# HP Inc Magyarország Kft. technikai és szervezési adatvédelmi intézkedései

**Tartalomjegyzék**



## 1. Bevezető rendelkezések

A jelen dokumentumban meghatározott technikai és szervezési intézkedések (TOM) az Adatfeldolgozási Megállapodásban meghatározott rendelkezések kiegészítéseként kerülnek bevezetésre (a GDPR 32. cikkében meghatározott követelmények végrehajtása érdekében). Az adatfeldolgozásra az Adatfeldolgozási Megállapodás rendelkezései változtatás nélkül alkalmazandók. A jelen Függelékben meghatározott rendelkezések az adott körülményektől függően további követelményként alkalmazandók. Az Adatfeldolgozási Megállapodás jelen Függelékében általános különbséget teszünk az alábbi változatok között:

- **1. sz. Változat:** Az adatfeldolgozó kizárólag vagy kiegészítőleg a saját informatikai infrastruktúráját (szerver/kliens, alkalmazás) (vagy egy alvállalkozó informatikai infrastruktúráját) vagy saját eszközeit használja.
  Vagy: Az adatfeldolgozó vagy az adatfeldolgozó által megbízott személy az adatkezelő személyes adatait az adatfeldolgozó/megbízott személy saját informatikai infrastruktúrájában vagy eszközein tárolja.
- **2. sz. Változat:** Az adatfeldolgozó az adatkezelő informatikai infrastruktúráját (szerver/kliens, alkalmazás) használja, és saját (vagy az alvállalkozói) eszközeivel fér hozzá az utóbbihoz. Az adatfeldolgozónál vagy harmadik félnél nem kerül sor adatok tárolására.
- **3. sz. Változat:** Az adatfeldolgozó kizárólag az adatkezelésért felelős ügyfél (adatkezelő) informatikai infrastruktúráját (szerver/kliens, alkalmazás) és eszközeit használja.

Az alábbi táblázatban az adott változatok esetén alkalmazandó rendelkezések találhatók:

| 1. sz. Változat | 2. sz. Változat | 3. sz. Változat |
|---|---|---|
| 1. Adatvédelmi cél - Rendelkezésre állás: | | |
| 1.1<br>1.2<br>1.3<br>1.4<br>1.5<br>1.6 | 1.1<br>1.2<br>1.3<br>1.4<br>1.5<br>1.6 | 1.5 |
| 2. Adatvédelmi cél - Integritás | | |
| 2.1<br>2.2<br>2.3<br>2.4<br>2.5 | 2.1<br>2.2<br>2.3<br>2.4 | 2.2<br>2.3 |
| 3. Adatvédelmi cél - Bizalmasság | | |
| 3.1<br>3.2 | 3.1<br>3.2 | |
| 4. Adatvédelmi cél - Összekapcsolhatatlanság | | |
| 4.1<br>4.2<br>4.3 | 4.1<br>4.2 | |
| 5. Adatvédelmi cél - Átláthatóság | | |
| 5.1<br>5.2<br>5.3<br>5.4<br>5.5 | 5.2<br>5.3<br>5.4 | 5.2<br>5.3<br>5.4 |
| 6. Adatvédelmi cél - Beavatkozás lehetősége | | |
| 6.1<br>6.2 | 6.2 | 6.2 |
| 7. Adatvédelmi cél - Adattakarékosság | | |
| 7.1<br>7.2<br>7.3 | 7.1<br>7.2 | |

## 1.1 A jelen dokumentumra vonatkozó felhasználói utasítások

A 2. pontban meghatározott intézkedések konkrétan megvalósítják a GDPR 32. cikkének követelményeit és védelmi céljait. A célok megállapítása függ a kezelésre kerülő adatok típusától, mennyiségétől és formájától, valamint a helyi körülményektől. Az adatfeldolgozás típusától függően további követelmények merülhetnek fel. Ezen követelmények lehetnek ágazatspecifikusak (pl. egészségügy, bankszektor), országspecifikusak (pl. országspecifikus jogszabályok) vagy további, Telekom Csoport specifikus követelmények.
A következő szakaszban az egyes adatvédelmi célokhoz tartozó intézkedések besorolása található.

## 1.2 Fogalom-meghatározások

A műszaki és szervezési intézkedésekre vonatkozó követelmények meghatározása körében különbség van a standard és magas védelmi szintek között. Magas védelmi szintre van szükség, ha:

- a feldolgozott személyes adatok a GDPR 9. cikkének (1) bekezdésében meghatározott különleges kategóriákba tartoznak vagy
- az adatkezelés formája megfelel a GDPR 35. cikkében vagy a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett hatásvizsgálati listáján szereplő, az adatvédelmi hatásvizsgálat elvégzésére irányuló kritériumoknak

Ha a személyes adatok különböző védelmi szinteket igényelnek, vagyis, ha az egyes elemek különböző védelmi kategóriákba tartoznak, a magasabb védelmi kategória alkalmazandó. A védelmi intézkedéseket ez alapján kell meghatározni.

