalat az incidens értékelése során az alábbi konkrét szempontok alapján értékeli:
- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok,
- az incidensben érintett személyes adatok száma meghaladja a 100 darabot,
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az incidensben érintett természetes személyek száma meghaladja a 100 főt,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím)
- az incidensben érintett adatkezelés jogalapja az érintett létfontosságú érdeke
- az incidensben érintett adatkezelés jogalapja jogos érdek/érdekmérlegelés szerinti jogalap, személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget okozzanak az érintettjüknek.

Az incidenst a Vállalat „1. kategória: valószínűsíthetően kockázattal nem járó „incidens”-nek minősíti, ha:
- a konkrét vizsgálandó szempontok közül legfeljebb kettő áll fenn és
- a Vállalat képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

Az incidenst a Vállalat „2. kategória: valószínűsíthetően alacsony kockázattal járó „incidens”-nek minősíti, ha:
- a konkrét vizsgálandó szempontok közül egy áll fenn és
- a Vállalat nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

Az incidens a Vállalat „3. kategória: valószínűsíthetően magas kockázattal járó „incidens”-nek minősíti, ha:
- a konkrét vizsgálandó szempontok közül legfeljebb kettő áll fenn és
- a Vállalat nem képes annak bizonyítására, hogy az érintett személyes adatokat olyan fizikai és/vagy informatikai védelemmel látta el, amely védelem az incidens bekövetkezése óta nem sérült.

3.17.3. Adatvédelmi incidensek felügyeleti hatóság részére történő bejelentése

Amennyiben a Vállalat az 2. kategóriába vagy a 3. kategóriába tartozónak minősíti az incidenst, úgy a központi adatvédelmi felelős az értékelés megtörténtét követően, de legkésőbb 72 órával azután, hogy az adatvédelmi incidens a Vállalat tudomására jutott, az adatvédelmi incidenst bejelenti a felügyeleti hatóság részére és az adatvédelmi incidensek nyilvántartásában rögzíti.

A felügyeleti hatóságnak történő bejelentésnek tartalmazza:
- az adatvédelmi incidenssel érintett adatok körét és hozzávetőleges számát,
- az adatvédelmi incidenssel érintett személyek körét és hozzávetőleges számát,

- az adatvédelmi incidens jellegét, körülményeit,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- az adatvédelmi incidens valószínűsíthető következményeit és
- az adatvédelmi incidens orvoslására és enyhítésére megtett intézkedéseket.

A 2. és 3. kategóriába tartozó adatvédelmi incidens esetén az érintetteket írásban, utólag igazolható módon szükséges tájékoztatni.

Az 1. kategóriába tartozó adatvédelmi incidens esetén bejelentés nem szükséges a felügyeleti hatósághoz, ugyanakkor az adatvédelmi incidensek nyilvántartásába az esetet a központi adatvédelmi felelős rögzíti.

3.18. Hivatkozások

- Európai Parlament és a Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679 rendelet
- információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

4.DEFINÍCIÓK

Az alábbi alapelvek, fogalmak megfelelnek a GDPR 4. cikkében és az Infotv. 3. §-ban meghatározott értelmező rendelkezéseknek, így különösen:

Adatállomány: az egy nyilvántartásban kezelt adatok összessége;

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;

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel. az adatkezelő és bármely, az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre tagállami vagy uniós jogszabály kötelezi;

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen a

- **gyűjtés:** adatok összerendezése és rögzítése akár gépi úton, akár emberi észlelő, leíró, rögzítő tevékenységgel, amely művelet során az adatok azonosíthatók és visszakereshetők;
- **rögzítés:** adat változatlan módon visszaidézhető formában történő, hordozóra való felvitele;
- **rendszerezés:** külön meghatározott szempontok szerinti csoportosítás, különböző tulajdonságok alapján besorolás;
- **tagolás:** adatok tételekre (csoportokra, indokolt esetben fajtákra) történő felosztása;
- **tárolás:** adatot tartalmazó hordozók elkülönített és biztonságos együttkezelése;
- **átalakítás vagy megváltoztatás:** az adat tartalmának vagy például valamely jellemzőjének körében foganatosított módosítása;
- **lekérdezés:** az adatkezelőhöz intézett, adathoz történő hozzáférésre irányuló kifejezett kérelem;
- **betekintés:** külön hozzájárulás alapján meghatározott adat megismerését célzó tevékenység;
- **felhasználás:** adat jogszabályban meghatározott célra történő alkalmazása, használata;

