**1. SZ. FÜGGELÉK**

**ADATFELDOLGOZÁSI MEGÁLLAPODÁS** ("**AFM**")

amely létrejött az alábbi, a jelen AFM **I. Mellékletében** meghatározott felek között:

az **IMPORTŐR**, melynek székhelye:André Citroën utca 1, 1194 Budapest, Magyarország, az alábbiakban meghatározottak szerint mint ADATKEZELŐ ("Adatkezelő") vagy mint ADATFELDOLGOZÓ ("Adatfeldolgozó") jár el aMEGÁLLAPODÁS 6. Mellékletében megjelölt személyes adatok kezelésével kapcsolatban

**és**

a **MÁRKASZERVIZ**, melynek székhelye xxxxxxxxxxxxxxx, az alábbiakban meghatározottak szerint mint ADATKEZELŐ ("Adatkezelő") vagy mint ADATFELDOLGOZÓ ("Adatfeldolgozó") jár el a MEGÁLLAPODÁS 6. Mellékletében megjelölt személyes adatok kezelésével kapcsolatban;

együttesen: "a **Felek**".

A "**MÁRKASZERVIZ-MEGÁLLAPODÁS**"(a "MEGÁLLAPODÁS") alapján a jelen AFM-mel az(ok) a Fél/Felek, aki(k) a MEGÁLLAPODÁS **6. Mellékletében** felsorolt és az itt említett célokból Adatkezelők(k)ént jár(nak) el, a jelen AFM **II. Mellékletében** leírt célokra való hivatkozással (kölcsönösen) Adatfeldolgozónak jelöli(k) egymást.

A Felek továbbá a Bizottság (EU) 2021/915 2021/915 végrehajtási határozata szerinti Általános Szerződési Feltételek (a "GDPR 28. Cikk szerinti ÁSZF”) módosítása érdekében a következő rendelkezésekben állapodnak meg. Ellentmondás esetén a hierarchiára vonatkozó 4. feltétel alkalmazandó.

1. **Időtartam**

A jelen AFM időtartama megegyezik a MEGÁLLAPODÁS időtartamával.

1. **Technikai és szervezési intézkedések**
2. A technikai és szervezési intézkedéseket a jelen AFM **III. Melléklete** tartalmazza.
3. Az alkalmazandó mértékben, az Adatfeldolgozó (adott esetben alvállalkozói, leányvállalatai vagy ügynökei tekintetében is) biztosítja a jelen AFM **III. Mellékletében** szereplőInformációbiztonsági Irányelvnek és annak mellékleteinek ("IBI") való megfelelést.
4. A technikai és szervezési intézkedések a technika fejlődésének és továbbfejlesztésének függvényei. A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK Rendelet hatályon kívül helyezéséről szóló, 2016. április 27-ei (EU) 2016/679 Európai Parlamenti és Tanácsi Rendelet ("GDPR") és a GDPR 28. Cikk szerinti ÁSZF-ek sérelme nélkül, megengedett, hogy az Adatfeldolgozó megfelelő alternatív intézkedéseket hajtson végre. Ennek során a meghatározott intézkedések biztonsági szintje nem csökkenhet. A lényeges változtatásokat pedig dokumentálni kell.
5. Az Adatfeldolgozó rendszeresen ellenőrzi a belső folyamatokat, valamint a technikai és szervezési intézkedéseket annak biztosítása érdekében, hogy a felelősségi körébe tartozó adatfeldolgozás összhangban legyen az alkalmazandó jogszabályi követelményekkel és az érintettek jogainak védelmével.
6. Az adatokról sem másolatok, sem másodpéldányok nem készíthetők az Adatkezelő tudta nélkül, kivételt képeznek ez alól azok a biztonsági másolatok, amelyek a szabályos adatfeldolgozás biztosításához, valamint az adatok megőrzésére vonatkozó jogszabályi előírások teljesítéséhez szükségek.
7. **Személyes adatok továbbítása az Európai Gazdasági Térségen kívülre**
8. Az Adatfeldolgozó vállalja, hogy nem továbbít személyes adatokat az EGT-n kívüli harmadik országba, ha a személyes adatok védelmének az EGT-n belüli védelemmel lényegében egyenértékű szintje nem biztosítható. Amennyiben az adott országra vonatkozóan nincs megfelelőségi határozat, úgy az Adatfeldolgozó aláírja a Bizottság (EU) 914/2021 végrehajtási határozata szerinti Általános Szerződési Feltételeket (azok megfelelő Modulját), és előzetesen elvégzi a megfelelő adatvédelmi szintre vonatkozó Adattovábbítási Hatásvizsgálatot (ATHV), és azt ellenőrzés során az Adatkezelő rendelkezésére bocsátja.
9. **Felelősség**
10. Az Adatfeldolgozó köteles teljes felelősséget vállalni, valamint kártalanítani és mentesíteni az Adatkezelőt minden olyan követeléssel, felelősséggel, költséggel, eljárással, kárral és kiadással (ideértve az észszerű jogi és egyéb szakértői díjakat) szemben, amely az Adatkezelőnél az Adatfeldolgozónak, ideértve az alkalmazottainak, leányvállalatainak vagy további adatfeldolgozóinak/aladatfeldolgozóinak a jelen AFM szerinti adatfeldolgozási tevékenységeivel kapcsolatos cselekménye vagy mulasztása miatt merül fel.
11. A Felek egyetértenek abban, hogy a MEGÁLLAPODÁS tekintetében előírt felelősségkorlátozás nem vonatkozik az AFM alapján kezelt adatok megsértése és/vagy az Adatfeldolgozó jogi és/vagy szerződéses kötelezettségeinek megszegése miatt elszenvedett károkra.
12. Ezen IV. Cikk bármely okból történő felmondás vagy lejárat után is fennmarad.
13. **Vegyes rendelkezések**
14. A visszatartás joga kifejezetten kizárt a kezelt adatok és a kapcsolódó adathordozók tekintetében az Adatkezelő és az Adatfeldolgozó közötti szerződéses kapcsolatból eredő valamennyi követelés tekintetében.
15. A jelen AFM-re és annak értelmezésére a magyar jog az irányadó. Felek a jelen AFM-mel kapcsolatos vagy abból eredő bármely jogvita esetére hatáskörtől függően kikötik a Székesfehérvári Törvényszék, illetve a Budai Központi Kerületi Bíróság illetékességét.
16. A jelen AFM-et érvényesen módosítani és kiegészíteni csak írásban lehet. Ez vonatkozik a felmondó vagy az írásbeliségről lemondó nyilatkozatokra is.
17. Amennyiben a jelen AFM bármely rendelkezése érvénytelenné, jogellenessé vagy végrehajthatatlanná válik, vagy azt bármely illetékes bíróság érvénytelennek vagy végrehajthatatlannak tekinti, úgy a jelen AFM fennmaradó rendelkezései teljes mértékben hatályban maradnak és azt a Felek kötelesek közösen az adott rendelkezés céljához legközelebb álló rendelkezéssel pótolni.
18. A jelen AFM hatálybalépésével a Felek megszüntetik a közöttük fennálló egyéb, korábbi adatfeldolgozási megállapodásokat az Importőri CRM rendszerre (Progression) vonatkozóan kötött adatfeldolgozási megállapodás kivételével, amely továbbra is hatályban marad.
19. **A Felek** **által módosított, a Bizottság (EU) 2021/915 végrehajtási határozata szerinti általános szerződési feltételek**

**I. SZAKASZ**

***1. feltétel Cél és alkalmazási kör***

1. Ezen általános szerződési feltételek (a továbbiakban: a feltételek) célja a következő cikknek való megfelelés: a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK Rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet 28. cikkének (3) és (4) bekezdése.
2. Az I. mellékletben felsorolt adatkezelők és adatfeldolgozók az (EU) 2016/679 rendelet 28. cikke (3) és (4) bekezdésének való megfelelés biztosítása érdekében elfogadták ezeket a feltételeket.
3. E feltételek a II. mellékletben meghatározott személyes adatok kezelésére vonatkoznak.
4. Az I-IV. melléklet a feltételek szerves részét képezi.
5. Ezek a feltételek nem érintik az adatkezelőre az (EU) 2016/679 rendelet értelmében háruló kötelezettségeket.
6. Ezek a feltételek önmagukban nem biztosítják az (EU) 2016/679 rendelet V. fejezete szerinti nemzetközi adattovábbításokkal kapcsolatos kötelezettségek teljesítését.

***2. feltétel A feltételek megváltoztathatatlansága***

1. A felek vállalják, hogy nem módosítják a feltételeket, kivéve, ha a mellékleteket további információkkal egészítik ki, vagy a bennük szereplő információkat frissítik.
2. Ez nem akadályozza meg a Feleket abban, hogy az e szerződési feltételekben meghatározott általános szerződési feltételeket egy szélesebb szerződésbe foglalják vagy egyéb záradékokkal vagy kiegészítő garanciákkal egészítsék ki, feltéve, hogy azok sem közvetlenül, sem közvetve nem mondanak ellent ezeknek a feltételeknek, és nem csökkentik az érintettek alapvető jogait vagy szabadságait.

***3. feltétel Értelmezés***

1. Amennyiben ezek a feltételek az (EU) 2016/679 rendeletben meghatározott fogalmakat használják, e fogalmak jelentése megegyezik az említett rendeletben foglaltakkal.
2. Ezeket a feltételeket az (EU) 2016/679 rendelet rendelkezéseinek fényében és az érintett Adatkezelő székhelye szerinti uniós tagállam adatvédelmi jogszabályaival összhangban kell értelmezni.
3. E feltételek nem értelmezhetők oly módon, amely ellentétes az (EU) 2016/679 rendeletben meghatározott jogokkal és kötelezettségekkel, vagy oly módon, amely sérti az érintettek alapvető jogait vagy szabadságait.

***4. feltétel Hierarchia***

Abban az esetben, ha ellentmondás áll fenn e feltételek és a Felek között az e feltételek elfogadásakor vagy az azt követően

létrejött kapcsolódó megállapodásokban foglalt rendelkezések között, ezek a feltételek az irányadók.