## 2. Technikai és szervezési intézkedések

***1. Adatvédelmi cél - Rendelkezésre állás***

A „Rendelkezésre állás" adatvédelmi cél arra irányul, hogy a személyes adatokhoz azonnal hozzá lehessen férni, azonnal fel lehessen dolgozni, illetve azokat a meghatározott folyamatban megfelelően fel lehessen használni. Az adatoknak az arra jogosult személyek számára hozzáférhetőnek kell lenni, és biztosítani kell a kezelésükre kijelölt módszerek használhatóságát.

### 1.1. Követelmény Fizikai védelem a külső fenyegetésekkel szemben

A belső és külső fenyegetések elleni intézkedéseket az Adatfeldolgozó határozza meg és hajtja végre. Ezek a következők elleni védelmet biztosítják:

- Természeti katasztrófák, támadások vagy balesetek,
- Áramkimaradás vagy egyéb ellátási problémák,
- A kábelek szakadása, sérülése.

A fizikai védelmi intézkedések hatékonyságát rendszeresen tesztelni kell. A védelmi koncepciót az adatfeldolgozásban bekövetkező változásokhoz kell igazítani. A megfelelő folyamatokat az adatfeldolgozónak kell végrehajtania.

### 1.2 Követelmény Az informatikai rendszerek és hálózatok védelme a külső fenyegetésekkel szemben

Az adatfeldolgozó olyan szabályokat határozott meg és hajtott végre, amelyek megvédik a személyes adatok kezelésére használt informatikai rendszereket, hálózatokat és komponenseket (műszaki berendezések, segédprogramok stb.) a jogosulatlan hozzáféréstől, jogosulatlan módosítástól, elvesztéstől vagy megsemmisüléstől, illetve a téves vagy jogellenes felhasználástól. Ezen szabályok a teljes életciklus alatt érvényesek.
Az adatvédelem és az adatbiztonság beépül az üzlet folytonosság menedzsmentbe, így a folyamatok, eljárások és intézkedések biztosítják, hogy az adatkezelés még kedvezőtlen helyzetekben is szerződésszerű legyen. Az adatfeldolgozó rendszeresen felülvizsgálja ezen intézkedések hatékonyságát, és biztosítja a rendelkezésre állást, például redundanciák útján.

### 1.3. Követelmény A rendszer megerősítése

Az információs és az információfeldolgozó berendezések védve vannak a rosszindulatú szoftverek ellen (malware), az információfeldolgozó rendszerek megerősítettek. A rendszerek védelme érdekében megfelelő szoftvereket (pl. víruskeresők, IDS) telepítenek és tartanak naprakészen. Egy rendszer megerősítésekor legalább a következőket kell figyelembe venni:

- A javítások (patchek) naprakészek.
- A rendszer telepítése gyakran magában foglalja olyan szoftverkomponensek telepítését vagy akár egyes szoftverrészek aktiválását, amelyek nem szükségesek a rendszer későbbi működéséhez és funkcionalitásához. Az ilyen komponensek vagy nem kerültek bele a

telepítésbe, vagy utólag távolították el őket. A rendszerekre nem telepítettek olyan szoftvert, amely nem szükséges a rendszer későbbi működéséhez, karbantartásához vagy funkcionalitásához.
- A szoftverfunkciók mellett a rendszer telepítése után nem aktiválódnak a rendszer működéséhez szükségtelen hardverfunkciók sem. Az olyan funkciók, mint pl. a szükségtelen interfészek, tartósan deaktiválva vannak, és biztosítva van, hogy a rendszer újraindítása esetén is deaktiváltak maradnak.
- A rendszerben és az interfészekben lévő összes szükségtelen szolgáltatás teljes mértékben ki van kapcsolva, és ezek a rendszer újraindításakor is kikapcsolt állapotban maradnak.
- A szolgáltatás elérhetőségét csak a jogosult kommunikációs partnerekre korlátozták a szükséges interfészeken keresztül.
- A nem szükséges, előre beállított szolgáltatásfiókokat törölték, és megváltoztatták az alapértelmezett jelszavakat.
- Gyakran előfordul, hogy a gyártók, fejlesztők vagy beszállítók előre konfigurálnak hitelesítési funkciókat, mint pl. jelszavak és kriptográfiai kulcsok. Az ilyen hitelesítési funkciókat olyan különálló funkciókra változtatták, amelyekről harmadik feleknek nincsen tudomása.
- Ha a rendszert felhőplatformon üzemeltetik, ez megakadályozza, hogy a rendszert (vagy a teljes ügyfelet/bérlőt az összes szolgáltatással és adattal együtt) véletlenszerűen vagy illetéktelenek részéről töröljék.