- **közlés:** adat külön meghatározott harmadik személy részére történő közvetlen továbbítása akként, hogy az adat illetéktelenek számára nem válik hozzáférhetővé;
- **továbbítás:** az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
- **terjesztés vagy egyéb módon történő hozzáférhetővé tétel:** az adatok bármilyen módon történő közlése bárkivel
- **összehangolás vagy összekapcsolás:** adatok egymáshoz történő végleges vagy időleges hozzárendelése, illetve logikai társítása akként, ezen művelet végrehajtásából új adat keletkezhet;
- **korlátozás:** a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
- **törlés:** az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
- **megsemmisítés:** az adatot tartalmazó adathordozó végleges, a benne foglalt információ helyreállításának lehetőségét kizáró módon történő hozzáférhetetlenné tétele, törlése,

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;

Adatminimalizálás: a kockázatok súlyosságának csökkentése az adatok minimalizálása révén (az adatok érzékenységének csökkentése például azok szűrésével, az adatkezelés célja szempontjából szükséges adatok eltávolítása, álnevesítés stb.).

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. Ez különösen, de nem kizárólagosan jelentheti személyes adat jogellenes kezelését vagy feldolgozását (jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés);

Adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából;

Bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntető eljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;

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;

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy;

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;

Hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adat - teljes körű vagy egyes műveletekre kiterjedő - kezeléséhez;

Irat: a Vállalat működése vagy személy tevékenysége során keletkezett vagy hozzá érkezett, egy egységként kezelendő rögzített információ, adategyüttes, amely jellemzően papír formátumban jelenik meg, tartalma lehet szöveg, adat, grafikon, hang, kép, mozgókép vagy bármely más formában lévő információ vagy ezek kombinációja,

Iratkezelés: az irat készítését, nyilvántartását, rendszerezését és a selejtezhetőség szempontjából történő válogatását, szakszerű és biztonságos megőrzését, használatra bocsátását, selejtezését, illetve irattárba adását együttesen magában foglaló tevékenység,

Kockázat: természetes személyek jogait érintő kockázatok származhatnak a személyes adatok kezeléséből, amelyek eredménye lehet fizikai, vagyoni, nem vagyoni kár, hátrányos megkülönböztetés, személyazonosság lopás, vagy személyazonossággal való visszaélés, szakmai titoktartási kötelezettség által védett személyes adat bizalmas jellegének sérülése, az álnevesítés engedély nélküli feloldása, gazdasági vagy szociális hátrány. A kockázatok közé sorolandó, ha az adatkezelés genetikai adatokra, egészségügyi adatokra, a szexuális életre, a büntetőjogi felelősség megállapítására vonatkozik, továbbá, ha a személyes jellemzők értékelésére, így a munkahelyi teljesítmény, gazdasági helyzet, egészségi állapot, személyes preferenciák, érdeklődési körök, megbízhatóság vagy viselkedés, tartózkodási hely vagy mozgás elemzésére és előrejelzésére kerül sor személyes profil létrehozása vagy felhasználása céljából. Külön nevesített kategóriája a kockázatnak, ha kiszolgáltatott személyek, különösen, ha gyermekek személyes adatainak kezelésére kerül sor, továbbá, ha az adatkezelés nagy mennyiségű személyes adat alapján történik és nagyszámú érintettre terjed ki.

Különleges adat: 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 és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok, valamint bűnügyi személyes adatok;

Módszeres: az alábbi kitételek közül egy vagy több megvalósul:
- módszer szerint zajlik;
- előre meghatározott, szervezett vagy tervszerű;
- általános adatgyűjtési terv részeként megy végbe;
- stratégia részeként történik.

Nyilvános hely: a nyilvánosság bármely tagja előtt nyitva álló bármely terület;

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;

Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;

Profilalkotás: az egyénre (vagy egyének csoportjára) vonatkozó információ gyűjtését és a személyek jellemzőinek vagy viselkedésének abból a célból történő értékelése abból acélból, hogy őket bizonyos kategóriába vagy csoportba sorolják, különösen, hogy például
- egy feladat teljesítésére vonatkozó képességüket,
- érdeklődésüket vagy
- valószínűsíthető viselkedésüket

elemezzék és/vagy azokból előrejelzéseket készítsenek;

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri;

Amennyiben a mindenkori hatályos adatvédelmi jogszabály (különösen is a GDPR és az Infotv.) fogalom meghatározásai eltérnek ezen fogalom meghatározásoktól, akkor a jogszabály által meghatározott fogalmak az irányadók.