***5. feltétel Dokkolási feltétel***

1. Az a jogalany, amely e feltételeknek nem részes fele, minden Fél beleegyezése mellett a mellékletek kitöltésével és az I. melléklet aláírásával bármikor csatlakozhat ezekhez a feltételekhez adatkezelőként vagy adatfeldolgozóként.
2. Az (a) pontban említett mellékletek kitöltését és aláírását követően a csatlakozó jogalanyt e feltételek részes felének kell tekinteni, és megilletik az adatkezelő vagy adatfeldolgozó jogai és kötelezettségei az I. mellékletben szereplő megnevezéssel összhangban.
3. A csatlakozó jogalany nem rendelkezik a részes féllé válást megelőző időszakból az e feltételekből eredő jogokkal vagy kötelezettségekkel.

**II. SZAKASZ A FELEK KÖTELEZETTSÉGEI**

***6. feltétel Az adatkezelés(ek) és az Általános Keretrendszer leírása***

Az adatkezelési műveletek részleteit, különösen a személyes adatok kategóriáit és azon adatkezelési célokat, amelyek miatt

a személyes adatokat az adatkezelő nevében kezelik, a II. melléklet határozza meg.

A II. Melléklet célja a Felek közötti adatközlés szabályainak megállapítása az ÜGYFÉL-igények jobb kielégítése, illetve következetes, zökkenőmentes és minőségi ügyfélélmény nyújtása érdekében.

A Megállapodásban meghatározottak szerinti adatközlés lehetőséget ad:

* a fejlettebb adatminőségnek és -teljességnek köszönhető jobb ÜGYFÉL-ismeretre. Így különösen ez lehetővé teszi a megfelelő termék/üzenet az ÜGYFELEK-nek való megfelelő időben történő átadását ezáltal növelve a marketingtevékenység hatékonyságát.
* valódi 360°-os látásmódra az ÜGYFELEK (beleértve a potenciális Ügyfeleket is) valamennyi kapcsolattartási ponton való felismeréséhez.

Ezen célok elérése érdekében a Felek egy valamennyi Ügyféladatot szabályozó Egyedi Ügyfélreferenciát („EÜR") alkalmaznak.

***6.1. feltétel Az Egyedi Ügyfélreferencia (EÜR) szerepe***

Az EÜR célja, hogy egyetlen referenciában összesítse a Stellantis és a Hálózata által használt adatbázisokban, digitális Adatokban és külső fájlokban meglévő valamennyi ÜGYFÉL-Adatot.

Ezen EÜR-en belül az Adatok másodpéldányainak törlésére, illetve az Adatok egyesítésére vonatkozó szabályok az ÜGYFÉL-Adatok megbízhatóságától és frissítési dátumától függően kerülnek implementálásra. Az EÜR az optimális adathasználat érdekében továbbfejlesztett és minőségi ÜGYFÉL-fájlokat tartalmaz.

A cél az, hogy a Stellantis és a márkaszerviz számára is egy olyan ÜGYFÉL-fájl álljon rendelkezésre, amely - a meghatározott szabályok tiszteletben tartásával - elérhetővé teszi a legfrissebb ÜGYFÉL-Adatokat.

***7. feltétel A Felek kötelezettségei***

1. **7.1 Utasítások**
2. Az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő. Ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja. Az adatkezelő a személyes adatok kezelésének teljes időtartama alatt további utasításokat is adhat. Ezeket az utasításokat mindig dokumentálni kell.
3. Az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha az adatfeldolgozó véleménye szerint az adatkezelő által adott utasítások sértik az (EU) 2016/679 rendeletet vagy az alkalmazandó uniós vagy tagállami adatvédelmi rendelkezéseket.
   1. **Célhoz kötöttség**

Az adatfeldolgozó a személyes adatokat kizárólag a II. mellékletben meghatározott konkrét cél(ok)ból kezelheti, amennyiben nem kap további utasításokat az adatkezelőtől.

1. **7.3 A személyes adatok kezelésének időtartama**

Az adatfeldolgozó általi adatkezelésre csak a II. mellékletben meghatározott ideig kerülhet sor.

1. **7.4 Az adatkezelés biztonsága**
2. Az adatfeldolgozó végrehajtja legalább a III. mellékletben meghatározott technikai és szervezési intézkedéseket a személyes adatok biztonságának garantálása érdekében. Ez magában foglalja az adatoknak a biztonság olyan megsértése elleni védelmét, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést eredményezi (adatvédelmi incidens). A megfelelő biztonsági szint értékelése során a Feleknek kellően figyelembe kell venni a technika állását, a végrehajtás költségeit, az adatkezelés jellegét, hatókörét, kontextusát és céljait, valamint az érintetteket érintő kockázatokat.
3. Az adatfeldolgozó csak a szerződés végrehajtásához, kezeléséhez és nyomon követéséhez feltétlenül szükséges mértékben biztosít hozzáférést a munkavállalói számára a kezelés alatt álló személyes adatokhoz. Az adatfeldolgozó biztosítja azt, hogy a kapott személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállaljanak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt álljanak.
4. **7.5 Különleges adatok**

Amennyiben az adatkezelés faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatot, természetes személy egyedi azonosítását célzó genetikai vagy biometrikus adatokat, egészségi állapotra vagy egy személy szexuális életére vagy a szexuális irányultságára vonatkozó adatokat vagy büntetőjogi felelősséget megállapító ítéletekre és bűncselekményekre vonatkozó adatokat tartalmaz („különleges adatok”), az adatfeldolgozó egyedi korlátozásokat és/vagy további garanciákat alkalmaz.

1. **7.6 Dokumentáció és megfelelés**
2. A Feleknek igazolniuk kell, hogy eleget tesznek az e feltételek szerinti kötelezettségeiknek.
3. Az adatfeldolgozó haladéktalanul és megfelelően kezeli az adatkezelőnek az e feltételekkel összhangban végzett adatkezeléssel kapcsolatos kérdéseit.
4. Az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e feltételekben meghatározott, közvetlenül az (EU) 2016/679 rendeletből eredő kötelezettségek teljesítésének igazolásához szükséges. Az adatkezelő kérésére az adatfeldolgozónak lehetővé kell tennie továbbá és hozzá kell járulnia az észszerű időközönkénti vagy a megfelelés elmaradására utaló jelek esetén történő ellenőrzéshez az e feltételek hatálya alá tartozó adatkezelési tevékenységekkel kapcsolatban. A felülvizsgálatra vagy ellenőrzésre vonatkozó döntés meghozatalakor az adatkezelő figyelembe veheti az adatfeldolgozó birtokában lévő vonatkozó tanúsítványokat.
5. Az adatkezelő dönthet úgy, hogy maga végzi el az ellenőrzést, vagy megbíz egy független könyvvizsgálót (vagy más ellenőrt). Az ellenőrzések kiterjedhetnek az adatfeldolgozó telephelyein vagy fizikai létesítményeiben végzett vizsgálatokra is, amelyeket, adott esetben, észszerű értesítés mellett kell elvégezni.
6. A Felek kérésre az illetékes felügyeleti hatóság(ok) rendelkezésére bocsátják az e feltételben említett információkat, beleértve az ellenőrzések eredményeit is.
7. **7.7. További adatfeldolgozók alkalmazása**
8. Az adatfeldolgozó az adatkezelő általános engedélyével további adatfeldolgozókat vehet igénybe. Az adatkezelő egy ilyen AFM aláírásával elfogadja, hogy az adatfeldolgozó a GDPR betartása mellett a MEGÁLLAPODÁS végrehajtásához szükséges további adatfeldolgozót vehet igénybe. Szükség esetén az adatfeldolgozó az adatkezelő rendelkezésére bocsátja a MEGÁLLAPODÁS-ban foglalt konkrét szolgáltatásban részt vevő további adatfeldolgozók azonosításához szükséges információkat.
9. Amennyiben az adatfeldolgozó meghatározott adatkezelési tevékenységek végzése céljából (az adatkezelő nevében) további adatfeldolgozót vesz igénybe, ezt olyan szerződés útján kell megtennie, amely lényegében ugyanazokat az adatvédelmi kötelezettségeket rója a további feldolgozóra, mint amelyeket e feltételekkel összhangban az adatfeldolgozó számára előírnak. Az adatfeldolgozó biztosítja, hogy a további adatfeldolgozó teljesítse azokat a kötelezettségeket, amelyek az adatfeldolgozóra e feltételek, valamint az (EU) 2016/679 rendelet értelmében alkalmazandók.
10. Az adatkezelő kérésére az adatfeldolgozónak az adatkezelő rendelkezésére kell bocsátania a további adatfeldolgozóra vonatkozó megállapodás és annak későbbi módosításai egy példányát. Az üzleti titok vagy más bizalmas információk, köztük a személyes adatok védelméhez szükséges mértékben az adatfeldolgozó a másolat megosztása előtt kivonatolhatja a megállapodás szövegét.
11. Az adatfeldolgozó továbbra is teljes mértékben felel az adatkezelő felé a további adatfeldolgozónak az adatfeldolgozóval kötött szerződése szerinti kötelezettségei teljesítéséért. Az adatfeldolgozó értesíti az adatkezelőt, ha a további adatfeldolgozó nem teljesíti a szerződéses kötelezettségeit.
12. Az adatfeldolgozó megállapodik a további adatfeldolgozóval a kedvezményezett harmadik félről szóló záradékról, amelynek értelmében az adatkezelő jogosult felmondani a további adatfeldolgozóra vonatkozó szerződést, és a további adatfeldolgozót a személyes adatok törlésére vagy visszaküldésére utasítani, ha az adatfeldolgozó ténylegesen eltűnt, megszűnt létezni a jog szerint, vagy fizetésképtelenné vált.
13. **7.8 Nemzetközi adattovábbítások**
14. Az adatfeldolgozó általi, harmadik országba vagy nemzetközi szervezet részére történő adattovábbításra kizárólag az adatkezelő dokumentált utasításai alapján vagy az adatfeldolgozóra vonatkozó uniós vagy tagállami jog valamely konkrét követelményének teljesítése céljából kerülhet sor, és azt az (EU) 2016/679 rendelet V. fejezetével összhangban kell végrehajtani.
15. Az adatkezelő egyetért azzal, hogy amennyiben az adatfeldolgozó a 7.7. feltétellel összhangban további adatfeldolgozót vesz igénybe meghatározott adatkezelési tevékenységeknek (az adatkezelő nevében történő) végzése céljából, és az adatkezelési tevékenységek az (EU) 2016/679 rendelet V. fejezete értelmében személyes adatok továbbításával járnak, az adatfeldolgozó és a további adatfeldolgozó a Bizottság általa az (EU) 2016/679 rendelet 46. cikkének (2) bekezdésével összhangban elfogadott általános szerződési feltételek alkalmazásával biztosíthatja az (EU) 2016/679 rendelet V. fejezetének való megfelelést, feltéve, hogy teljesülnek az említett általános szerződési feltételek alkalmazásának feltételei.