**1.4 Követelmény Backup koncepció**

Az adatfeldolgozó által meghatározott és alkalmazott szabályok biztosítják a megfelelő biztonsági mentési stratégia működését. A stratégia különösen figyelembe veszi a rendszer rendelkezésre állására, a helyreállíthatóság rendszeres tesztelésére és a tárolásra vagy törlésre vonatkozó jogi követelményeket.
Ezen intézkedés célja annak biztosítása, hogy vészhelyzet esetén folyamatos maradjon az élő adatok feltérképezése (data mapping). A keretfeltételektől függően ebben az esetben különböző stratégiák alkalmazhatók. A klasszikus biztonsági mentési megoldás mellett lehetőség van tükröző rendszerek használatára egy elkülönült, biztonságos területen, vagy akár a két stratégia kombinációjára is.

**1.5. Követelmény A védelmi célok biztosítására vonatkozó személyzeti koncepció**

Az adatfeldolgozó olyan személyzeti koncepciót vezetett be, amely az alábbi intézkedésekkel támogatja az adatvédelmet:
- Csak olyan szakértő személyeket alkalmaznak, akik bizonyíthatóan részt vettek a szükséges adatvédelmi képzéseken, és megfelelő titoktartási kötelezettség alatt állnak.
- A személyes adatok minden feldolgozásához felelős kapcsolattartó kerül kijelölésre. Rendelkeznek érvényes helyettesítési protokollal.

A munkaviszony, szerződés vagy megállapodás megszűnése esetén a munkavállalók és az adatfeldolgozók visszaszolgáltatják a szervezetnek (adatkezelőnek/adatfeldolgozónak) azon eszközöket, amelyeket korábban a feladatuk ellátásához kaptak. Ezen eszközök közé tartoznak a hozzáférési eszközök, számítógépek, adathordozók és mobil eszközök.

**1.6. Követelmény Vészhelyzeti intézkedések az adatfeldolgozási tevékenység helyreállítása céljából**

Az adatfeldolgozó vészhelyzeti tervet / koncepciót vezetett be az adatfeldolgozás helyreállítására. A koncepció célja a rendelkezésre állás helyreállítása egy esetleges incidenst követően. A vészhelyzeti koncepciónak meg kell felelnie a következő követelményeknek/kritériumoknak:
- Vannak olyan szabályok, amelyek egy incidenst követően meghatározzák az adatfeldolgozás helyreállításához szükséges időt.
- Az adatok helyreállításához szükséges erőforrások rendelkezésre állnak
- A felelősségi körök kijelölésre kerültek
- Meghatározták az incidens elleni védekezésre és a szabályos működés helyreállítására vonatkozó ellenőrzött intézkedéseket
- Megvannak az információs és eszkalációs láncok
- Meghatározták a megfelelő folyamatokkal és szabályokkal (backup tervvel, személyi koncepcióval stb.) való interakciókat

***2. Adatvédelmi cél - Integritás***

Az "integritás" adatvédelmi célja szerint az informatikai folyamatoknak és rendszereknek folyamatosan meg kell felelniük a rájuk vonatkozó előírásoknak/specifikációnak, hogy folyamatosan el tudják látni a meghatározott funkciókat. Másrészről az „integritás" annak biztosítására is utal, hogy a kezelendő adatok sértetlenek, teljeskörűek, helytállóak és naprakészek maradnak.

**2.1. Követelmény A folyamatok megcélzott működésének meghatározása, alkalmazása és nyomon követése**

Az adatfeldolgozó a menedzsment vagy a vezető testület útján az adatvédelemre és az információbiztonságra vonatkozóan kötelező érvényű folyamatokat hozott létre. Ezen folyamatokat írásban rögzítik, szabadon hozzáférhetővé teszik, minden belső és külső munkatárs számára átadják és alkalmazzák. A rendelkezések célja, hogy a személyes adatok kezelése közben a folyamatok meghatározott működése mindenkor biztosított legyen. A rendelkezéseket rendszeresen felülvizsgálják azok hatékonyságának, naprakészségének és jogszabályi megfelelésének biztosítása érdekében.

