Elnöki Hivatal Európa

IRÁNYELVEK ÉS ELJÁRÁSOK

SZAKPOLITIKA NÉV	**ADATVÉDELMI POLITIKA**				
HATÁLYOS DÁTUM	február 3, 2022	**AZ UTOLSÓ FELÜLVIZSGÁLAT DÁTUMA**	február 3, 2022	**VERSION NO.**	1
KIADTA	Az elnöki hivatal vezetője Európa, jogi ügyek COE				
SZAKPOLITIKAI ÜGYINTÉZŐ	COE szabályzat (COE) <policies.coe@motherson.com>			**DOKUMENTUM ID**	FY22-LEG-02

A KÖVETKEZŐKRE VONATKOZIK					
REGION (RCO)	COE	BUSINESS	Minden	ORSZÁG OSZTÁLY AZ RCO-N BELÜL	Minden

POLITIKAI FŐ CÉLKITŰZÉS	Az adatvédelmi politika szigorú követelményeket határoz meg az üzleti partnerekre és alkalmazottakra vonatkozó személyes adatok feldolgozására vonatkozóan. Megfelel az európai általános adatvédelmi irányelv ("GDPR") követelményeinek, és biztosítja a nemzeti és nemzetközi adatvédelmi jogszabályok elveinek való megfelelést. A szabályzat adatvédelmi és biztonsági szabványt határoz meg vállalatunk számára, és szabályozza az információk csoportunk vállalatai közötti megosztását.
BIZALMASSÁGI SZINT	Ez a dokumentum **BELSŐ HASZNÁLATRA** készült, és minden alkalmazott számára elérhetővé tehető.

TARTALOMJEGYZÉK

A COE VEZETŐJÉNEK ELŐSZAVA

Hölgyeim és Uraim!

Nemzetközi vállalatként kötelességünknek tekintjük, hogy világszerte megfeleljünk a személyes adatok gyűjtését és feldolgozását szabályozó különböző jogi szabályozásoknak. Legfőbb prioritásunk a személyes adatok kezelésére vonatkozó, általánosan alkalmazható, világméretű szabványok biztosítása. Számunkra minden egyes személy személyes jogainak és magánéletének védelme a bizalom alapja üzleti kapcsolatainkban.

Adatvédelmi szabályzatunk szigorú követelményeket határoz meg az üzleti partnerekre és alkalmazottakra vonatkozó személyes adatok feldolgozására vonatkozóan. Megfelel az európai általános adatvédelmi irányelv ("GDPR") követelményeinek, és biztosítja a világszerte hatályos nemzeti és nemzetközi adatvédelmi törvények elveinek való megfelelést.

A szabályzat globálisan alkalmazandó adatvédelmi és biztonsági szabványt határoz meg vállalatunk számára, és szabályozza az információk megosztását csoportunk vállalatai között. Több adatvédelmi alapelvet - köztük az átláthatóságot, az adattakarékosságot és az adatbiztonságot - határoztunk meg irányadónak. Vezetőink és alkalmazottaink kötelesek betartani a vállalati adatvédelmi politikát, és betartani a helyi adatvédelmi törvényeket. Szívesen válaszolunk a Motherson ("Vállalat" vagy "Csoport") adatvédelemmel kapcsolatos kérdéseire.

1. BEVEZETÉS

Ez az adatvédelmi szabályzat a Motherson által belsőleg, de a Motherson telephelyein kívül is feldolgozott információk szokásos kezelését írja le a GDPR értelmében. Az Adatvédelmi szabályzat tehát fontos hozzájárulást jelent a személyes adatok jogszerű kezeléséhez valamennyi üzleti tevékenység esetében, és a Motherson adatvédelmi irányítási rendszerének kulcsfontosságú elemét képezi, amely az adatvédelmet nemcsak jogi kötelezettségnek, hanem fontos üzleti célnak tekinti. A Mothersonnak különösen és aktívan védenie kell a személyes ügyfél- és munkavállalói adatokat, mivel az ügyfeleknek és a személyzetnek az 1.2. cikkben meghatározottak szerint bíznia kell abban, hogy a Motherson nem él vissza személyes adataikkal.

Az adatvédelem mindenekelőtt olyan vezetői felelősség, amelynek a vállalat vezetősége meg kíván felelni. Mivel az adatvédelem nem (csak) felülről lefelé írható elő, hanem minden Motherson alkalmazott által megélhető, ez az adatvédelmi szabályzat egyértelmű utasításokkal segíti a munkatársakat abban, hogy munkahelyükön figyelembe vegyék az adatvédelmi szempontokat. A munkatársak kötelesek betartani és végrehajtani ezt a politikát.

1.1. Általános adatvédelem Megjegyzések

Az adatvédelmi jog a személyes adatok kezelésére vonatkozó szabályokat tartalmaz az érintettek személyiségi jogainak védelme érdekében. A cél az "átlátható egyének" megelőzése és az érintettek személyes jogainak védelme.

A GDPR minden uniós tagállam számára előírja az adatvédelem minimális szintjét. Ez az adatvédelmi politika különösen a GDPR követelményeihez kíván hozzájárulni, hogy biztosítsa a megfelelőséget ezen a területen. Biztosítja a GDPR által előírt megfelelő szintű adatvédelmet és a határokon átnyúló adattovábbításra vonatkozó nemzeti jogszabályokat, beleértve azokat az országokat is, amelyek még nem rendelkeznek megfelelő adatvédelmi jogszabályokkal.

1.2. Terjedelem

Ez az adatvédelmi politika a személyes adatok kezelésének keretfeltételeit jelenti. A személyes adatok kezelésére vonatkozó egyéb utasítások, kötelezettségek, irányelvek és vállalati megállapodások kiegészítésnek tekintendők, kivéve, ha azok ellentétesek a jelen Szabályzattal. Ez a szabályzat vonatkozik az üzleti ügyfelek, szerződéses partnerek és kapcsolattartók adatainak, más külső irodák adatainak, valamint az alkalmazottak, gyakornokok, jelentkezők és egyéb személyek adatainak kezelésére, függetlenül a foglalkoztatás típusától.

Ez az adatvédelmi politika a csoport valamennyi vállalatára vonatkozik, és az egyes vállalatok valamennyi alkalmazottjára vonatkozik, függetlenül a foglalkoztatás típusától, beleértve a szabadúszókat, a kölcsönzött munkavállalókat, a diákokat, a gyakornokokat és az egyéb munkavállalókat ("alkalmazottak").

1.3. Adatsértés Következmények

A személyes adatok jogellenes kezelése az érintettek kártérítési követeléseit és jó hírnévvesztést is eredményezhet; az ilyen következményes károkat nehéz számszerűsíteni, de nem szabad alábecsülni. A személyes adatok gondatlan kezelése panaszokhoz is vezethet, amelyeket az egyének a felügyeleti hatóságokhoz nyújtanak be. A GDPR-nak való megfelelés elmulasztása jelentős bírságokat vonhat maga után, amelyeknek jelentős hatása van.