***8. feltétel Segítségnyújtás az adatkezelőnek***

1. Az adatfeldolgozó haladéktalanul értesíti az adatkezelőt az érintettől kapott valamennyi kérelemről. A kérelemre ő maga nem válaszolhat, hacsak erre az adatkezelő fel nem hatalmazza.
2. Az adatfeldolgozó segíti az adatkezelőt azon kötelezettségei teljesítésében, hogy válaszoljon az érintetteknek a jogaik gyakorlásával kapcsolatos kérelmeire, figyelembe véve az adatkezelés jellegét. Az adatfeldolgozó az a) és b) pont szerinti kötelezettségei teljesítése során köteles betartani az adatkezelő utasításait.
3. Az adatfeldolgozó azon kötelezettségén túl, hogy segítséget nyújt az adatkezelőnek a 8. feltétel b) pontja értelmében, az adatfeldolgozónak segítenie kell az adatkezelőt a következő kötelezettségek teljesítésében is, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat:
   * + 1. a tervezett adatkezelési műveletek személyes adatok védelmére gyakorolt hatásának értékelésére vonatkozó kötelezettség (a továbbiakban: adatvédelmi hatásvizsgálat), amennyiben az adatkezelés valamely típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve;
       2. ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az illetékes felügyeleti hatósággal/hatóságokkal való konzultációra irányuló kötelezettség;
       3. a személyes adatok pontosságának és naprakészségének biztosítására vonatkozó kötelezettség, az adatkezelő haladéktalan tájékoztatásával, amennyiben az adatfeldolgozó tudomására jut, hogy az általa kezelt személyes adatok pontatlanok vagy elavulttá váltak;
       4. az (EU) 2016/679 rendelet 32. cikkében foglalt kötelezettségek.
4. A Felek a III. mellékletben meghatározzák a megfelelő technikai és szervezési intézkedéseket, amelyek alapján az adatfeldolgozó köteles segítséget nyújtani az adatkezelőnek a jelen feltétel alkalmazásában, valamint a szükséges segítségnyújtás hatókörét és mértékét.

***9. feltétel Adatvédelmi incidensről szóló értesítés***

Adatvédelmi incidens esetén az adatfeldolgozónak együtt kell működnie az adatkezelővel és segítenie kell az adatkezelőt az (EU) 2016/679 rendelet 33. és 34. cikke szerinti kötelezettségei teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat.

**9.1 Az adatkezelő által kezelt adatokkal kapcsolatos adatvédelmi incidens**

Az adatkezelő által kezelt személyes adatokkal kapcsolatos adatvédelmi incidens esetén az adatfeldolgozó segíti az adatkezelőt a következőkben:

1. adott esetben az adatkezelő tudomására jutását követően indokolatlan késedelem nélkül értesíti az illetékes felügyeleti hatóságo(ka)t az adatvédelmi incidensről (kivéve, ha az adatvédelmi incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve);
2. megszerzi a következő információkat, amelyeket az (EU) 2016/679 rendelet 33. cikkének (3) bekezdése értelmében az adatkezelő értesítésében fel kell tüntetni, és amelyeknek legalább a következőket kell tartalmazniuk:
   1. a személyes adatok jellege, beleértve - ha lehetséges - az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett személyes adatok kategóriáit és hozzávetőleges számát;
   2. az adatvédelmi incidens valószínűsíthető következményei;
   3. az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Ha és amennyiben nem lehetséges egyidejűleg az összes információt megadni, a kezdeti értesítésnek tartalmaznia kell az akkor rendelkezésre álló információt, és amint rendelkezésre állnak, a további információkat a későbbiekben indokolatlan késedelem nélkül meg kell adni.

1. az (EU) 2016/679 rendelet 34. cikke értelmében azon kötelezettség teljesítése, hogy indokolatlan késedelem nélkül tájékoztassa az érintettet a személyes adatok megsértéséről, amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.

**9.2 Az adatfeldolgozó által kezelt adatokkal kapcsolatos adatvédelmi incidens**

Az adatfeldolgozó által kezelt személyes adatokkal kapcsolatos adatvédelmi incidens esetén az adatfeldolgozó indokolatlan késedelem nélkül értesíti az adatkezelőt, azt követően, hogy az adatfeldolgozó tudomást szerzett az adatvédelmi incidensről. Az ilyen értesítés magában foglalja legalább a következőket:

1. az adatvédelmi incidens jellegének leírása (beleértve lehetőség szerint az érintettek és az érintett adatok kategóriáit és hozzávetőleges számát);
2. egy olyan kapcsolattartó pont adatai, ahol az adatvédelmi incidenssel kapcsolatban további információk szerezhetők be;
3. a valószínűsíthető következmények, valamint az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések ismertetése, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is.

Ha és amennyiben nem lehetséges egyidejűleg az összes információt megadni, a kezdeti értesítésnek tartalmaznia kell az akkor rendelkezésre álló információt, és amint rendelkezésre állnak, a további információkat a későbbiekben indokolatlan késedelem nélkül meg kell adni.

A Felek a III. mellékletben meghatározzák azt az összes egyéb elemet, amelyet az adatfeldolgozónak meg kell adnia, amikor segítséget nyújt az adatkezelőnek az (EU) 2016/679 Rendelet 33. és 34. cikke szerinti kötelezettségek teljesítésében.

**III. SZAKASZ ZÁRÓ RENDELKEZÉSEK**

***10. feltétel A feltételeknek való nem meg felelés és a szerződés felmondása***

1. Az (EU) 2016/679 rendelet bármely rendelkezésének sérelme nélkül, abban az esetben, ha az adatfeldolgozó megszegi az e szerződési feltételek szerinti kötelezettségeit, az adatkezelő utasíthatja az adatfeldolgozót, hogy függessze fel a személyes adatok kezelését mindaddig, amíg az adatfeldolgozó eleget nem tesz e feltételeknek, vagy a szerződés meg nem szűnik. Az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha bármilyen okból nem tud megfelelni ezeknek a feltételeknek.
2. Az adatkezelő jogosult a szerződés felmondására, amennyiben az személyes adatok e feltételek szerinti kezelésére vonatkozik, ha:
   1. az adatfeldolgozó általi adatkezelést az adatkezelő felfüggesztette az a) pont alapján, és ha észszerű időn belül, de legkésőbb a felfüggesztést követő egy hónapon belül nem áll helyre az e feltételeknek való megfelelés;
   2. az adatfeldolgozó súlyosan vagy tartósan megsérti ezeket a feltételeket vagy az (EU) 2016/679 rendelet szerinti kötelezettségeit;
   3. az adatfeldolgozó nem tesz eleget az illetékes bíróság vagy felügyeleti hatóság(ok) kötelező erejű határozatának az e feltételek vagy az (EU) 2016/679 rendelet szerinti kötelezettségei tekintetében.
3. Az adatfeldolgozó jogosult felmondani a szerződést, amennyiben a személyes adatok e feltételek szerinti kezelésére vonatkozóik, ha az adatkezelő – miután az adatfeldolgozó tájékoztatta az adatkezelőt arról, hogy utasításai sértik a 7.1. feltétel b) pontja szerinti, alkalmazandó jogi követelményeket – ragaszkodik az utasítások teljesítéséhez.
4. A szerződés megszűnését követően az adatfeldolgozó az adatkezelő választása szerint törli az adatkezelő nevében kezelt valamennyi személyes adatot, és igazolja az adatkezelő felé, hogy ezt megtette, vagy az összes személyes adatot visszaküldi az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog előírja a személyes adatok tárolását. Az adatok törléséig vagy visszaküldéséig az adatfeldolgozó továbbra is biztosítja az e feltételeknek való megfelelést.

I. MELLÉKLET

**A Felek listája**

**IMPORTŐR**

Cím: André Citroën utca 1, 1194 Budapest, Magyarország

A kapcsolattartó neve, beosztása és elérhetősége: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**MÁRKASZERVIZ**

Cím: xxxxxxxxxxxxxxxxxxxx

A kapcsolattartó neve, beosztása és elérhetősége: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