**2.2. Követelmény Engedélyezési koncepció**

Az adatfeldolgozó olyan naprakész engedélyezési/hozzáférési koncepciókat alkalmaz, amelyek kötelező jelleggel meghatározzák, hogy ki, mikor és milyen rendszerekhez, adatbázisokhoz vagy hálózatokhoz férhet hozzá. Ezen koncepciónak a következő előírásoknak kell megfelelni:

- A meghatározott jogosultságok szerepkörök formájában kerültek létrehozásra, melyek alapjául az üzleti, biztonsági és adatvédelmi követelmények szolgálnak.
- A szerepkörök dokumentáltak és naprakészek.
- A szerepkörök egyedileg vannak hozzárendelve a felhasználókhoz vagy gépekhez.
- A felhasználók kizárólag azokhoz a hálózatokhoz, rendszerekhez és adatokhoz férhetnek hozzá, amelyekre kifejezetten felhatalmazást kaptak.
- A hozzáférési jogok kiosztása céljából bevezették a regisztrációra és a regisztráció törlésére vonatkozó formális eljárást.
- A felhasználói hozzáférések biztosítására formális folyamatot vezettek be, amely minden felhasználótípus számára minden rendszerhez és szolgáltatáshoz való hozzáférési jog biztosítására vagy visszavonására alkalmas.
- Az emelt szintű (privileged) hozzáférési jogok kiosztását és használatát korlátozzák és folyamatosan ellenőrzik.
- A hozzáférési jogok kiosztását monitorozzák, hogy ezzel megakadályozzák a jogosultságok különböző funkciókon átívelő kiosztását.

**2.3. Követelmény Identitáskezelés**

A személyes adatokhoz való hozzáférés engedélyezése csak a felhasználó egyedi azonosítása után történik. A rendszer a felhasználókat egyértelműen azonosítani tudja. Ennek érdekében minden felhasználóhoz egyedi felhasználói fiókot (account) használnak. Nincsenek csoportos fiókok, mely esetben egy felhasználói fiókot több személy használhat.
Ez alól a követelmény alól kivételt képeznek a gép fiókok (machine account). Ezeket a rendszerek közötti vagy a rendszeralkalmazások hitelesítésére és engedélyezésére használják, így ezeket nem lehet egyetlen személyhez rendelni. Az ilyen felhasználói fiókok rendszerenként vagy alkalmazásonként külön-külön kerülnek hozzárendelésre. Ez biztosítja, hogy az ilyen jellegű felhasználói fiókokkal ne lehessen visszaélni.

**2.4. követelmény Kriptográfia koncepció**

Az adatfeldolgozó iránymutatások útján meghatározta és végrehajtotta a személyes adatok védelmét szolgáló kriptográfiai intézkedéseket. Ez az iránymutatás szabályozza és garantálja a következőket:

- A legkorszerűbb kriptográfiai eljárások alkalmazása
- A személyes adatok szükséges védelmi szintje a kockázatértékelés alapján
- A kriptográfiai kulcsok kezelése és használata
- A kriptográfiai kulcsok védelme az életciklusuk során (létrehozás, tárolás, használat és megsemmisítés).

A kriptográfiai koncepció célja:

- Az érzékeny adatok sértetlenségének biztosítása
- Az identitáskezelési folyamatok biztosítása
- Az engedélyezési folyamatok támogatása
- Az érzékeny adatok titkosságának és sértetlenségének biztosítása

### 2.5. Követelmény Az adatok naprakészségének biztosítására szolgáló folyamatok

Az adatfeldolgozó olyan folyamatokat határozott meg, vezetett be és kommunikált, amelyek biztosítják a személyes adatok naprakészségét és megfelelését az alábbi követelményeknek:

- Az eljáró személyek engedélyezési, módosítási és törlési kérelmei azonnal megtörténnek, és minden elmentett adatrekordra vonatkoznak.
- A személyes adatok automatikusan vagy folyamatokkal vezérelve módosulnak vagy törlődnek az összes elmentett adatrekordban.
- Az adatokon végrehajtott módosítások időbélyegzővel különböztethetők meg egymástól.
- A tárolási és törlési időszakokat a jogszabályi vagy szerződéses előírásoknak megfelelően határozták meg.

## *3. Adatvédelmi cél - Bizalmasság*

A „Bizalmasság" adatvédelmi cél azon követelményre vonatkozik, hogy a személyes adatokhoz illetéktelen személy ne férhessen hozzá, illetve ne használhassa fel azokat. Jogosulatlan személynek nem csak az adatkezelőn kívüli harmadik személyek minősülnek, hanem a technikai szolgáltatók azon munkavállalói is, akiknek a szolgáltatás biztosításához nincs szükségük a személyes adatokhoz való hozzáférésre, vagy olyan szervezeti egységekben dolgozó személyek, akiknek nincs tartalmi vonatkozású információra szükségük az adatkezelési tevékenység vagy az érintett tekintetében.