2. FOGALMAZÁSOK

Az adatvédelmi törvény kulcsfontosságú elemei a **személyes adatok**, amelyek magukban foglalják az egyén személyes vagy anyagi helyzetére vonatkozó bármely információt. Ennélfogva bármilyen információ személyes adatnak minősülhet, ha az bizonyos személyekhez köthető, és ez magában foglalhat triviális tényeket, valamint nyilvánvaló és nyilvánosan hozzáférhető információkat is. Az olyan statisztikák azonban, amelyek nem teszik lehetővé az egyének azonosítását, általában nem minősülnek személyes adatnak.

Személyes adat: azonosított vagy azonosítható természetes személyekre ("érintett") vonatkozó bármely információ; azonosíthatónak minősül az a természetes személy, aki közvetlenül vagy közvetve azonosítható olyan azonosítókon keresztül, mint a név, személyi azonosító szám, helymeghatározó adatok, online azonosítók és az ilyen természetes személyek fizikai, fiziológiai, genetikai, mentális, gazdasági, kulturális vagy szociális identitását jellemző egy vagy több jellemző.

A személyes adatok a következők lehetnek:

- név, életkor, családi állapot, születési dátum, foglalkozás, cím, telefonszám, e-mail cím;
- fizetési információk, preferált fizetési típusok, számlaszámok/hitelkártyaszámok, hitelképességi információk, fizetési előzmények vagy kötelezettségek;
- azonosítók (ügyfél/személyzeti számok);
- biometrikus (magasság) és egészségügyi (meglévő betegségek) adatok;
- rokonok és társadalmi kapcsolatok;
- ügyféljellemzők (meglévő szerződések, szerződéses előzmények);
- fogyasztás (fogyasztási adatok, közlekedési eszközök, szemetesek tartalma);
- böngészési szokások (böngészési információk, böngészési előzmények);

- videofelvételek és fényképek.

Az egyénekre vonatkozó egyes információk különösen érzékenynek minősülnek. A **személyes adatok** e **különleges** kategóriájába tartoznak a faji vagy etnikai származásra, politikai véleményre, vallási/ideológiai meggyőződésre, szakszervezeti tagságra, genetikai adatokra, természetes személyek azonosítására szolgáló biometrikus adatokra, egészségügyi adatokra és szexuális életre/orientációra vonatkozó adatok. Amint az egyénekre vonatkozó információk ezekre a részterületekre vonatkoznak, különös figyelmet kell fordítani.

Az adatfeldolgozás magában foglalja az adatkezeléssel kapcsolatos valamennyi lépést, beleértve, de nem kizárólagosan, az adatgyűjtést, rögzítést, rendszerezést, strukturálást, tárolást, kiigazítást vagy módosítást, visszakeresést, betekintést, felhasználást, továbbítás, terjesztés vagy más módon történő hozzáférhetővé tétel, összehangolás vagy kombinálás, korlátozás, törlés vagy megsemmisítés, továbbítás, továbbítás, továbbítás, módosítás, kombinálás, elemzés és törlés, valamint bármely más típusú felhasználást.

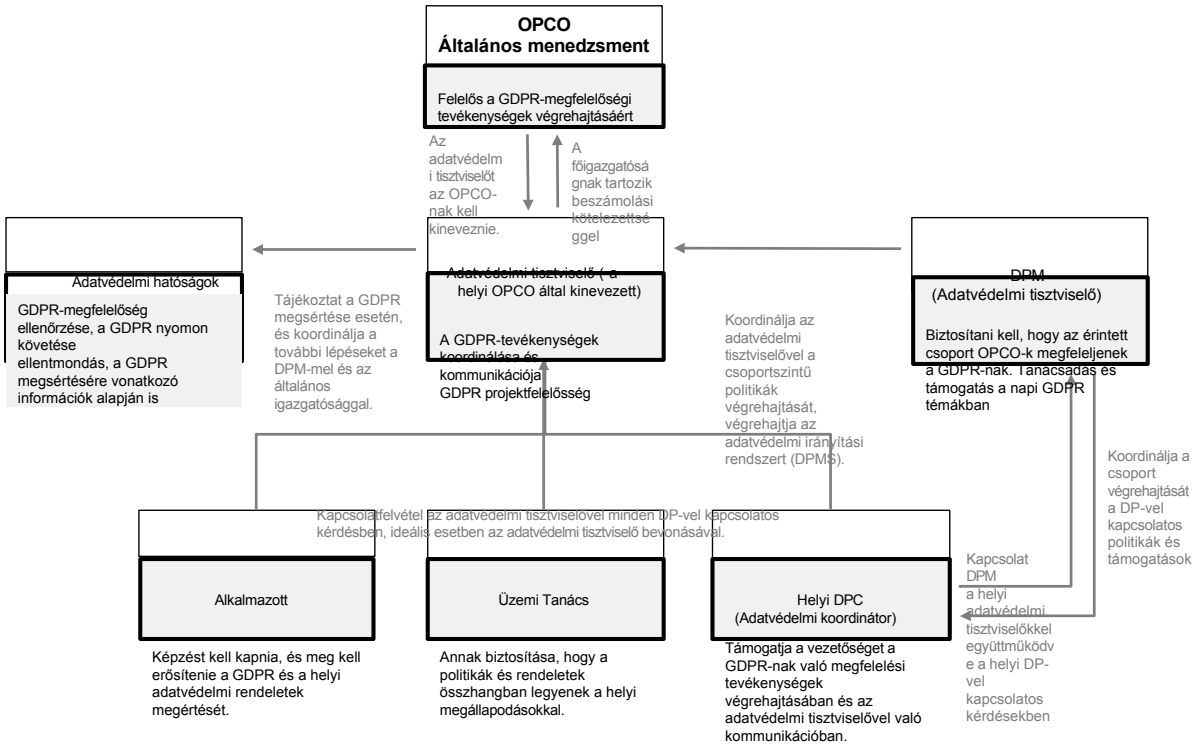
Az adatvédelmi jog értelmében az **érintettek** olyan személyek, akik a személyes adatok alapján azonosíthatók, azaz az adatkezelési tevékenységek által érintett személyek. Az adatvédelmi jog értelmében minden érintettet megilletnek bizonyos elidegeníthetetlen jogok.