II. MELLÉKLET

**A különböző célok alapján kezelt adatkategóriák leírása és jogalapja.**

**1.**

|  |  |
| --- | --- |
| ***A kezelt ÜGYFÉL-Adatok kategóriái*** | * Azonosító adatok (pl. név, cím, e-mail cím) * Családi állapot (pl. családi állapot, egyéb családtagok) * Csatlakozási adatok (pl. felhasználói azonosító, jelszó) * Szakmai adatok (pl. funkció, pozíció a szervezetben – céges kapcsolattartó esetén) * Szokásokra és magatartásra vonatkozó adatok (pl. érdeklődési kör, utazásokkal és egyesületi tagsággal kapcsolatos adatok) * Személyazonosító adatok (pl. vezetői engedély, személyi igazolványszám, útlevélszám) * Gazdasági, vagyoni, pénzügyi és biztosítási adatok (pl. fizetés, kölcsönök, jelzáloghitelek, hitelek) * Banki adatok (pl. IBAN, betét/hitelkártya száma) * Jármű adatok (pl. alvázszám, a kapcsolt jármű adatai, alkatrészek és tartozékok műszaki adatai, gyártási státusz) * Kereskedelmi adatok (pl. számlázás, marketing) * Szerződéses adatok (pl. munkaszerződés, szállítási szerződés, MÁRKASZERVIZ szerződés) * Követelésekre vonatkozó adatok * Értékesítéssel és szolgáltatással kapcsolatos adatok (pl. szervizeltetés vagy új gépjármű vásárlás ténye, szervizeltetés esetén a munkalap felvételének dátuma és az igénybe vett márkaszerviz neve, új gépjármű vásárlása esetén a forgalomba helyezés dátuma és az igénybe vett márkakereskedés neve) * Szervizadatok   Ez különösen - de nem kizárólag - a következő adatelemeket tartalmazza:   * Kereszt- és vezetéknév * Nem * Születési idő * Születési hely/ország * Családi állapot * Adóazonosító * Lakcím * Személyes telefon/fax/mobilszám * Személyes e-mail cím * Munkakör * Munkáltató * Üzleti cím, részleg stb. * Üzleti e-mail cím * Üzleti telefon/fax/mobilszám * Jövedelem, adó és/vagy foglalkoztatással kapcsolatos juttatások * Bankszámla, betéti/hitelkártya adatai * Jelzálog és egyéb zálogjogok * Hiteltörténet és hitelreferencia-adatok * Kiadásokra vonatkozó információk vagy adatok * IP-cím * Felhasználói azonosító/CID * Rendszernaplók * A biztonsági kérdésekre adott válaszok, a kijelölt berendezések/szoftverek sorozatszámai * Helyadatok (pl. GPS) * Alvázszám * Képzettség (pl. önéletrajz) * Szokások * Klub- és egyesületi tagságok   Mint szervizadatok:   * Számla száma * Esemény dátuma * MÁRKASZERVIZ kódja * Rendszámtábla száma * Kilométeróra * Szervizelés típusa * Alkatrészek leírása   A beavatkozás adatai (nem alkalmazandó a csak potenciális Ügyfelekre):   * A beavatkozás dátuma * Számlaazonosító * A beavatkozás leírása * Költségviselés (ügyfél, garancia, biztosítás) * Alkatrészleírás * Alkatrészreferencia * Műveletleírás * Műveletkód |
| *A kezelt érzékeny adatok (adott esetben).* | A jelen AFM alapján a személyes adatok következő különleges kategóriái kerülnek kezelésre:   * Egészségügyi adatok (beleértve az egészségi állapotot, fogyatékosságokat, megbetegedéseket, betegségeket vagy orvosi kezeléseket), így különösen mozgáskorlátozottak részére átalakított gépjármű vagy egyéb támogatott gépjármű esetén |
| ***A MÁRKASZERVIZ alkalmazottai kezelt adatainak kategóriái*** | * Vezeték- és keresztnév * Munkakör * Munkáltató * Üzleti cím, részleg stb. * Üzleti e-mail cím * Személyes e-mail cím * Üzleti telefon/fax/mobilszám * Személyes telefon/fax/mobilszám * IP-cím * Felhasználói azonosító/CID * Rendszernapló * Elvégzett tréningek |

**ÜGYFÉL-Adatok**

Amennyiben az Adatokat olyan statisztikai célokra használják fel, amelyek eredményeként csak összesített adatok állnak rendelkezésre, a Feleknek olyan technikai vagy szervezési intézkedéseket kell hozniuk, mint például az anonimizálás. Valamennyi lehetséges alkalommal visszavonhatatlanul anonimizálni kell az Adatokat.

1. **A szerződéskötést megelőző és szerződéses kötelezettségek teljesítése/szerződés teljesítése és/vagy szerződéskötés (GDPR 6. Cikk (1) bekezdés b) pont)**

Amennyiben a személyes adatok felhasználása és/vagy kezelése szerződés, szerződéses kötelezettségek teljesítéséhez/megvalósításához és/vagy szerződéskötéshez szükséges, úgy az érintett Adatkezelő az ÜGYFÉL-Adatokat – különösen (de nem kizárólagosan) – az alábbiak szerint használhatja fel és kezelheti (az alábbi táblázat azon adatkezeléseket is tartalmazza, amelyek esetében az Autógyártó az adatkezelő, míg a Felek vagy azok valamelyike – az esetek többségében – adatfeldolgozó):

|  |  |  |  |
| --- | --- | --- | --- |
| **Cél(ok)** | **Adatkezelő(k)** | **Adatfeldolgozó(k)** | **Az adatkezelés tárgya, jellege** |
| Lead Menedzsment:  Felismerési folyamat (beazonosítás) | Importőr  MÁRKASZERVIZ | MÁRKASZERVIZ  / | A MÁRKASZERVIZ az Importőr adatbázisának felismerési célú lekérdezése céljából Adatfeldolgozó. |
| Járműütemezés és gyártás  Szállítás (gépjárművek, alkatrészek stb.)  Árvédelem biztosítása | MÁRKASZERVIZ  Importőr | / | Ezekre a célokra ez az AFM nem terjed ki. |
| Garanciafeldolgozás (beleértve a garancia meghosszabbítását). | Importőr  MÁRKASZERVIZ | / | Ezekre a célokra ez az AFM nem terjed ki. |
| A probléma-, panasz- és kérelemfeldolgozás, különösen a Stellantis csoport megfelelő segítségnyújtó/problémaelhárító központjai által. | Importőr  MÁRKASZERVIZ | / | Ezekre a célokra ez az AFM nem terjed ki. |
| Gépjárműszoftver- és hardverfrissítés | Autógyártó | MÁRKASZERVIZ | A frissítések elvégzését a MÁRKASZERVIZ bonyolítja le az Ügyfelei tekintetében |
| Marketingösztönzők, bónusz vagy egyéb programok adminisztrációja. | Importőr  MÁRKASZERVIZ | / | Ezekre a célokra ez az AFM nem terjed ki. |
| Ellenőrzések/adatvédelmi ellenőrzések és dokumentumellenőrzések adminisztrációja. | Autógyártó/Importőr  MÁRKASZERVIZ | / | Ezekre a célokra ez az AFM nem terjed ki. |
| (Alap) kapcsolt (connected) járműszolgáltatások | Autógyártó | MÁRKASZERVIZ  Importőr | Ezen szolgáltatások nyújtása tekintetében a MÁRKASZERVIZ és az Importőr támogatást nyújt az Autógyártó számára, így például az Ügyfélpanaszok továbbítása az Autógyártó felé. |
| Standard és opcionálisan kapcsolt (connected) járműszolgáltatások | Autógyártó | MÁRKASZERVIZ  Importőr | Ezen szolgáltatások nyújtása tekintetében a MÁRKASZERVIZ és az Importőr támogatást nyújt az Autógyártó számára. így például az Ügyfélpanaszok továbbítása az Autógyártó felé. |
| - Alkalmazás és weboldal szolgáltatások  - Helyalapú szolgáltatások nyújtása weboldalon/alkalmazáson keresztül, pl. közeli MÁRKASZERVIZ /képviselő, a legközelebbi MÁRKASZERVIZ /képviselőhöz vezető útvonal keresése. | Autógyártó | / | Ezekre a célokra ez az AFM nem terjed ki. |
| Adatvédelemmel kapcsolatos érintetti kérelmek teljesítése | Autógyártó  MÁRKASZERVIZ  Importőr | / | Ezekre a célokra ez az AFM nem terjed ki. |

1. **Jogi kötelezettségek (GDPR 6. Cikk (1) bekezdés c) pont):**

Amennyiben a személyes adatok felhasználása és/vagy kezelése jogi kötelezettségek teljesítéséhez szükséges, az érintett Adatkezelő az ÜGYFÉL-Adatokat - különösen (de nem kizárólagosan) - az alábbiak szerint használhatja fel és kezelheti:

|  |  |  |  |
| --- | --- | --- | --- |
| **Cél(ok)** | **Adatkezelő(k)** | **Adatfeldolgozó** | **Az adatkezelés tárgya, jellege** |
| Termékhiba/felelősség (a Minőségellenőrzéssel/ Minőségbiztosítással összefüggésben) és esetleges visszahívási kampányok. | Autógyártó | MÁRKASZERVIZ | A MÁRKASZERVIZ támogatást nyújt az Autógyártó számára, így különösen az Ügyfeleivel való ilyen tárgyú kommunikáció útján, valamint a javítás elvégzésével. |
| Az Európai Bizottság (EU) 2021/392 végrehajtási rendelete a CO2-kibocsátás nyomon követéséről. | Autógyártó | MÁRKASZERVIZ | A MÁRKASZERVIZ továbbítja az Autógyártó részére a gépjármű EU végrehajtási rendelet szerinti valós vezetési feltételek melletti adatait és a jármű-azonosító számát, amikor a jármű karbantartása vagy javítása esedékes, vagy más beavatkozásra kerül sor, és le kell olvasni a fedélzeti adatokat a jármű fedélzeti diagnosztikai soros portjáról. |

1. **Jogos érdek (GDPR 6. Cikk (1) bekezdés f) pont), kivéve, ha az ügyfél élt a tiltakozáshoz való jogával (GDPR 21. Cikk (1) bekezdés):**

Amennyiben az ÜGYFÉL-Adatok felhasználása és/vagy kezelése olyan tevékenységek elvégzéséhez szükséges, amelyek a mi mint üzleti vállalkozás jogos érdekében állnak, különösen (de nem kizárólagosan) - az alábbiak szerint:

|  |  |  |  |
| --- | --- | --- | --- |
| **Cél(ok)** | **Adatkezelő(k)** | **Adatfeldolgozó(k)** | **Az adatkezelés tárgya, jellege** |
| ÜGYFÉL-elégedettségi felmérések a termékekkel és szolgáltatásokkal kapcsolatban. | Importőr  MÁRKASZERVIZ | MÁRKASZERVIZ | A MÁRKASZERVIZ az általa felvett ügyféladatokat továbbítja az Importőr részére annak érdekében, hogy az Importőr ügyfélelégedettségi kérdőívet tudjon küldeni az érintetteknek és ügyfélelégedettségmérést tudjon végezni |
| A Minőségellenőrzéshez/ Minőségbiztosításhoz is kapcsolódó termék-, szolgáltatás- és minőségfejlesztés, helyszíni kampányok, utómunka kampányok, folyamatos termékfejlesztés (elhasználódásra, diagnosztikára és javításra vonatkozó információk). | Autógyártó | MÁRKASZERVIZ  Importőr | A MÁRKASZERVIZ és az Importőr támogatást nyújt az Autógyártó számára a cél szerinti feladatok elvégzésében, így különösen a releváns információk továbbításával az Autógyártó felé. |
| A termék minőségével kapcsolatos esetleges olyan szerviz kampányok, amelyek ajánlat nélkül csupán a termékhasználat javítására korlátozódnak. | Autógyártó | MÁRKASZERVIZ  Importőr | A MÁRKASZERVIZ és az Importőr támogatást nyújt az Autógyártó számára a cél szerinti feladatok elvégzésében, így különösen a releváns információk továbbításával az Autógyártó felé, illetve a szerviz elvégzésével. |
| Az ÜGYFÉL-Adatok Importőr és MÁRKASZERVIZ közötti kommunikációjának és továbbításának megkönnyítése és biztosítása érdekében CRM és/vagy egyéb vállalatirányítási rendszer biztosítása az Importőr által a MÁRKASZERVIZ részére | MÁRKASZERVIZ | Importőr | Az Importőr lehetővé teszi a MÁRKASZERVIZ  számára az importőri rendszerhez való adott mértékű hozzáférést és annak használatát. |