### 3.1. Követelmény Az engedélyezett erőforrások és kommunikációs csatornák használatának meghatározása és nyomon követése

Az adatfeldolgozó a következő intézkedésekkel biztosítja, hogy a személyes adatok kezeléséhez használt erőforrások és kommunikációs csatornák meghatározásra kerüljenek, és hogy használatukat monitorozzák:

- A védelmi szint függvényében területeket határoznak meg; a szükséges biztonsági peremfeltételeket meghatározzák és végrehajtják. A védelmi szint besorolása a területeken található személyes adatok vagy információfeldolgozó rendszerek (beleértve a mobil munkaállomásokat is) alapján történik.
- Megfelelő beléptetési szabályokat határoznak meg és használnak, melyekkel biztosítják, hogy csak jogosult személyek lépjenek be a meghatározott területekre.
- A szervezetnél az adatvédelmi előírások és a biztonsági követelmények alapján rendszerhozzáférés szabályozási irányelvet kell kidolgozni és bevezetni. Ez az irányelv a személyes adatokhoz való hozzáférést a szükséges védelmi szint függvényében és a „szükséges ismeret" (need-to-know) alapelv szerint szabályozza. Ez különösen a személyes adatokat tartalmazó informatikai rendszerekhez, hálózatokhoz és adatbázisokhoz való hozzáférésre vonatkozik.
- Az adathordozók kezelésére vonatkozó eljárásokat a meghatározott védelmi szintnek megfelelően hajtják végre.
- Ha a személyes adatokat mobil adathordozókon tárolják, azokat hatékonyan kell titkosítani (lásd a 2.4. pontot).
- Az adathordozók szállítására vonatkozó szabályokat a személyes adatokra vonatkozó védelmi szintnek megfelelően hozzák létre. Ha a személyes adatokat nem titkosítják, megfelelő alternatív védelmi intézkedéseket kell hozni. Ha valamely területen magas szintű védelemre van szükség, különleges követelmények vannak a szállítás megbízhatóságára, az adatok titkosítására, valamint a dokumentációval, a naplózással és a bizonyítással kapcsolatos kötelezettségekre.

- Minden típusú kommunikációs berendezés (beleértve a mobil munkaállomásokat) esetében vannak irányelvek, biztonsági eljárások és ellenőrzések az információátvitel védelmére. A személyes adatok nyilvános hálózatokon keresztüli továbbítása esetén az adatokat mindig titkosítják.
- A szervezetnél a mobil eszközök (laptopok, külső adathordozók, mobiltelefonok) használatával kapcsolatosan beazonosított kockázatoknak megfelelően megfelelő iránymutatásokat és intézkedéseket hajtanak végre a személyes adatok bizalmas kezelésének és sértetlenségének biztosítására. Ezen szabályok célja a személyes adatokhoz való hozzáférés minimalizálása, tárolásuk és továbbításuk titkosítása, valamint a külső adathordozók használatának az abszolút minimumra csökkentése.

### 3.2. Követelmény Biztonságos hitelesítési eljárások

A rendszerekhez és alkalmazásokhoz biztonságos hitelesítési eljárás segítségével lehet hozzáférni. A hitelesítési eljárásnak meg kell felelnie a sikeres hitelesítés után hozzáférhetővé váló személyes adatokra vonatkozó védelmi szintnek. Ha a védelmi szint magas, akkor a birtokláson és megfelelő tudáson alapuló bejelentkezési eljárásokat kell alkalmazni (kétfaktoros hitelesítés). Magas védelmi szintet kell feltételezni a GDPR 9. cikkének (1) bekezdése alá tartozó adatokhoz való hozzáférés esetén. Ha a védelmi szint alacsony, elegendő a felhasználónévvel és jelszóval történő hitelesítés. A kiválasztott hitelesítési eljárás általánosságban megfelel a következő kritériumoknak:

- A rendszerben minden felhasználói fiók védve van az illetéktelen használat ellen. Ebből a célból a felhasználói fiókot olyan hitelesítési funkcióval látják el, amely lehetővé teszi a hozzáféréssel rendelkező felhasználó egyedi hitelesítését. A hitelesítési jellemzők közé tartoznak a jelszavak, jelszó-kifejezések, PIN-kódok, (faktorismeret)/kriptográfiai kulcsok, tokenek, intelligens kártyák, OTP (tulajdon)/vagy biometrikus jellemzők, például ujjlenyomat vagy kézgeometria (tulajdonság).
- A jelszavak létrehozására vonatkozó követelményeket (hosszúság, összetettség, újra felhasználás stb.) naprakész és élvonalbeli technológia határozza meg.
- Ha hitelesítési funkcióként jelszavakat használnak, akkor az online támadások, például a szótári és a brute force (találgatásos) támadások ellen is védelmet nyújtanak.
- A rendszer funkciói lehetővé teszik a felhasználók számára, hogy bármikor megváltoztathassák jelszavukat.
- A jelszavak mentése a legmodernebb, erre a célra alkalmas és biztonságosnak minősített egyirányú kriptográfiai funkcióval történik (ún. „jelszó-hashelés").
- A jelszavak kezelésére és kiosztására használt rendszerek biztosítják az erős jelszavak használatát. Ha a hozzáférés automatikusan, segédprogramokon vagy a szoftverfejlesztés során alkalmazott rutinokon keresztül történik, a használatot a lehető legkisebbre csökkentik, és a vonatkozó alkalmazást rendszeresen ellenőrzik.
- A rendszeren belüli kiterjesztett jogosultságokkal rendelkező felhasználók, pl. a rendkívül érzékeny személyes adatokhoz, konfigurációs beállításokhoz vagy rendszergazdai hozzáférésekhez legalább két, egymástól független hitelesítési funkciót kapnak a megfelelő szintű védelem érdekében. Az alkalmazott hitelesítési jellemzőknek különböző tényezőkből kell állniuk (ismeret, tulajdon, tulajdonság). Ez a megközelítés általánosságban MFA (többfaktoros hitelesítés) néven ismert. Az MFA egy speciális típusa a 2FA (2-faktoros hitelesítés), amely két hitelesítési funkciót kombinál. Az ugyanazon faktor hitelesítési jellemzőinek kombinációja (például két különböző jelszó) nem megengedett.

## *4. Adatvédelmi cél - Összekapcsolhatatlanság*

Az „Összekapcsolhatatlanság" adatvédelmi cél azt a követelményt jelenti, miszerint a személyes adatok nem vonhatók össze, azaz nem láncolhatók. Ezt különösen akkor kell megvalósítani, ha az összevonandó adatokat különböző célból gyűjtötték. Minél nagyobb és jelentőségteljesebb adatrekordokról van szó, annál nagyobb lehet az igény az adatok eredeti jogalapon kívüli felhasználására.

### 4.1. Követelmény Az adatkezelés céljának meghatározása

Az adatfeldolgozó megfelelő intézkedésekkel biztosítja, hogy a személyes adatok csak a szerződéses céllal összefüggésben kerüljenek kezelésre. Ezek az intézkedések a következők:

- A meghatározott cél belső dokumentálása és kommunikációja minden adatkezelési eljárás során
- Szabályozott adatkezelési cél módosítási eljárások

**4.2. Követelmény A célhoz kötöttség megvalósítását biztosító intézkedések**

Az adatfeldolgozó biztosítja, hogy a személyes adatokat kizárólag a szerződésben meghatározott célból kezeljék, és hogy csak az adatok kezelésére jogosult személyek által/esetekben férhetnek hozzá az adatokhoz. A rendelkezésre állás, sértetlenség és bizalmas jelleg adatvédelmi céljaira meghatározott követelmények mellett a következő intézkedéseket vezették be a különböző célú korlátozások alá eső adatrekordok láncolásának megakadályozására:

- A feldolgozás, felhasználás és továbbítás jogainak korlátozása az adatkezeléshez feltétlenül szükséges mértékig
- Szervezeti/területi határok szerinti elkülönítés
- A környezetek elkülönítése szerepkoncepciók alapján, többszintű hozzáférési jogosultságokkal identitáskezelés alapján, biztonságos hitelesítési eljárásokkal.
- A fejlesztési, tesztelési és üzemeltetési környezeteket legalább logikailag el kell választani egymástól. Megfelelő hozzáférés-ellenőrzéseket vezettek be annak biztosítására, hogy a hozzáférést a megfelelő felhatalmazással rendelkező személyekre korlátozzák. Ezekben a környezetekben a személyes adatok feldolgozása elkülönítésre került az egyéb adattípusoktól. A szétválasztást fizikailag vagy logikailag hajtották végre.
- Ha a teszthálózatoknak, fejlesztői hálózatoknak vagy eszközöknek hozzáférésre van szükségük a működő hálózathoz, mindez szigorú hozzáférési ellenőrzések alapján történik.
- Személyes adatok nem dolgozhatók fel teszt és fejlesztési környezetben. A fenti szabály alóli kivételeket az ügyfél külön, írásos utasításában kell meghatározni.

**4.3. Követelmény Anonimizálási eljárások meghatározása, végrehajtása és alkalmazása**

Az adatfeldolgozó úgy szervezi meg a személyes adatok kezelését, hogy az kizárólag a célhoz kötöttség mentén történjen. Ha a célhoz kötöttség nincs biztosítva, a szükségtelen adatok törlésre kerülnek. Ha az adatok törlése nem lehetséges, a vonatkozó rekordokat anonimizálják. Ehhez speciális célú álneveket, anonimizálási szolgáltatásokat, anonim hitelesítő adatokat és álnevesített vagy anonimizált adatok feldolgozását alkalmazzák; ezen kívül olyan adatmaszkokat is használnak, melyek elfedik az adatmezőket, mindemellett vannak automatikus zárolási és törlési rutinok, álnevesítési és anonimizálási eljárások is. Megjegyzés: az álnevesítési intézkedések jogilag csak néhány esetben megengedettek.