Az **adatkezelő az** érintettek megfelelője. Az adatkezelő bármely természetes vagy jogi személy, hatóság, létesítmény vagy egyéb szerv, amely egyedül vagy közösen dönt a személyes adatok feldolgozásának céljairól és eszközeiről. Adatkezelőnek nevezzük az adatkezelési tevékenységeket irányító vállalatokat vagy más szerveket, azaz azokat, akik meghatározzák az adatkezelés céljait és az érintettek adatainak feldolgozásának módját. Az adatkezelési tevékenységek kiszervezhetők más irodákhoz is (például a Motherson csoporthoz tartozó vállalatokhoz vagy külső szolgáltatókhoz), de az ügyfél továbbra is az adatkezelő marad. Ezekben az esetekben különösen fontos megvizsgálni, hogy ki az adatkezelő az adott adatkezelés tekintetében. Az adatkezelő egyértelmű azonosítása azért fontos, mert az érintetteknek egyértelmű, egyetlen kapcsolattartóval kell rendelkezniük.

Azonosítható természetes személy: olyan személy, aki közvetlenül vagy közvetve azonosítható, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy az adott természetes személy fizikai, fiziológiai, genetikai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző egy vagy több tényező alapján.

Névtelen és álnévtelen adatok: A személyes adatok ellentéte az "anonim adatok", amelyeket nem lehet konkrét személyekhez rendelni. A munkanélküliségi adatok vagy a tömegközlekedés átlagos használatára vonatkozó statisztikák nem teszik lehetővé az egyénekre vonatkozó megállapításokat, vagyis anonim adatokról van szó. Mivel az anonim adatok nem kapcsolódnak egyénekhez, nem tartoznak az adatvédelmi törvény hatálya alá; azonban különleges titoktartás alá eshetnek, ha vállalati adatokról van szó (például üzleti adatok, belső statisztikák). Első pillantásra az "álneves adatok" hasonlóak az anonim adatokhoz; az álneveket "álneveknek" is nevezhetjük. Az anonim adatokkal ellentétben azonban az álnevek esetében továbbra is lehetséges a személyekhez való hozzárendelés. A hozzárendelés egyszerűen egy további lépést foglal magában, például az ügyféladatbázisokkal vagy a személyzeti nyilvántartásokkal való összehasonlítást vagy keresést. Az álneves adatok tehát az adatvédelmi törvény hatálya alá tartozó személyes adatok.

3. SZEREPEK ÉS FELELŐSSÉGI KÖRÖK



Az OPCO (Operatív Vállalat) vezérigazgatósága és a részlegek szintjén a vállalatvezetés által kinevezett tisztviselők felelősek az adatvédelmi koncepció végrehajtásáért a mindennapi üzleti műveletekben. Az adatvédelem azonban a Motherson valamennyi munkatársára vonatkozik, ami azt jelenti, hogy nekik kell védeniük a személyes adatokat.

3.1. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselőt a GDPR 37. cikkében foglalt feltételek szerint kell kinevezni.

A tisztviselő a törvény és a jelen adatvédelmi politika által ráruházott feladatát szakértelme alkalmazásával, korlátozások nélkül látja el. E célból az érintett szervezeti egységek biztosítják a szükséges információkat, dokumentumokat stb., és ez vonatkozik a megkeresésekre, panaszokra és információszolgáltatási kérelmekre is. Felhívjuk figyelmét, hogy az adatvédelmi tisztviselő nem helyettesíti a helyi adatvédelmi tisztviselőt, akit minden egységnek külön-külön kell bejelentenie. Ennek vagy belső személynek, vagy külső szolgáltatónak kell lennie, és az adatvédelmi hatóságoknak nyilvántartásba kell venniük, amikor a törvény előírja.

Minden Motherson alkalmazott az adatvédelmi tisztviselőhöz fordulhat bármilyen kérdéssel, észrevétellel, javaslattal vagy panasszal, amelyet kérésre titokként kezelnek.

Az adatvédelmi tisztviselő feladatait a GDPR 39. cikke a következőképpen határozza meg:

- a vezetőség és a munkavállalók tájékoztatása és tanácsadás a GDPR-nek és más adatvédelmi jogszabályoknak való megfeleléssel kapcsolatos kötelezettségekről;

- a GDPR-nek és más adatvédelmi jogszabályoknak, valamint az adatvédelmi politikáknak való megfelelés ellenőrzése, beleértve a belső adatvédelmi tevékenységek irányítását;
- az adatvédelmi kérdések tudatosítása, a személyzet képzése és belső ellenőrzések elvégzése;
- az adatvédelmi hatásvizsgálatokkal kapcsolatos tanácsadás és azok nyomon követése;
- együttműködni a felügyeleti hatósággal;
- és a felügyeleti hatóságok első számú kapcsolattartója;
- az összes adatvédelmi eljárás és politika rendszeres felülvizsgálata és jóváhagyása;
- az eljárásoknak, a politikáknak és az alkalmazandó adatvédelmi és magánélet védelmére vonatkozó jogszabályoknak való megfelelés ellenőrzése;
- a személyzet, az igazgatótanács tagjai és más érdekelt felek adatvédelmi kérdéseire való válaszadás;
- válaszadás olyan magánszemélyeknek, például ügyfeleknek és alkalmazottaknak, akik tudni szeretnék, hogy milyen adatokat tárolnak róluk, valamint a vállalat adatait kezelő harmadik felekkel az adatfeldolgozásra vonatkozó szerződések vagy megállapodások ellenőrzése és jóváhagyása;
- az adatvédelmi hatásvizsgálatok felügyelete és felülvizsgálata;

3.2. ADATVÉDELEM MENEDZSER

Az adatvédelmi tisztviselőt (DPM) a COE jelöli ki. Feladata, hogy támogassa az összes szervezeti egységet a GDPR-szabályok megfelelő végrehajtásában, és általános kérdésekben a megfelelő partner legyen. Kidolgozza az adatvédelmi szabályokat és biztosítja a szükséges sablonokat, de rendelkezésre áll az adatvédelmi ellenőrzésekkel kapcsolatos kérdések és támogatási igények esetén is, illetve az adatvédelemmel kapcsolatos bármilyen eszkalációs szinten. Ezenkívül támogatja a csoport adatvédelmi tisztviselői közötti kommunikációt és szinergiák kialakítását. Az adatvédelmi tisztviselő aktívan támogatja az adatvédelmi tisztviselőket feladataik és kötelezettségeik teljesítésében.

3.3. ADATVÉDELMI ORSZÁGKOORDINÁTOR (CC) / ADATVÉDELMI VEZETŐK (DPL)

A CC-k vagy DPL-k az adatvédelmi kérdésekkel foglalkozó kapcsolattartók telephelyenként/országonként. Ők végezhetnek ellenőrzéseket, és meg kell ismertetniük az alkalmazottakkal az adatvédelmi irányelvek tartalmát. Az illetékes vezetésnek segítenie kell a CC/ DPL erőfeszítéseit. Az üzleti folyamatokért és projektekért felelős részlegeknek időben tájékoztatniuk kell az adatvédelmi koordinátorokat a személyes adatok új feldolgozásáról.