1. **Hozzájárulás (GDPR 6. Cikk (1) bekezdés a) pont)**

Amennyiben a hozzájárulás megadása megtörtént, az érintett Adatkezelők az alábbiak szerint használhatják és kezelhetik az ÜGYFÉL-Adatokat, kivéve, ha az ÜGYFÉL élt a hozzájárulás visszavonásához való jogával (GDPR 7. Cikk (3) bekezdés):

|  |  |  |  |
| --- | --- | --- | --- |
| **Cél(ok)** | **Adatkezelő(k)** | **Adatfeldolgozó(k)** | **Az adatkezelés tárgya, jellege** |
| Az Importőr marketingtevékenységei. | Importőr | MÁRKASZERVIZ | A MÁRKASZERVIZ az Importőr adatfeldolgozója az Importőr javára végzett marketing- vagy profilalkotási tevékenységekhez való ügyfélhozzájárulás gyűjtése és a fenti tevékenységek esetleges végrehajtása során. |
| Marketinginformációt tartalmazó felmérések. | Importőr  MÁRKASZERVIZ | MÁRKASZERVIZ  / | A MÁRKASZERVIZ az Importőr adatfeldolgozója az Importőr javára végzett ilyen marketing- vagy profilalkotási tevékenységekhez való ügyfélhozzájárulás gyűjtése és a fenti tevékenységek esetleges végrehajtása során. |
| Olyan profilalkotási célok, amelyek lehetővé teszik a kiválasztott adatkezelő számára, hogy felmérje az ügyfelek érdeklődését és viselkedését, elemezze és megjósolja az ügyfelek preferenciáit, és javítsa a Stellantis márkák termékeit és szolgáltatásait.  A profilalkotásra kizárólag az ügyfelet érintő joghatásokat eredményező vagy őt hasonlóképpen jelentősen érintő automatizált döntéshozatal nélkül kerül sor. | Importőr  MÁRKASZERVIZ | MÁRKASZERVIZ | A MÁRKASZERVIZ az Importőr adatfeldolgozója az Importőr javára végzett ilyen profilalkotási tevékenységekhez való ügyfélhozzájárulás gyűjtése és a fenti tevékenységek esetleges végrehajtása során. |
| A MÁRKASZERVIZ marketingtevékenységei | MÁRKASZERVIZ | Importőr | Az Importőr a MÁRKASZERVIZ adatfeldolgozója akkor, amikor az Importőri rendszeren belül rögzíti a MÁRKASZERVIZ számára adott Ügyfél marketinghozzájárulásokat, illetve továbbítja azokat a MÁRKASZERVIZ számára. |
| A MÁRKASZERVIZ profilalkotó tevékenységei | MÁRKASZERVIZ | / | Ezekre a célokra ez az AFM nem terjed ki. |

**A MÁRKASZERVIZ Alkalmazottainak Adatai**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cél(ok)** | **Adatkezelő(k)** | **Adatfeldolgozó(k)** | **Az adatkezelés tárgya, jellege** |
| A MÁRKASZERVIZ-MEGÁLLAPODÁS-ban említett tevékenységekhez rendelkezésre bocsátott rendszerekhez (eszközökhöz) való hozzáférés biztosítása. | MÁRKASZERVIZ | Autógyártók és Importőr | Az Autógyártó és Importőr lehetővé teszi a MÁRKASZERVIZ számára ezen rendszer(ek)hez való adott mértékű hozzáférést és annak használatát. |
| Tanfolyam/tréning tevékenységek | MÁRKASZERVIZ  Importőr | / | Az Importőr ezeket az adatokat az adott tréning lebonyolítása, illetve a bónusz- és egyéb, a kereskedelem politikában meghatározott feltételeknek való megfelelés ellenőrzése érdekében kezeli. |
| Felmérési tevékenységek | Autógyártó | MÁRKASZERVIZ | A MÁRKASZERVIZ támogatást nyújt az Autógyártó számára a cél szerinti feladatok elvégzésében, így különösen a felérés Autógyártó számára való elvégzésében. |

1. **Adatmegőrzési Szabályok**

* **A szerződéses kötelezettség végrehajtása / teljesítése** céljából kezelt Adatokat a polgári jogi elévülési időhöz igazodva a szerződéses jogviszony megszűnésétől számított 5 évig tároljuk. Az Adatok azonban hosszabb ideig is tárolhatók potenciális és/vagy tényleges követelések, valamint ebből eredő kötelezettségek és/vagy egyéb kötelező jogszabályi megőrzési követelmény és/vagy tárolási kötelezettség esetén.
* **A marketing és profilalkotás** céljából kezelt ÜGYFÉL-Adatokat az adatkezelők az érintett hozzájárulásának visszavonásáig őrizik meg.
* **A jogszabályi kötelezettségek teljesítése** érdekében kezelt ÜGYFÉL-Adatok a jogszabályok által előírt ideig kerülnek megőrzésre.
* **Az ügyfélelégedettségi felmérések** céljából kezelt ÜGYFÉL-Adatok 6 hónapig őrizhetők meg.
* **Minden egyéb esetben az Adatok az adott cél eléréséhez feltétlenül szükséges ideig kezelhetők**. Az Adatfeldolgozó köteles az Adatkezelő mindenkori, hatályban lévő adatkezelési tájékoztatója szerinti maximális adatkezelési időtartamot betartani az adott cél szerinti adatkezelési tevekénysége vonatkozásában.

III. MELLÉKLET

**Technikai és szervezési intézkedések, beleértve az adatok biztonságát biztosító technikai és szervezési intézkedéseket**

Az Adatfeldolgozó (és annak bármely aladatfeldolgozója) a jelen AFM a MEGÁLLAPODÁS szerint történő végrehajtása során vállalja, hogy megfelel az alábbi Információbiztonsági Irányelvnek és annak mellékleteinek ("IBI"). A jelen dokumentum az Adatkezelő és az Adatfeldolgozó tulajdonában lévő rendszerekre vonatkozó biztonsági intézkedésekre vonatkozik.

**A blue and black logo

Description automatically generated**

**Információbiztonsági Irányelv (IBI)**  
**KÜLSŐ BESZERZÉS**

**VERZIÓELŐZMÉNYEK**

|  |  |  |
| --- | --- | --- |
| **Verzió** | **Dátum** | **Változások** |
| 1.0 | 2009 JANUÁR | A dokumentum első változata |
| 2.0 | JANUÁR 2010 | Ez a verzió új biztonsági követelményeket kap |
| 3.0 | 2010 JÚLIUS | Ez a verzió új biztonsági szolgáltatásokat kap |
| 4.0 | 2011 NOVEMBER | Ez a verzió új biztonsági szabványt kap |
| 4.1 | 2015 JÚLIUS | Ez a verzió új Cégnevet és új logót kap |
| 5.0 | 2020 FEBRUÁR | Ez a verzió új sablonokat kap és megfeleltetésre kerül a nemzetközi szabványnak |
| 5.0s | 2022 ÁPRILIS | Ez a verzió új Cégnevet és új logót kap |

**TARTALOM**

[1. Áttekintés 16](#_Toc150788278)

[2. Alkalmazhatóság 16](#_Toc150788279)

[3. Biztonságpolitika kivételek 16](#_Toc150788280)

[4. A jelen dokumentum által lefedett rendszertípusok 17](#_Toc150788281)

[5. Információbiztonsági politikák 17](#_Toc150788282)

[6. Az információbiztonság megszervezése 17](#_Toc150788283)

[7. Humánerőforrás-biztonság 18](#_Toc150788284)

[8. Eszközkezelés 18](#_Toc150788285)

[8.1. Hordozható Adathordozók 18](#_Toc150788286)

[9. Hozzáférés-ellenőrzés 18](#_Toc150788287)

[10. Kriptográfia 19](#_Toc150788288)

[11. Fizikai és környezeti biztonság 19](#_Toc150788289)

[12. Műveletbiztonság 20](#_Toc150788290)

[12.1. Védelem Rosszindulatú Szoftverek ellen 20](#_Toc150788291)

[12.2. Keményítés 21](#_Toc150788292)

[12.3. Állandó Biztonsági & Sértetlenségi folyamat 21](#_Toc150788293)

[13. Hálózatbiztonság 21](#_Toc150788294)

[14. Rendszer Beszerzése, Fejlesztése és Karbantartása 22](#_Toc150788295)

[15. Szolgáltatói kapcsolatok kezelése 22](#_Toc150788296)

[16. Információbiztonsági incidenskezelés 23](#_Toc150788297)

[17. Az üzletmenet-folytonossági menedzsment információbiztonsági szempontjai 23](#_Toc150788298)

[18. Biztonsági megfelelés 23](#_Toc150788299)

[18.1. Biztonsági Tesztek 24](#_Toc150788300)

[A. melléklet: Ellenőrzések 25](#_Toc150788301)

[B. melléklet: Felhő-ellenőrzések 30](#_Toc150788302)

[C. melléklet: Adatvédelmi ellenőrzések 32](#_Toc150788303)

# 

# Áttekintés

A jelen dokumentum (IBI) tartalmazza és részletezi azokat a kölcsönösen elfogadott biztonsági szabályokat, melyeket a SZOLGÁLTATÓ biztonsági szempontból köteles elfogadni.