***5. Adatvédelmi cél - Átláthatóság***

Az "átláthatóság" adatvédelmi cél arra utal, hogy az érintettek, a rendszerek üzemeltetői, és az ellenőrző szervek különböző mértékben tudják beazonosítani, hogy az adott adatkezelés során mikor és milyen adatokat gyűjtenek és kezelnek, milyen rendszereket és folyamatokat használnak, az adatok milyen célból hová áramlanak, és ki viseli a jogi felelősséget az adatokért és a rendszerekért a különböző adatkezelési fázisokban.

**5.1. Követelmény Az eljárások nyilvántartása**

A GDPR 30. cikkének alábbi követelményét az adatfeldolgozó teljes mértékben végrehajtotta:
"Minden adatfeldolgozó és - ha van ilyen - az adatfeldolgozó képviselője nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

- Az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
- Az egyes adatkezelők nevében végzetti tevékenységek kategóriái;
- Adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;

- Ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

A nyilvántartást írásban kell vezetni. Ez lehet elektronikus formátumban is.
Az adatkezelő vagy az adatfeldolgozó, valamint - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselője megkeresés alapján a felügyeleti hatóság rendelkezésére bocsátja a nyilvántartást.
Ezen kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

**5.2. Követelmény Az adatfeldolgozás dokumentálása**

Az adatfeldolgozó a személyes adatok kezelését az alábbiak szerint dokumentálja:

- A személyes adatok kezelését dokumentáltan, teljes mértékben átláthatóan végzik. Ez a teljes feldolgozási ciklusra vonatkozik, vagyis a személyes adatok befogadásától/létrehozásától azok továbbításáig/törléséig.
- Az incidenseket, az adatfeldolgozási/adatkezelési problémákat, továbbá az adatkezelésii tevékenységeket, illetve a technikai és szervezési intézkedések módosításait dokumentálják.
- Az is dokumentálásra kerül, hogy ki és mikor fér hozzá az adatokhoz.

**5.3. Követelmény A szerződések, megállapodások és utasítások dokumentálása és tárolása**

Az adatfeldolgozó minden szerződést, megállapodást vagy utasítást biztonságos körülmények között tárol. Ez azt jelenti, hogy a dokumentumok a szerződő felek vagy a felügyeleti hatóságok számára bármikor hozzáférhetők.

**5.4. Követelmény Az adatfeldolgozás naplózása**

A felhasználók és a rendszergazdák személyes adatokhoz való hozzáférését naplózni és rendszeresen ellenőrizni kell, figyelembe véve az adattakarékosság elvét és a védelmi szintet. A hozzáférés és a hozzáférés típusa (pl. olvasás, szerkesztés, törlés) naplózásra kerül.
A vonatkozó eseményeket, kivételeket, incidenseket és információbiztonsági eseményeket naplózzák és rendszeresen ellenőrzik.
A naplókat úgy tárolják, hogy a bejelentkezett rendszergazdák vagy felhasználók ne férhessenek hozzá.

**5.5. Követelmény Az információszolgáltatási kötelezettségek biztosítása**

Az adatfeldolgozó olyan eljárást vezetett be, amely a GDPR 15. cikkének megfelelően támogatja az érintettek hozzáférési jogát. A folyamatot rendszeresen ellenőrzik a hatékonyságának biztosítása érdekében.

***6. Adatvédelmi cél - Beavatkozás lehetősége***

A „beavatkozás lehetősége" adatvédelmi cél arra utal, hogy az érintettnek azonnal és ténylegesen joga van az értesítéshez, tájékoztatáshoz, helyesbítéshez, törléshez, korlátozáshoz, adathordozhatósághoz, tiltakozáshoz és az automatizált egyedi döntésekbe való beavatkozáshoz, ha az erre vonatkozó jogi követelmények fennállnak, és az adatfeldolgozó szervezeti egység köteles végrehajtani a megfelelő intézkedéseket.

**6.1. Követelmény Az érintettek jogaira vonatkozó folyamatok végrehajtása**

Az adatfeldolgozó intézkedéseket vezetett be az érintettek jogainak védelmére. Általánosságban véve az alábbiakban felsorolt intézkedések megfelelőnek minősülnek:

- Kivéve, ha adatkezelő ezt már korábban bevezette, az adatfeldolgozónak folyamatot kell bevezetnie azon személyek azonosítására és hitelesítésére, akik szeretnék gyakorolni az érintettek jogait.
- Az adatkezelő és az adatfeldolgozó közösen határozzák meg azon jellemzőt, amellyel az érintettet a szervezeti határokon átnyúlóan egyértelműen azonosítani lehet.