Új feldolgozás

A CC/ DPL-nek értékelnie kell a földrajzi területén végrehajtott minden új feldolgozás GDPR-megfelelőségét (függetlenül attól, hogy ez a feldolgozás az ő osztályán történik-e vagy sem).

A CC/ DPL összegyűjti a feldolgozáshoz szükséges összes adatot, amelyet a feldolgozási tevékenységek nyilvántartásában kell létrehozni. A KK/ DPL létrehozza az új feldolgozást a feldolgozási tevékenységek nyilvántartásában.

Meglévő feldolgozás

A CC/ DPL felelős a meglévő feldolgozási tevékenységek nyilvántartásának frissítéséért (függetlenül attól, hogy ez a

feldolgozás az ő osztályán történik-e vagy sem).

IT-biztonság

A CC/ DPL felelős a nem központi szinten végzett feldolgozás informatikai biztonságáért. Szükség esetén a CC/ DPL-nek konzultálnia kell a CISO-val, aki segít az értékelés elvégzésében.

Auditálás

Az ellenőrzések során a CC/ DPL a megfelelőségi ellenőr tárgyalópartnere.

GDPR hálózat

A CC/ DPL integrálja a GDPR-hálózatot az adatvédelmi tisztviselővel és a többi CC/ DPL-rel.

4. ADATVÉDELMI TÖRVÉNY ALAPVETŐ FELTÉTELEK

A Mothersonra az alábbi adatvédelmi jogi alapfeltételek vonatkoznak:

4.1. JOGSZERŰSÉG; CÉL KORLÁTOZÁS

Az adatfeldolgozásra a GDPR rendelkezései szerinti, felhatalmazás fenntartásával történő úgynevezett tilalom vonatkozik. Ez azt jelenti, hogy a személyes adatok feldolgozása általánosságban tilos, kivéve, ha azt kifejezetten engedélyezték.

A GDPR 6. cikke és a hasonló ágazati szabályok szerint a személyes adatok feldolgozása csak akkor megengedett, ha:

- az érintettek hozzájárultak személyes adataiknak egy vagy több meghatározott célból történő kezeléséhez;
- az adatkezelés olyan szerződések teljesítéséhez szükséges, amelyekben az érintettek szerződő felek, vagy az érintettek kérésére szerződéskötést megelőző intézkedések végrehajtásához;
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettségek teljesítéséhez szükséges;
- az adatkezelésre az érintettek vagy más személyek létfontosságú érdekeinek védelme érdekében van szükség;
- az adatkezelésre az adatkezelő vagy harmadik felek jogos érdekeinek védelme érdekében van szükség, kivéve, ha a személyes adatok védelmét kérő érintettek érdekei, alapvető jogai vagy szabadságai elsőbbséget élveznek, különösen, ha az érintettek gyermekek.

A személyes adatok feldolgozása során a Motherson garantálja, hogy a feldolgozáshoz szükséges engedélyezési elemek rendelkezésre állnak. Az adatfeldolgozás alapulhat egyedi törvényeken és nemzeti jogszabályokon is.

Az olyan adatok feldolgozása esetén, amelyekre nincs jogi felhatalmazás, a Motherson gondoskodik arról, hogy az érintettektől jogi felhatalmazást szerezzen be. A kizárólag automatizált feldolgozáson alapuló döntésekre vonatkozó jogi követelményeket - beleértve a profilalkotást is -, amelyek jogi vagy hasonló hatásokkal járnak az érintettekre nézve, betartják.

4.1.1. AZ ÉRINTETTEK HOZZÁJÁRULÁSA

A törvényes adatkezelési felhatalmazás mellett az érintettek hozzájárulása a GDPR 6. cikkének 1a. pontja értelmében az adatok jogszerű feldolgozásának lehetőségét jelenti. Mind a GDPR, mind a bírósági ítéletek szigorú (a GDPR 7. cikkében szabályozott) követelményeket írnak elő az ilyen hozzájáruló nyilatkozatokra vonatkozóan, kimondva, hogy az érintetteknek önkéntes és tájékozott alapon kell megadniuk hozzájárulásukat.

4.2. ELŐIRÁNYÍTÁS

Az adatfeldolgozás célja azon a vonatkozó szakfeladaton alapul, amelynek elvégzése érdekében az adatokat gyűjtötték. Ezeknek a céloknak egyértelműnek és jogszerűnek kell lenniük, és az adatgyűjtés időpontjában fel kell tüntetni őket. Az adatvédelmi jogszabályok előírják, hogy a személyes adatok általában csak arra a célra dolgozhatók fel, amelyre eredetileg gyűjtötték őket. Az adatfeldolgozási tevékenységeknek meghatározott céljai vannak, és a Motherson általában nem rendelkezik olyan személyes adatokkal, amelyek "szabadon" felhasználhatók meghatározatlan célra; ha az adatokra már nincs szükség az eredeti céljukhoz, azokat törölni kell, kivéve, ha a törvény előírja, hogy archiválni kell őket.

Az eredeti céltól eltérő célú adatkezelés a GDPR 6. cikkének 4. pontja értelmében célváltoztatásnak vagy kivételnek minősül, és csak a GDPR 6. cikkének 4. pontjában foglalt követelmények szerint lehetséges. Ez vonatkozik arra az esetre is, ha az adatokat a kisegítő funkciókat meghaladó feladatokat ellátó más hivatalok részére kell továbbítani.

A Motherson biztosítja, hogy a személyes adatok feldolgozása csak arra a célra történik, amelyre azokat gyűjtötték, hogy a törvényes felhatalmazások megvannak, és hogy a GDPR 6. cikkének 4. pontja szerinti követelmények teljesülnek, ha a célt meg kívánják változtatni.

4.3. PONTOSSÁG

A Motherson garantálja, hogy a csoport által tárolt adatok helyesek, és hogy szükség esetén frissítésre kerülnek.

4.4. ADATOK MINIMALIZÁLÁSA

A személyes adatok tárolása nem hosszabb ideig történik, mint amennyi a személyes adatok feldolgozásának céljaihoz szükséges, kivéve, ha jogszabály hosszabb tárolási időt ír elő. A Motherson ezt minden folyamatánál figyelembe veszi, beleértve a személyes adatok feldolgozását is.