Leírja azokat a Szolgáltatások nyújtásához kapcsolódó, elfogadott biztonsági szabályokat:

* 1. amelyekhez a SZOLGÁLTATÓ eltérő rendelkezés hiányában, szükség esetén a jelenleg nyújtott valamennyi Szolgáltatást hozzáigazítja;
  2. amelyek mellett a SZOLGÁLTATÓ valamennyi Új Szolgáltatásot nyújt.

A SZOLGÁLTATÓ a Szolgáltatások keretében Biztonsági Megoldásokat kutat, vizsgál, tesztel és valósít meg, ideértve többek között a tűzfalakat, titkosító kártyákat, behatolásérzékelő szoftvereket, hitelesítő eszközöket, felhasználói adatbázis-kezelést, valamint a rendszerek és az adatbázisok keményítését.

A SZOLGÁLTATÓ felelős azért, hogy a biztonsági szabályok megfeleljenek azoknak a jogszabályoknak és szabályozásoknak, amelyekről IT SZOLGÁLTATÓ-i minőségében a szokásos gondossággal eljárva tudnia kellene. Az Ügyfél felel a biztonsági szabályok rá vonatkozó jogszabályoknak, szabályozásoknak és munkaszerződéseknek, valamint minden egyéb, e bekezdés szerint nem a SZOLGÁLTATÓ felelősségi körébe tartozó jogszabálynak, szabályozásnak és munkaszerződésnek való megfeleléséért.

# Alkalmazhatóság

|  |
| --- |
| **Célkitűzés:** A SZOLGÁLTATÓ Szolgáltatásainak, Ügyfeleinek, eszközeinek és alkalmazottainak védelmét szolgáló biztonsági gyakorlatok és eljárások kialakítása.  **Hatály:** Ez a dokumentum alapként szolgál a SZOLGÁLTATÓ és az Ügyfél által elfogadott biztonsági követelmények meghatározására és dokumentálására.  **Megfelelés:** A jelen iránymutatásnak való globális megfelelés a SZOLGÁLTATÓ és az Ügyfél általi jóváhagyást követően az Audit ellenőrzés tárgyát képezi.  **Célpont:** Valamennyi STELLANTIS vállalat és leányvállalat; beleértve a korábbi FCA, PSA, Opel leányvállalatokat is. |

Az A. Melléklet tartalmazza azoknak a Biztonsági Követelmények taxatív listáját, amelyeknek a SZOLGÁLTATÓ köteles megfelelni a Szolgáltatások és Alkalmazások nyújtása során, a jelen dokumentumban foglalt elveknek megfelelően.

A Felhőinfrastruktúrán alapuló Szolgálatások esetében a SZOLGÁLTATÓ az A. Melléklet szerinti felel valamennyi Biztonsági Követelményért, és a B. Melléklet szerint felel a Felhőszolgáltatások biztonságáért.

Az Adatvédelmi Információkat (PII) kezelő Szolgáltatások esetében a SZOLGÁLTATÓ az A. melléklet szerinti felel valamennyi Biztonsági Követelményért, és a C. melléklet szerinti felel Adatvédelmi és Biztonsági szabályokért.

A Felhőinfrastruktúrában kezelt Adatvédelmi Információkat (PII) kezelő Szolgáltatások esetében a Szolgáltató az A. melléklet szerinti felel valamennyi Biztonsági Követelményért, és a B. és C. mellékletek szerinti felel az Felhőszolgáltatásra is kiterjedő Adatvédelmi és Biztonsági szabályokért.

Eltérő megállapodás hiányában a jelen dokumentum az Időtartam hátralevő részében érvényes és hatályos.

# Biztonságpolitika kivételek

A korrekciós tervnek megfelelő biztonsági szabályok végrehajtása a technikai megvalósíthatósági és a Változáskezelési Folyamat függvénye. A SZOLGÁLTATÓ dokumentálja az Ügyfél irányába az alkalmazhatatlanság okát, és elvégez egy Kockázatelemzési és Elfogadási eljárást.

**Az Alkalmazás rendellenes működése** miattvégre nem hajtható biztonsági szabályok esetében a következőket kell figyelembe venni:

az alkalmazást az ÜGYFÉL kezeli, az ÜGYFÉL felelős az alkalmazás módosításáért, és a Kockázatelemzési és Elfogadási folyamat elvégzéséért.

az alkalmazást a SZOLGÁLTATÓ fejleszti és kezeli:

* 1. amennyiben az alkalmazás kifejlesztésekor az IBI verzióban meghatározott biztonsági követelményeket NEM alkalmazták, akkor a SZOLGÁLTATÓ felel ennek a megváltoztatásáért;
  2. amennyiben az alkalmazás fejlesztésekor az IBI verzióban meghatározott biztonsági követelmények alkalmazásra kerültek, úgy az ÜGYFÉL választása szerint Kockázatelemzési és Elfogadási folyamaton mehet át vagy kezdeményezheti az alkalmazás legújabb IBI verziónak megfelelő frissítését;
  3. mennyiben az IBI verzióban meghatározott biztonsági követelményeket az alkalmazás fejlesztésekor már alkalmazták, azonban az IBI irányelvek a SZOLGÁLTATÓ felelősségi körén kívül eső okból nem alkalmazhatók, úgy ÜGYFÉL választása szerint Kockázatelemzési és Elfogadási folyamaton mehet át vagy kezdeményezheti az alkalmazás legújabb IBI verziónak megfelelő frissítését.

**Személyzetre vonatkozó hivatkozások**

A jelen dokumentumban az Ügyfél kifejezés az Ügyfél alkalmazottjaira és az Ügyfél számára munkát végző vállalkozókra vagy alvállalkozókra is vonatkozik.

A jelen dokumentumban a SZOLGÁLTATÓ kifejezés a SZOLGÁLTATÓ alkalmazottjaira és a SZOLGÁLTATÓ számára munkát végző vállalkozókra vagy alvállalkozókra is vonatkozik.

# A jelen dokumentum által lefedett rendszertípusok

A jelen dokumentum határozza meg a SZOLGÁLTATÓ által az ÜGYFÉL számára támogatott rendszertípusok biztonsági szabályait. A jelen irányelv hatálya alá tartozó rendszertípusokat az alábbi táblázat határozza meg. Felhívjuk a figyelmet arra, hogy a különböző rendszertípusokhoz eltérő szabályok is meghatározhatók. Ilyen esetben, vagy duplikálja a következő szakaszok megfelelő táblázatait, vagy adjon hozzá címkéket a táblázatok bejegyzéseihez a különböző típusú rendszerek szabályainak azonosítása érdekében.

|  |  |  |
| --- | --- | --- |
| **A jelen Dokumentum Által Lefedett Rendszerek/Szerverek típusai** (P = Elsődleges, A = Másodlagos) | **SZOLGÁLTATÓ** | **STELLANTIS** |
| A SZOLGÁLTATÓ részére adandó tájékoztatás a SZOLGÁLTATÓ által kezelt rendszerek/szerverek helytelen besorolásáról. | **A** | **P** |

A jelen Dokumentum által lefedett Rendszerek/Szerverek típusai:

* Gyártás
* Rendszer/Elfogadási teszt
* Fejlesztés (\*)
* Teszt (\*)

(\*) az Ügyféllel egyeztetve másfajta szabályok alkalmazása is lehetséges.

# Információbiztonsági politikák

A SZOLGÁLTATÓ köteles:

* biztonsági szabályzatokat, folyamatokat és eljárásokat kidolgozni és végrehajtani;
* megfelelni a STELLANTIS Biztonsági Szabályzatában foglaltaknak;
* dokumentumokkal igazolni az Ügyfél vagy egy külső fél, például egy ellenőr részére, hogy a szabályzatokat, folyamatokat és eljárásokat teljes mértékben végrehajtották.

# Az információbiztonság megszervezése

A Szolgáltatónak a munkaköröket és szerepköröket a Feladatok Szétválasztásának (SoD) elvével összhangban kell megterveznie és végrehajtania.

Ha a csökkentett létszám miatt az SoD nem lehetséges, akkor kiegyennlítő ellenőrzési tevékenységként részletes irányításfelügyeleti és ellenőrzési tevékenységet kell végezni.

Az információbiztonsággal már tervezési szakaszban foglalkozni kell, függetlenül attól, hogy milyen típusú projektben vesz részt az ÜGYFÉL INFORMÁCIÓBIZTONSÁGI FŐTISZTVISELŐJE.

# Humánerőforrás-biztonság

A SZOLGÁLTATÓ ÜGYFÉL-lel kapcsolatban álló alkalmazottainak megfelelő biztonságtudatossági oktatásban és képzésben kell részesülniük, valamint munkakörüknek megfelelően rendszeresen értesülniük kell a legfrissebb szervezeti szabályzatokról és eljárásokról.

A SZOLGÁLTATÓ formalizált és dokumentált Személyzetbiztonság Szabályzatot dolgoz ki a szerepek, a felelősségi körök, a menedzsment elkötelezettség és a koordináció szabályozása érdekében. Ezen szabályzatot kérésre az ÜGYFÉL rendelkezésére bocsátják.

# Eszközkezelés

A SZOLGÁLTATÓ köteles:

* a biztonsági szint igazolása érdekében architektúra - és információs rendszer-tanúsítást végezni;
* az Eszközök legmagasabb szintű védelmét megvalósítani és garantálni, ideértve többek között a beszerzési gyakorlatok meghatározását, a változások kezelését, az ellopott és elveszett eszközök kezelését és a kivezetésikövetelményeket is.

Teljesen kiszervezett szállítás esetén az eszközöket a STELLANTIS Biztonsági Szabályzatainak megfelelően kell kezelni.

## Hordozható Adathordozók

A Hordozható Adathordozók közé tartoznak a mágnesszalagok, optikai lemezek, Flash eszközök és kazetták. A hordozható adathordozók gondnoka olyan személy, aki más személyek nevében felelősséget vállalt a hordozható adathordozók tárolásáért.

A Hordozható Adathordozók csak a következőkre használhatók:

* üzleti feldolgozáshoz történő rutinszerű fel- és lecsatlakoztatás, vagy
* az iratok megőrzése szempontjából lényegesnek minősített információkat tárolása, vagy
* összeomlás utáni helyreállítás szempontjából lényegesnek ítélt információk tárolása.