- Az adatfeldolgozó olyan rendszereket, szoftvereket és eljárásokat vezetett be, amelyek lehetővé teszik a hozzájárulás, a hozzájárulás visszavonása és a tiltakozás differenciált lehetőségeit.
- Az adatfeldolgozó operatív lehetőségeket biztosított az egy adott személyre vonatkozóan tárolt összes információ összeállítására, helyesbítésére, zárolására és törlésére.
- Előnyben részesülnek azok az automatizált adatkezelési folyamatok (nem döntéshozatali folyamatok), amelyek a kezelt adatokhoz való hozzáférést elhagyhatóvá teszik, és a párbeszéd-vezérelt folyamatokhoz képest korlátozzák a befolyásgyakorlást.

**6.2. Követelmény Az érintettek jogainak a rendszer tervezésekor történő figyelembevételét célzó intézkedések bevezetése (beépített adatvédelem/privacy by design))**

Az adatfeldolgozó a rendszer tervezése során figyelembe veszi az érintettek jogait és az adatvédelmi követelményeket. A következő intézkedéseket kell végrehajtani a rendszer tervezése során (folyamatok és szoftver):

- Alapértelmezett beállítások meghatározása az érintettek részére, melyek az adatkezelés céljához szükséges mértékben korlátozzák az adataik kezelését.
- Program konfigurációs lehetőségek biztosítása az érintettek számára, hogy a programok az adatvédelmi követelményeknek megfelelően konfigurálhatók legyenek.
- Az egyes funkciók kikapcsolásának lehetősége anélkül, hogy az a rendszer egészét befolyásolná.
- Standard lekérdezési és párbeszéd interfészek biztosítása az érintettek számára az igények érvényesítésére és/vagy végrehajtására.
- Az érintettek által hívható, strukturált, géppel olvasható adat interfész működtetése.
- A feldolgozási lehetőségek csökkentése a feldolgozási lépésekben, vagyis az adatok a lehető legkevesebb adatkezelési lépésnek legyenek kitéve.
- A szükséges adatmezők létrehozása, pl. a zárjelzők, értesítések, hozzájárulások, ellentmondások, ellennyilatkozatok számára.
- A szükségtelen adatmezők és opciók eltávolítása, a kimenetek csökkentése az adatbázisokban történő keresések esetén, az export és nyomtatási funkciók minimalizálása.

***7. Adatvédelmi cél - Adattakarékosság***

Az "adattakarékosság" adatvédelmi célja magában foglalja azt az alapvető adatvédelmi elvet, miszerint a személyes adatok kezelését a célnak megfelelő, releváns és szükséges mértékre kell korlátozni. Ez a minimalizálási kötelezettség drasztikusan befolyásolja a védelmi program körét és intenzitását, amelyet a többi adatvédelmi cél határoz meg.

**7.1. Követelmény Operatív intézkedések az adatok minimalizálására**

Az adatfeldolgozó operatív intézkedéseket hoz azzal a céllal, hogy a személyes adatok meghatározott célú kezelését a lehető legkisebb mértékűre korlátozza. A következő intézkedéseket kell végrehajtani:

- Az érintettre vonatkozóan rögzített attribútumokat a szükséges minimumra kell korlátozni.
- Személyes adatok továbbítása esetén csak azokat az attribútumokat továbbítják, amelyek a következő adatkezelési lépés szempontjából elengedhetetlenek.

**7.2. Követelmény Az adattakarékosságra irányuló technikai intézkedések**

Az adatfeldolgozó technikai intézkedéseket hoz annak érdekében, hogy a személyes adatok meghatározott célú kezelését a lehető legkisebb mértékűre korlátozza. Erre a következő intézkedések alkalmasak:

- A feldolgozási lehetőségek korlátozása a feldolgozási lépésekben, vagyis az adatok a lehető legkevesebb adatkezelési lépésnek legyenek kitéve.
- Az adatmezőket elfedő adatmaszkok, valamint automatikus zárolási és törlési rutinok, álnevesítési és anonimizálási eljárások bevezetése.
- A rendelkezésre álló adatokhoz való hozzáférés (megjelenítési lehetőségek, keresőmezők stb.) lehető legalacsonyabb szintre történő korlátozása.

**7.3. Követelmény Törlési koncepció meghatározása, végrehajtása és ellenőrzése**

A személyes adatok feldolgozásakor az adatfeldolgozó minden egyes alkalommal törlési koncepciót készít, amely a következőket tartalmazza:

- A törlendő adatmezők

- A törlési időszakok meghatározása
- A törlés ellenőrzése és igazolása
- Irányítás