4.5. TRANSPARENCIA

Az érintetteknek mindig jogukban áll rendelkezni saját személyes adataikkal, meg kell tudniuk érteni, hogy ki tárolja és kezeli mely személyes adatokat milyen célból, és legkésőbb a gyűjtéskor tájékoztatni kell őket az adatkezelés céljairól. Ezért az adatokat soha nem lehet titokban feldolgozni anélkül, hogy az érintettek erről ne tudnának. Az átláthatóság biztosítása érdekében fontos az adatfeldolgozás lépéseinek alapos ismertetése, valamint az esetleges kérdések komoly, teljes és őszinte megválaszolása. A GDPR 13. cikke például kimondja, hogy az érintetteket különösen tájékoztatni kell az adatvédelmi tisztviselő elérhetőségéről, a célról (az adatkezelés minden egyes esetére vonatkozóan), az adatkezelés időtartamáról, a tájékoztatáshoz és a tiltakozáshoz való jogról, az adatkezelés jogalapjáról és az érdekek érthető mérlegeléséről. Általánosságban az érintetteket tájékoztatni kell minden jogról, azaz a hozzáféréshez, a helyesbítéshez, a törléshez, az adatkezelés korlátozásához, a tiltakozáshoz való jogról.

és az adatok hordozhatósága. Az érintetteket arról is tájékoztatni kell, hogy a döntéshozatal kizárólag automatizált adatfeldolgozáson (ideértve a profilalkotást is) alapul.

Ebben a tekintetben figyelembe kell venni, hogy az információkat az érintetteknek az adatgyűjtést követően azonnal meg kell küldeni. A GDPR 12. cikke előírja, hogy ezt a tájékoztatást "átlátható, érthető és könnyen hozzáférhető formában, világos és közérthető nyelven" kell megadni az érintetteknek, és ehhez elegendő a szóbeli, írásbeli és elektronikus információátadás. A kifejezetten a gyermeknek címzett információknak különösen egyértelműnek kell lenniük. Csak akkor nem áll fenn tájékoztatási kötelezettség, ha az érintettek már rendelkeznek a szükséges információkkal az adatfeldolgozási ügyekben; a Motherson köteles erre vonatkozóan bizonyítékot szolgáltatni.

4.6. ADATVÉDELMI HATÁSVIZSGÁLAT

A GDPR 35. cikke előírja az adatvédelmi hatásvizsgálatok, azaz kockázatértékelések elvégzését, amelyeket a Motherson köteles elvégezni a személyes adatok feldolgozása előtt. Általában csak akkor kell ilyen adatvédelmi kockázatértékelést végezni, ha az érintettek jogaira és szabadságaira nézve magas kockázat áll fenn, mint például az alábbi esetekben:

- értékelési, pontozási vagy profilalkotási célú adatok, különösen a munkára, gazdasági helyzetre, egészségi állapotra, személyes preferenciákra/érdeklődésre, hitelképességre, szokásokra, tartózkodási helyre vonatkozó adatok;
- jogi következményekkel járó automatizált döntéshozatal;
- érzékeny adatok, például egészségügyi adatok feldolgozása;
- átfogó feldolgozási eljárások;
- összekapcsolt vagy kombinált adathalmazok;
- a védelemre szoruló személyek, például gyermekek, idősek, betegek vagy a személyzet adatai;
- az új technológiák használata.

Amennyiben a GDPR 35. cikke értelmében adatvédelmi hatásvizsgálatra van szükség, az adatvédelmi tisztviselőt és szükség esetén az adatvédelmi tisztviselőt is be kell vonni, ezért a Motherson munkatársainak haladéktalanul tájékoztatniuk kell az adatvédelmi tisztviselőt az új személyesadat-kezelő rendszerek bevezetéséről, hogy az ellenőrizhesse azok adatvédelmi jogi elfogadhatóságát.

Figyelem: a GDPR 36. cikke szerinti konzultációs kötelezettséget figyelembe kell venni a kockázatos adatfeldolgozás esetén. Ezért az adatvédelmi tisztviselőnek és/vagy a vállalatvezetésnek kapcsolatba kell lépnie a felügyeleti hatósággal, ha az adatvédelmi hatásvizsgálat azt mutatja, hogy az adatkezelés az adatvédelmi jog szempontjából magas kockázattal jár.

5. JELENTÉSI KÖTELEZETTSÉG A GDPR SZERINT

A Motherson számára a személyes adatok védelme rendkívül fontos. Ha azonban mégis előfordulnak adatvédelmi incidensek, a Motherson tisztában van bejelentési kötelezettségével, amelyet indokolatlan késedelem nélkül teljesít. Ilyen jogsértés akkor következik be, ha az adatbiztonság megsértése (szándékolatlanul vagy jogellenesen) a továbbított, tárolt vagy más módon feldolgozott személyes adatok megsemmisítéséhez, elvesztéséhez, módosításához vagy jogosulatlan nyilvánosságra hozatalához/hozzáféréshez vezet.

Az általános adatvédelmi rendelet 33. és 34. cikke meghatározza, hogyan kell eljárni adatvédelmi incidensek esetén: a felügyeleti hatóságot mindig tájékoztatni kell; kivétel csak akkor áll fenn, ha az adatvédelmi incidensek valószínűleg nem járnak kockázattal az érintettek számára. Ezért a Motherson munkatársainak haladéktalanul tájékoztatniuk kell az adatvédelmi tisztviselőt az adatvédelmi incidensekről, hogy az értékelni tudja az érintetteket érintő, az adatvédelmi incidensből eredő kockázatot. Az érintetteket csak akkor kell tájékoztatni, ha jogaikra és szabadságaikra nézve magas kockázat áll fenn.

Mivel az adatvédelmi incidenseket 72 órán belül jelenteni kell az illetékes felügyeleti hatóságoknak, a személyzetnek nem szabad késlekednie, hogy gyorsan tájékoztassa az adatvédelmi tisztviselőt az adatvédelmi incidensekről.

6. ADATTOVÁBBÍTÁS HARMADIK FÉLNEK

Az egyéb szervek, például külső szolgáltatók, hatóságok, a rendőrség vagy az ügyészség részére történő adattovábbítás szintén adatvédelmi jogi szempontból releváns folyamat, amely minden egyes esetben tényszerű indokolást igényel. Ezért minden adattovábbítást alaposan meg kell vizsgálni, és a felügyelőnek vagy az adatvédelmi tisztviselőnek jóvá kell hagynia.

6.1. CSOPORTON BELÜLI ÁTVITEL

A Motherson csoport más vállalatai felé történő adattovábbítást is meg kell vizsgálni, mivel az adatokat nem lehet egyszerűen a csoport vállalatai között továbbítani, összevonni, összehasonlítani vagy más módon hozzáférhetővé tenni; nincs átfogó csoportos előjog. A Mothersonon belüli adattovábbításokat is meg kell indokolni az érdekek mérlegelésével összefüggésben.

Mivel csak azok a részlegek férhetnek hozzá ezekhez az adatokhoz, amelyeknek tevékenységükhöz szükségük van az adatokra, a csoport más vállalatai számára történő továbbítás csak akkor megengedett, ha az egyes esetekben jogalap áll fenn. A vállalatoknak ellenőrizniük kell az egyes eljárások jogi elfogadhatóságát, és figyelembe kell venniük az érintettek érdekeit.