Ezért lehetővé kell tenni, hogy az adathordozók mozgását és ellenőrzését a gondnok adathordozó-nyilvántartásában nyomon követhető legyen.

Megjegyzés: A gyorsan cserélhető adathordozók fix lemeznek minősülnek, ezért a többi rendszerelemmel megegyező módon kezelendők.

A különleges/jogszabályon alapuló személyes adatokat tartalmazó hordozható adathordozókat más, az ilyen adatok kezelésére nem jogosult felhasználó csak akkor használhatja újra, ha azokat olvashatatlanná tették.

# Hozzáférés-ellenőrzés

A SZOLGÁLTATÓ a következő Rendszergazda Szolgáltatásokat nyújtja:

1. a hozzáférési szabályzatok és eljárások elemzése, tervezése és végrehajtása;
2. felhasználói profil adatbázis kezelése (létrehozás, törlés, frissítés);
3. a felhasználói hozzáférési követelmények kezelése.

A rendszergazda szintű hozzáférés csak erős hitelesítéssel biztosítható. A hálózatokhoz vagy a hálózatok egyes részeihez való hozzáférés csak erős hitelesítéssel engedélyezhető. Erős hitelesítés hiányában kizárólag bizonyos gépekhez való meghatározott, nem rendszergazda szintű hozzáférést lehet biztosítani.

A SZOLGÁLTATÓ olyan információbiztonsági megközelítést alkalmaz, amely forrás-tulajdonosi koncepciót követ a biztonság, a tulajdonosok tanúsítása és a számítógép-felhasználók engedélyezett hozzáférésének időszakos felülvizsgálata tekintetében.

A SZOLGÁLTATÓ köteles:

1. fél évente vagy kérésre (reaktiválás céljából) felülvizsgálni és az ÜGYFÉL rendelkezésére bocsátani az ÜGYFÉL rendszerbébe való bejelentkezési azonosítók listáját;
2. fél évente (reaktiválás céljából) felülvizsgálni és ellenőrzi a rendszerbe való bejelentkezési azonosítókat a SZOLGÁLTATÓ azon személyzete tekintetében, akiknek már nincs üzleti igénye és/vagy akiknek a vezetőség a továbbiakban nem engedélyezte a rendszerhez való hozzáférést;
3. haladéktalanul törölni azon személyek SZOLGÁLTATÓ-i azonosítóit, akiknek már nincs üzleti igénye és/vagy akik számára a vezetőség a továbbiakban nem engedélyezte a rendszerekhez való hozzáférést;
4. az ÜGYFÉL által megadott információk alapján törölni az ÜGYFÉL azon személyekre vonatkozó bejelentkezési azonosítóit, akiknek már nincs üzleti igénye és/vagy akik számára a vezetőség a továbbiakban nem engedélyezte a rendszerhez való hozzáférést;
5. biztosítani a hozzáférés-ellenőrző szoftver azon funkcióit és jellemzőit, amelyek megfelelnek az ÜGYFÉL jelen dokumentumban meghatározott biztonsági gyakorlatának;
6. megvalósítani a támogatott operációs rendszerek azon biztonsági rendszerértékeit és jellemzőit, amelyek megfelelnek az ÜGYFÉL jelen dokumentumban meghatározott biztonsági gyakorlatának;
7. meghatározni a Szolgáltatások körébe tartozó operációs rendszer- és alkalmazás-források védelmi követelményeit;
8. végrehajtani az operációs rendszer és az alkalmazások forrásaihoz való jogosulatlan hozzáférés megakadályozására szolgáló védelmi követelményeket;
9. rögzíteni és a közösen megállapított megőrzési időszak alatt megőrizni az audit nyilvántartásokat, és kérésre jelentést készíteni az ÜGYFÉL számára;
10. létrehozni, módosítani, deaktiválni és eltávolítani az ÜGYFÉL és a SZOLGÁLTATÓ személyzetének bejelentkezés-azonosítóit és kapcsolódó hozzáférési jogosultságait;
11. visszaállítani és átadni az arra jogosult személyzetnek az ÜGYFÉL és a SZOLGÁLTATÓ személyzetének bejelentkezés-azonosító jelszavait;
12. felülvizsgálni, jóváhagyni és engedélyezi a privilegizált felhasználói jogosultságok iránti kérelmeket;
13. rendszeresen felülvizsgálni a privilegizált felhasználói jogosultságokat, és eltávolítani azokat, amelyekhez már nincs vezetői engedély;
14. hozzáadni, módosítani és törölni a betárcsázási szolgáltatásokhoz való felhasználói hozzáférést;
15. koordinálni a jelszóváltoztatásokat. Az ÜGYFÉL jóváhagyásától függően a SZOLGÁLTATÓ felel az összes helyi jelszó szükség szerinti megváltoztatásáért és teszteléséért.

Az ÜGYFÉL köteles:

* évente (újrahitelesítés céljából) felülvizsgálni és ellenőrizni az ÜGYFÉL személyzetének bejelentkezési azonosítóit, és értesíti a SZOLGÁLTATÓT, hogy törölje azon személyek azonosítóit, akiknek már nincs üzleti szükségük és/vagy akiknek a vezetőség a továbbiakban nem engedélyezte a rendszerhez való hozzáférést;

# Kriptográfia

A kriptográfiai funkciók - a szükséges biztonság erősségétől függően változó hosszúságú kriptográfiai kulcsok alkalmazásával - az egyszerű szöveges információt titkosított szöveggé alakítják át. Mind a Titkos, mind a Nyilvános/Magánkulcsos kriptográfia esetében létezniük kell olyan kezelési technikáknak, amelyekkel a kriptográfiai kulcsok életciklusát - például létrehozását, terjesztését, érvényesítését, frissítését, tárolását, használatát és lejáratát – kezelni lehet.

A SZOLGÁLTATÓ köteles:

* 1. az iparágban elfogadott algoritmusok és eljárások alkalmazásával titkosítani valamennyi legalább bizalmasnak minősített ÜGYFÉL-adatot;
  2. az iparágban elfogadott algoritmusok és eljárások alkalmazásával a továbbítás során valamennyi ÜGYFÉL-adatot;
  3. a kriptográfiai kulcsok megfelelő kezelésére szolgáló eljárást létrehozni.

# Fizikai és környezeti biztonság

A fizikai biztonság alatt az ÜGYFÉL Adathordozói és Eszközei Fizikai integritásának fenntartására irányuló intézkedések és tevékenységek értendők.

A SZOLGÁLTATÓ köteles:

1. az ÜGYFÉL Létesítményeiben az ÜGYFÉL - közös megegyezés szerinti - fizikai biztonsági szabályzatainak, szabványainak és eljárásainak megfelelni;
2. a SZOLGÁLTATÓ (beleértve a vállalkozóit és alvállalkozóit is) Adatközpontjainál, beleértve a nyilvános Felhőszolgáltatókat:
   1. a Fizikai biztonsági előírások végrehajtásához megfelelő felszerelést (pl. beléptetés-ellenőrzés, tűzjelző) biztosítani;
   2. a biztonsági előírások megsértésének naplózására, riasztására és jelentésére vonatkozó eljárásokat megállapítani;
   3. rendszeres időközönként felülvizsgálni azokat az adatfeldolgozási területeket, amelyekért a SZOLGÁLTATÓ biztonsági felelősséggel tartozik, beleértve a hozzáférési bejelentkezések szokatlan eseményeinek felülvizsgálatát, és a jelen dokumentumban meghatározott eljárásokkal összhangban nyomonkövetési tevékenységeket végezni;
   4. védeni az illetéktelen hozzáféréstől a SZOLGÁLTATÓ telephelyén lévő LAN-szervereket és az infrastruktúra eszközeit;
   5. a SZOLGÁLTATÓ ellenőrzése alatt álló nyomtatott kiadványokat a jogosulatlan hozzáféréstől védő szabályokat kialakítani; és
   6. biztosítani a SZOLGÁLTATÓ ellenőrzése alatt álló cserélhető adathordozók biztonságos tárolását.
3. a berendezés leszerelésekor a SZOLGÁLTATÓ a berendezést egy központi helyre szállítja, ahol megtisztítja az (rögzített vagy cserélhető) adathordozókat a védett adatok minden nyomától.

## 

# Műveletbiztonság

A SZOLGÁLTATÓ a következő szolgáltatások nyújtására köteles:

* 1. naplók elérhetősége és közzététele;
  2. a rendszer naplófájljainak behatolás és rosszindulatú tevékenység nyomai után kutató elemzése;
  3. a hozzáférési kivételek (pl. szuperfelhasználók) naplózása ellenőrzési nyomvonal készítése céljából, és kérésre az ilyen adatok az ÜGYFÉL rendelkezésére bocsátása;
  4. azonosított biztonsági kockázatokkal kapcsolatos tanácsadás és az ilyen kockázatok minimalizálására ajánlott eljárásokra és intézkedésekre vonatkozó javaslattétel az ÜGYFÉL-nek; a rendszerek biztonsági szintjének behatolási támadások révén való tesztelése a lehetséges hibapontok felkutatása érdekében, az egyes Ügyfelekre szabott megoldások és termékek tesztelésére és a biztonsági kockázatok értékelésére szolgáló különleges környezetek felhasználásával;
  5. a fejlesztési, tesztelési és üzemeltetési létesítmények egymástól való elkülönítése szükséges az operatív rendszerhez való illetéktelen hozzáférés vagy az operatív rendszer megváltoztatása kockázatának csökkentése érdekében;
  6. a szervezet, az üzleti folyamatok, az információfeldolgozó létesítmények és rendszereket érintő valamennyi változás ellenőrzése;
  7. az források felhasználásának figyelemmel kísérése, és a szükséges rendszerteljesítmény biztosítása érdekében jövőbeni kapacitásigények előjelzése;
  8. az információkról, a szoftverekről és a rendszerképekről biztonsági másolatok készítése, és azok rendszeresen tesztelése az elfogadott biztonsági mentésre vonatkozó szabályzattal összhangban;
  9. az információs rendszerek műszaki sérülékenységéről megfelelő időközönként értékelés készítése, az ilyen sérülékenységeknek való kitettséget értékelése, és a kapcsolódó kockázat kezelésére megfelelő intézkedések megtétele.