A Motherson vállalatok közötti adattovábbítást adatvédelmi szerződésekkel kell kiegészíteni (ha szükséges) a jogilag megengedett feldolgozás garantálása érdekében.

6.2. KÜLSŐ SZOLGÁLTATÓK ÉS ADATFELDOLGOZÁS A MOTHERSON NEVÉBEN

Ha külső szolgáltatókat vesznek igénybe, akiknek a Motherson személyes adatokat továbbít, vagy akiknek jogot biztosítanak a tárolt adatokhoz való hozzáférésre, az érintett részlegek vezetőinek biztosítaniuk kell, hogy az

adatvédelmi tisztviselőt tájékoztassák, és szükség esetén "adatkezelő-adatfeldolgozói megállapodást" kössenek.

Ezenfelül figyelembe kell venni az "nem biztonságos" harmadik országokba, azaz az Európai Unión kívüli országokba történő adatfeldolgozás vagy adattovábbítás sajátos szempontjait, és szükség esetén kiegészítő szerződéseket kell kötni.

Ha külső szolgáltatókat vesznek igénybe, akik a Motherson nevében személyes adatokat dolgoznak fel ("adatfeldolgozók"), írásos szerződést kell kötni. Az adatfeldolgozókat körültekintően kell kiválasztani, figyelembe véve a technikai és

szervezési intézkedések, és csak megadott utasítások alapján dolgozhatnak fel adatokat. Az ilyen szerződések tartalmára vonatkozó, a GDPR 28. cikke szerinti követelményeket figyelembe kell venni, és ennek biztosítása érdekében az adatvédelmi tisztviselőt tájékoztatni kell az ilyen "adatkezelő és adatfeldolgozó közötti megállapodás" megkötésének szándékáról.

7. TITOKTARTÁSI ÉS ADATVÉDELMI MEGFELELÉS KÖTELEZETTSÉG

A Motherson munkatársait munkaszerződésük aláírásakor tájékoztatni kell a titoktartási és adatvédelmi kötelezettségükről, és alá kell írniuk egy erre vonatkozó nyilatkozatot, amelyet a személyi aktákhoz csatolnak. Ezen túlmenően a Motherson rendszeresen tart adatvédelmi képzéseket.

8. ADATOK TÍPUSOK

8.1. PÁLYÁZÓ ADATOK

Az érintett személyek csoportjába tartoznak a pályázók és az üres álláshelyek iránt érdeklődők.

Ezek az adatok a pályázók személyes és ténybeli helyzetére vonatkozó, a pályázati eljárás során megadott egyedi információkra vonatkoznak, azaz például:

- név;
- cím;
- születési dátum;
- fotó;
- a szülők neve/születési ideje/szakmája/vallási vagy politikai meggyőződése (nem kötelező, de gyakran önkéntesen megadják);
- oktatás: végső jegyek és oktatási intézmények;
- korábbi munkáltatók, referenciák és ajánlások;
- a jelenlegi felmondási idő, a kívánt fizetések és a rendelkezésre állás;
- harmadik országból származó kérelmezők esetében: az érvényes tartózkodási/munkavállalási engedélyek típusa és időtartama;
- útlevélmásolatok.

Az adatokat pályázatkezelési célokra használják fel, és a törvényes határidőknek megfelelően törlik őket.

8.2. MUNKAVÁLLALÓ ADATOK

Az adatok a személyzet személyes és ténybeli helyzetére vonatkozó egyedi információkra vonatkoznak, azaz például:

- nevek és születési nevek;
- címek (hivatalos címek);
- születési dátum;

- számlaadatok;

- adószám, adóosztály, felekezeti hovatartozás, családi állapot, állampolgárság;
- iskolai végzettség;
- egészségügyi és társadalombiztosítási adatok;
- munkaszint/fizetés;
- mobiltelefonszám/helyhez kötött telefonszám; privát e-mail cím (önkéntes), vészhelyzeti kapcsolattartók (név és telefonszám (önkéntes));
- különleges esetekben: útlevélmásolat (tartózkodási engedély a harmadik országbeli alkalmazottak esetében);
- a tevékenységgel kapcsolatos munkavállalói adatok, pl. bérszámfejtési adatok, költségszámlák, szabadságok és betegszabadságok, munkaidő-nyilvántartás, figyelmeztetések, értékelések.

Ezeket az adatokat a munkaszerződések feldolgozásához és a személyzet adóhivataloknál, egészség- és nyugdíjbiztosítóknál történő nyilvántartásához használják fel.

8.3. SZÁMVITELI ADATOK

Az érintett személyek csoportjába tartoznak a számviteli és pénzügyi alkalmazottak, a beszállítók és a vevők.

Az adatok a személyzet, a beszállítók és az ügyfelek személyes és ténybeli helyzetére vonatkozó egyedi információkra vonatkoznak, azaz például:

Számviteli és pénzügyi személyzet

- kapcsolattartó partnerek neve;
- kapcsolattartó partnerek címei;
- számlainformációk, beleértve az adószámokat és a számlaadatokat.

Szállítók

- kapcsolattartó partnerek neve;
- cím;
- számlainformációk, beleértve az adószámokat és a számlaadatokat.

Az adatokat számviteli célokra használják fel.

8.4. HASZNÁLAT ADATOK

Az érintett személyek csoportjába tartoznak a Motherson weboldalának felhasználói a www.motherson.com címen.

Az adatok a felhasználók személyes és ténybeli helyzetére vonatkozó egyedi információkra vonatkoznak, azaz például:

- az IP-címet a hozzáférő számítógépektől;
- hozzáférés dátuma és időpontja;
- a letöltött fájl neve és URL címe;
- adatátviteli mennyiség;

- sikeres lekérdezésről szóló értesítés;
- böngésző és operációs rendszer felismerési adatok.

Ezeket az adatokat a Motherson weboldal használatának lehetővé tételére, valamint reklámozásra, piackutatásra és a Motherson vállalat weboldalának megfelelő strukturálására használják fel.

8.5. ÜGYFÉL ADATOK

Az érintett személyek csoportjába tartoznak a Motherson ügyfelei. A Motherson elsősorban a B2B szektorban tevékenykedik, így a személyes adatok ebben az összefüggésben csak kis mértékben érintettek, például a kapcsolattartó partnerek nevei és e-mail címei formájában:

- kapcsolattartó partnerek neve;
- (e-mail) címek;
- kommunikációs tartalmak.

9. AZ ÉRINTETTEK JOGAINAK VÉDELME

Az érintetteknek joguk van a hozzáféréshez, a helyesbítéshez, a törléshez, az adatkezelés korlátozásához, a tiltakozáshoz és az adathordozhatósághoz. A Motherson biztosítja, hogy az indokolt kérelmekhez szükséges adatokat egy hónapon belül gyorsan és teljes körűen rendelkezésre bocsátja.

9.1. ACCESS

A GDPR 15. cikke értelmében az érintettek jogosultak arra, hogy az adatkezelőtől tájékoztatást kapjanak például arról, hogy milyen személyes adataikat milyen célból tárolják, kinek továbbítják az adatokat, és honnan származnak.

Ehhez rendkívül fontos az érintettek biztonságos azonosítása, mivel az ügyfelek/személyzet számára más ügyfelekről/személyzetről szóló információk átadása súlyos adatvédelmi incidenst jelentene. A teljes és valós adatokat térítésmentesen kell megadni.

9.2. TÁJÉKOZTATÁS

A GDPR 16. cikke értelmében az érintettek kérhetik személyes adataik azonnali helyesbítését, és a Motherson kérésre haladéktalanul helyesbíti a helytelen adatokat.

9.3. FELDOLGOZÁS KORLÁTOZÁSOK

A GDPR 18. cikke szerint az adatkezelést korlátozni kell, ha az érintettek vitatják az adatok helyességét, arra az időtartamra, amely lehetővé teszi a Motherson számára a személyes adatok pontosságának ellenőrzését, ha az adatkezelés jogellenes, de az érintettek tiltakoznak az adatok törlése ellen, ha az érintetteknek továbbra is szükségük van az adatokra jogi igények érvényesítéséhez, vagy ha az érintettek tiltakoztak a személyes adatok kezelése ellen.

feldolgozását, és az ezzel kapcsolatos határozat még mindig függőben van. A Motherson azonban akkor is korlátozza a feldolgozást, ha a tárolás megengedett, a feldolgozás azonban nem.

9.4. ERASURE

A GDPR 17. cikke értelmében az érintettek kérhetik az adatkezelőtől a személyes adatok azonnali törlését, amely szerint az adatkezelőnek haladéktalanul törölnie kell a személyes adatokat, ha az alábbi négy ok egyike fennáll:

- az adattárolás már nem szükséges az adatgyűjtési cél eléréséhez;
- az érintett visszavonja az adatkezeléshez adott hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az adatokat jogellenesen dolgozták fel;
- az adatokat a Mothersonnak a törvényes törlési kötelezettségek miatt törölnie kell.
- A Motherson nem gyakorolja a törléshez való jogot, ha:
- a vélemény- és információszabadság érvényesül;
- az adattárolás megfelel a jogi kötelezettségeknek;
- az egészségügy területén a közérdek érvényesül;
- tudományos vagy történelmi kutatási célokat szolgálnak;
- az adatokra a jogi igények védelme érdekében van szükség.

9.5. ADATOK HORDOZHATÓSÁG

Az adathordozhatóságot a GDPR 20. cikkének 1. pontja szabályozza; ez egyrészt magában foglalja az egyes adatkészletek rendelkezésre bocsátásának kéréséhez való jogot, valamint az érintettnek vagy más adatkezelőknek való továbbításhoz való jogot. A Motherson strukturált, szabványos és géppel olvasható formátumban bocsátja az érintettek rendelkezésére a vonatkozó adatkészletet. Ha az érintettek ezt az adatkészletet más adatkezelőknek kívánják továbbítani, a Motherson nem akadályozhatja vagy akadályozhatja meg ezt a folyamatot.

9.6. TEKINTET

Az érintettek bármikor tiltakozhatnak a személyes adatok feldolgozása ellen a GDPR 6. cikkének 1. e vagy f pontja alapján. Ha az adatokat a fenti követelmények bármelyike alapján jogszerűen gyűjtötték, az érintettek bármikor tiltakozhatnak az ilyen adatok feldolgozása ellen, még akkor is, ha az adatgyűjtés jogszerű volt. A Motherson tiszteletben tartja az ilyen tiltakozást, és megszünteti az adatkezelést, ha a tiltakozáshoz való jog az érintettek "különleges helyzetéből" ered, amelynek során a Motherson nem csak a különleges helyzetet, hanem a "túlsúlyt" is bizonyítani köteles.

A GDPR 21. cikkének 2. pontja biztosítja a nem fizetett tiltakozáshoz való jogot, amely bármikor gyakorolható, ha az érintettek személyes adatainak feldolgozása közvetlen reklámtevékenységgel kapcsolatos. A Motherson tiszteletben tartja az ilyen tiltakozást, és megszünteti az adatkezelési tevékenységeket.

10. A FELDOLGOZÁSI TEVÉKENYSÉGEK NYILVÁNTARTÁSA / DOKUMENTÁLÁSA FELADATOK

Az általános adatvédelmi rendelet az Art. 30. cikke szerint írásos dokumentációt és áttekintést a személyes adatok feldolgozására vonatkozó eljárásokról. Az adatkezelési tevékenységek nyilvántartásának tartalmaznia kell az adatkezelésre vonatkozó lényeges információkat, beleértve az adatkategóriákat, az érintettek csoportját, az adatkezelés célját és az adatátvevőket. Ezeket kérésre teljes körűen a hatóságok rendelkezésére kell bocsátani.

Az adatfeldolgozási tevékenységekhez az alábbi információk áttekintését kell megadni:

- (cég) az adatkezelő(k) neve;
- adatvédelmi tisztviselők;
- az adatkezelő címe;
- az adatfeldolgozás jogalapja;
- az érintett személycsoportok és a kapcsolódó adatok (kategóriák) leírása;
- az adatok címzettjei (kategóriák);
- rendszeres adattörlési időszakok;
- tervezett adattovábbítás harmadik országokba;
- általános leírás, amely lehetővé teszi a feldolgozás biztonságát garantáló intézkedések megfelelőségének előzetes értékelését;
- adatgyűjtési cél;
- tartalom;
- a feldolgozás típusaira és a védelmi intézkedésekre vonatkozó információk.

A csoport minden egyes vállalatának dokumentálnia kell a személyes adatok feldolgozásának eljárásait a feldolgozási tevékenységek nyilvántartásában. A Motherson által a dokumentációra vonatkozóan megállapított rendelkezéseket (például szoftvereszközök és dokumentációs utasítások) be kell tartani. A Motherson már létrehozott egy formanyomtatványok és dokumentumok keretét, valamint egy Microsoft SharePoint alapú informatikai megoldást, amelyet használni lehet.

11. TECHNIKAI ÉS SZERVEZETI ADATVÉDELMI INTÉZKEDÉSEK

A Mothersonnak bizonyítania kell, hogy a személyes adatok feldolgozása olyan módon történik, amely ésszerű adatbiztonsági szintet biztosít. Ezt technikai és szervezési intézkedések végrehajtásával teszi.

Az Art. A GDPR 32. cikke szerint olyan technikai és szervezési intézkedéseket kell hozni, amelyek többek között a védendő személyes adatok (kategóriák) típusától függően megfelelő védelmi szintet biztosítanak.

Art. 32. cikke a különböző technikai és szervezési intézkedések nem teljes körű felsorolását tartalmazza, amely a célkitűzésekhez hasonló konkrét és absztrakt intézkedések minimális intézkedéskatalógusát jelenti. Mivel ezek minimumkövetelmények, az egyedi esetektől függnek, de nem mindig szükségesek. Ez a katalógus a következőket tartalmazza

- személyes adatok álnevesítése és titkosítása: Az álnévtelenítés elvileg csak "további adatok", például azonosító kulcsok "bevonásával" teszi lehetővé az egyének azonosítását. A titkosítás esetében az egyének azonosítása továbbra is lehetséges, de az adatokat úgy változtatják meg, hogy azok nem olvashatók, ha nem dekódolják őket;
- a rendszer és a szolgáltatások bizalmassága, integritása, rendelkezésre állása és rugalmassága: Ez a harmadik felek hozzáférésének megakadályozását hivatott szolgálni, de technikai szempontokat is magában foglal, például a feldolgozórendszer túlterhelésének megelőzését. A vonatkozó intézkedések a tervezett védelmi céltól függenek, és a bizalmas kezelés a hozzáférés ellenőrzésével biztosítható.
- a személyes adatok elérhetőségének és hozzáférhetőségének gyors helyreállítása fizikai vagy technikai zavarok után: Ez a kérdés az adatállományok többszöri biztonsági mentése mellett elsősorban olyan technikai és szervezési intézkedésekre vonatkozik, amelyekkel a személyzeti hiányra reprezentációs tervek készülnek, vagy amelyekkel a kiesések vészhelyzeti áramellátás révén megelőzhetők;
- a technikai és szervezési intézkedések hatékonyságának nyomon követésére és értékelésére szolgáló eljárások a feldolgozás biztonságának garantálása érdekében: Biztosítani kell, hogy a fenti biztonsági intézkedések rendszeresen és alaposan nyomon követhetők és ellenőrizhetők legyenek, és ennek érdekében belső és külső ellenőrzési jelentéseket készítenek és értékelnek. Szükség esetén ezt megfelelő intézkedéseknek kell követniük.

A Motherson számára a technikai és szervezeti adatvédelmi intézkedések végrehajtása a legfontosabb prioritás, nemcsak a személyzet és az ügyfelek védelme, hanem az ipari kémkedés elleni hatékony küzdelem érdekében is.

DOKUMENTUM VERZIÓJA ELŐZMÉNYEK

VERZIÓTÖRTÉNET		
VERSION	**FELÜLVIZSGÁLÁSI DÁTUM**	**A VÁLTOZÁS LEÍRÁSA**
v.1	február 3, 2022	Eredeti dokumentum közzététele

1. FÜGGELÉK - PÉLDÁK A TECHNIKAI ÉS SZERVEZETI INTÉZKEDÉSEKRE

Titoktartás (GDPR 32. cikk (1) bekezdés b) pont)

- Fizikai hozzáférés-ellenőrzés
  Nincs jogosulatlan hozzáférés az adatfeldolgozó létesítményekhez, pl.: mágneses vagy chipkártyák, kulcsok, elektronikus ajtónyitók, létesítménybiztonsági szolgálatok és/vagy a bejárati biztonsági személyzet, riasztórendszerek, video-/CCTV-rendszerek.
- Elektronikus hozzáférés-ellenőrzés
  Az adatfeldolgozó és adattároló rendszerek jogosulatlan használata, pl.: (biztonságos) jelszavak, automatikus blokkolási/zárási mechanizmusok, kétfaktoros hitelesítés, az adathordozók/tárolóeszközök titkosítása.
- Belső hozzáférés-ellenőrzés (az adatokhoz való hozzáférési és módosítási jogosultságok)
  Az adatok jogosulatlan olvasása, másolása, módosítása vagy törlése a rendszeren belül, pl. jogosultsági koncepció, szükségletalapú hozzáférési jogok, a rendszerhez való hozzáférési események naplózása.
- Izolációs vezérlés
  A különböző célokból gyűjtött adatok elkülönített feldolgozása, pl. több ügyfél támogatása, homokozó dobozolás;
- Álnévtelenítés (GDPR 32. cikk (1) bekezdés a) pont; GDPR 25. cikk (1) bekezdés)
  A személyes adatok olyan módon történő feldolgozása, hogy az adatok további információk nélkül nem kapcsolhatók egy adott Érintetthez, feltéve, hogy ezeket a további információkat elkülönítve tárolják, és megfelelő technikai és szervezési intézkedésekkel biztosítják.

Integritás (GDPR 32. cikk (1) bekezdés b) pont)

- Adattovábbítás ellenőrzése
  Tilos az adatok jogosulatlan olvasása, másolása, módosítása vagy törlése elektronikus átvitel vagy szállítás esetén, pl.: Titkosítás, virtuális magánhálózatok (VPN), elektronikus aláírás;
- Adatbevitel-ellenőrzés
  Annak ellenőrzése, hogy a személyes adatokat az Adatkezelési Rendszerbe felveszik-e, módosítják-e vagy törlik-e, és ha igen, ki által, például: Naplózás, dokumentumkezelés

Elérhetőség és rugalmasság (GDPR 32. cikk (1) bekezdés b) pont)

- Rendelkezésre állás ellenőrzése
  A véletlen vagy szándékos megsemmisülés vagy veszteség megelőzése, pl.: Biztonsági mentési stratégia (online/offline; helyben/helyszínen), szünetmentes áramellátás (UPS), vírusvédelem, tűzfal, jelentési eljárások és vészhelyzeti tervezés.
- Gyors helyreállítás (GDPR 32. cikk (1) bekezdés c) pont) (GDPR 32. cikk (1) bekezdés c) pont);

Rendszeres tesztelési, értékelési és értékelési eljárások (GDPR 32. cikk (1) bekezdés d) pont; GDPR 25. cikk (1) bekezdés)

- Adatvédelem kezelése;
- Incidenskezelés;
- Tervezett és alapértelmezett adatvédelem (GDPR 25. cikk (2) bekezdés);
- Megrendelés vagy szerződés ellenőrzése
  A GDPR 28. cikke szerinti harmadik fél általi adatfeldolgozás az Ügyfél megfelelő utasításai nélkül, pl.: világos és egyértelmű szerződéses megállapodások, formalizált megrendeléskezelés, a Szolgáltató kiválasztásának szigorú ellenőrzése, előzetes értékelési kötelezettség, felügyeleti nyomon követési ellenőrzések.