### 

## Védelem Rosszindulatú Szoftverek ellen

A SZOLGÁLTATÓ köteles:

* 1. rosszindulatú szoftverek elkerülését, felismerését és szoftveres eltávolítását biztosítani olyan Gépek számára, amelyeknek szükségük van és képesek a rosszindulatú szoftverek elleni programok futtatására;
  2. reagálni a rosszindulatú szoftverek támadásaira és az észlelésnek megfelelőenkorrekciós intézkedéseket kezdeményezni a rosszindulatú szoftverek eltávolítása érdekébe;
  3. tájékoztatni az ÜGYFEL-et a nem helyreállítható rosszindulatú szoftverfertőzésekről;
  4. ellenőrizni, hogy az összes Támogatott Szerveren a legfrissebb rosszindulatú szoftverek Aláíró Fájljai vannak-e telepítve;
  5. automatikusan telepíteni a legújabb termékeket és mintákat a Támogatott Munkaállomásokon;
  6. rendszeresen jelentést készíteni az ÜGYFÉL-nek a telepített frissítések és a minták hatékonyságának igazolása érdekében;
  7. időszakos biztonsági állapotfelméréseket végezni az alábbiak validálása érdekében:
     1. hozzáférés-szabályozási beállítások,
     2. privilegizált felhasználók,
     3. az operációs rendszer erőforrásainak védelme,
     4. a rosszindulatú szoftvereket ellenőrző programok telepítése és működtetése a megfelelő platformokon.

### 

## Keményítés

A SZOLGÁLTATÓ köteles:

* + értékelni a kritikus szerverbiztonságot és amennyiben alkalmazandóokat,, fokozott Biztonsági Megoldás "keményítés"-t végezni;
  + a különböző szerverplatformok számára "keményítés"-i szabályzatokat meghatározni;
  + megszerezni az ÜGYFÉL "keményítés"-i szabályzatokra vonatkozó jóváhagyását; és
  + a gépekre vonatkozó "keményítés"-i szabályzatoknak megfelelő fokozott biztonsági "keményítés"-t végrehajtani.

## Állandó Biztonsági & Sértetlenségi folyamat

A SZOLGÁLTATÓ köteles:

* + Állandó Biztonsági/Sértetlenségi Tanácsadási Folyamatot (Rendszer, Hálózat és Folyamatok) alkalmazni a Biztonsági kérdések és kockázatok elemzése érdekében;
  + a folyamat eredményeit tartalmazó dokumentumokat készíteni; és
  + a jelen dokumentumban meghatározott irányelveknek megfelelően közölni az eredményeket az ÜGYFÉLLEL.

# Hálózatbiztonság

A SZOLGÁLTATÓ köteles:

* 1. kezelni és fenntartani valamennyi a SZOLGÁLTATÓ és az ÜGYFÉL Adathálózatát összekötő és a szolgáltatások nyújtásához szükséges tűzfalat és átjáró készüléket;
  2. hálózatbiztonsági szabályokat menedzselni és fenntartani;
  3. megvalósítani és módosítani TCP/IP hálózatok konfigurációját;
  4. tűzfal-struktúrákat tervezni;
  5. az ÜGYFÉL biztonsági követelményeinek megfelelően beállítani és konfigurálni a Tűzfalat; és
  6. a Tűzfalhoz való hozzáférés engedélyezését úgy kezelni, hogy a konfigurációs módosítások nem befolyásolják szokásos Szolgáltatási Szint-Megállapodásokat;
  7. bevezetni egy gyanús tevékenységeket figyelő rendszert (pl. IDS/IPS);
     1. amennyiben a hálózat-alapú védelem technikailag nem valósítható meg meg (pl. nyilvános felhőkörnyezet), úgy az ilyen típusú gyanús viselkedés azonosítására hoszt-alapú védelmet (hoszt-tűzfalak és hoszt-IDS) kell telepíteni és konfigurálni;
  8. bármely, az Internetnek kitett komponens esetében beállítani és konfigurálni egy Webes Alkalmazás Tűzfalat (WAT) és az Elosztott Szolgáltatásmegtagadással járó Támadás elleni (anti-DDoS) komponenseket.

# Rendszer Beszerzése, Fejlesztése és Karbantartása

A SZOLGÁLTATÓ köteles:

* 1. Biztonsági Megoldásokat kutatni, felülvizsgálni, tesztelni és végrehajtani, beleértve többek között a tűzfalakat, titkosító kártyákat, behatolásérzékelő szoftvereket, hitelesítési eszközöket, felhasználói adatbázis-kezelést, valamint a rendszerek és az adatbázisok keményítését;
  2. Az ÜGYFÉL INFORMÁCIÓBIZTONSÁGI FŐTISZTVISELŐ-je által jóváhagyandó biztonságos rendszer- és hálózati architektúrát tervezni, megtervezni és megvalósítani;
  3. Az ÜGYFÉL kérésére:
  4. Segíteni az ÜGYFEL-et az ÜGYFÉL biztonsági követelmények meghatározásában, a kockázatok értékelésében, valamint a biztonsági mentési és helyreállítási követelmények meghatározásában;
  5. Amennyiben a SZOLGÁLTATÓ szoftverfejlesztést és/vagy -karbantartást végez, úgy a következő szabályokat alkalmazni:
  6. A rendszereknek a fejlesztési cikluson belüli módosításait formális módosítás-ellenőrzési eljárások alkalmazásával szükséges ellenőrizni;
  7. A biztonsági rendszerek tervezésének elveit szükséges meghatározni, dokumentálni, fenntartani és alkalmazni valamennyi információs rendszer bevezetésére irányuló erőfeszítés során;
  8. Biztonságos fejlesztési környezetet biztosítani;
  9. Rendszertesztelést végezni;
  10. a Vizsgálati adatokat gondosan kiválasztani, védeni és ellenőrizni.

# Szolgáltatói kapcsolatok kezelése

A SZOLGÁLTATÓ köteles:

1. kijelölni egy a napi szintű biztonsági irányításért felelős Központot;
2. támogatni az ÜGYFEL-et a biztonsági audit során;
3. támogatni az ÜGYFÉL INFORMÁCIÓBIZTONSÁGI FŐTISZTVISELŐ-jét az időszakos Biztonsági Audit végén létrehozandó Jelentés elkészítésében. Ez a jelentés azonosítja egy rendszer, egy hálózat vagy egy szervezet sérülékenységeit. A jelentés az üzleti szükséglet követelménye szerint lehet informális vagy formális is;
4. támogatni az ÜGYFÉL INFORMÁCIÓBIZTONSÁGI FŐTISZTVISELŐ-jét a Biztonságfejlesztési Terv elkészítésében. Ez egy olyan, a Biztonsági Auditról készített Jelentést kiegészítő jelentés, amely részletesen ismerteti a szervezet biztonságának fokozásához szükséges fejlesztések;
5. tájékoztatni az ÜGYFEL-et minden újonnan észlelt sérülékenységről (megállapodás szükséges a Függelékkel kapcsolatban);
6. értesíteni az ÜGYFEL-et a SZOLGÁLTATÓ belső biztonsági szabályzatáról;
7. tájékoztatni az ÜGYFEL-et a SZOLGÁLTATÓ belső biztonsági folyamatáról és szervezetéről;
8. elkülöníteni az ÜGYFÉL és más Ügyfelek rendszereit, ellenkező esetben a SZOLGÁLTATÓ-nak az ÜGYFÉL INFORMÁCIÓBIZTONSÁGI FŐTISZTVISELŐ-jének írásbeli engedélyét kell kérnie;
9. ellenőrizni, hogy minden folyamat és új implementáció megfelel-e az ÜGYFÉL biztonságpolitikájának;
10. a jelen dokumentummal összhangban biztonságirányítási jelentéseket készíteni az ÜGYFÉL-nek;
11. haladéktalanul tájékoztatni az ÜGYFEL-et a biztonsági fenyegetésekről, és lehetséges korrekciós intézkedéseket javasolni.

Az ÜGYFÉL köteles:

1. létrehozni egy napi szintű biztonsági irányításért felelős ÜGYFÉL-központot;
2. periodikusan felülvizsgálni a Végfelhasználói rendszer hozzáférési jogosultságait az azonos hozzáférési követelmények fenntartására vonatkozó igény megerősítésére, és a SZOLGÁLTATÓ-t tájékoztatni a szükséges változtatásokról;
3. tájékoztatni a Végfelhasználókat a biztonsági eljárásokról (például bejelentkezési eljárások, jelszókövetelmények, károkozó szoftver-ellenes programok használata, adat- és eszközbiztonsági eljárások);
4. megtervezni a Biztonsági Auditot;
5. meghatározni és a SZOLGÁLTATÓ rendelkezésére bocsátani az ÜGYFÉL:
   1. adatosztályozását és szabályozási kritériumait,
   2. adatvédelmi és adatkezelési követelményeit,
   3. adattitkosítási követelményeit;
6. haladéktalanul visszaigazolni a SZOLGÁLTATÓ által az ÜGYFÉL részére bejelentett biztonsági fenyegetések tudomásulvételét, és tájékoztatni a SZOLGÁLTATÓ-t a SZOLGÁLTATÓ által javasolt korrekciós intézkedések ÜGYFÉL általi elfogadásáról vagy elutasításáról, illetve az ÜGYFÉL által végrehajtott egyéb korrekciós intézkedésekről;
7. megtenni a megfelelő, elfogadott korrekciós intézkedéseket a biztonság minden olyan megsértésének orvoslására, amelyről a SZOLGÁLTATÓ értesítette az ÜGYFEL-et;
8. meghatározni a jelszavak visszaállítására és az ilyen jelszavaknak az arra felhatalmazott személyek számára történő átadására vonatkozó eljárási feltételeket.

# Információbiztonsági incidenskezelés

A SZOLGÁLTATÓ köteles:

1. ellenőrizni a Szolgáltatások hatálya alá tartozó adatfeldolgozó forrásokhoz való engedélyezett hozzáférést. Naplózni, nyomon követni és jelenteni az egyes hozzáférési visszaéléseket. Rendszeres felülvizsgálatokat és statisztikákat készíteni a feltételezett jogsértésekről;
2. az ÜGYFÉL kérésére:
   1. a biztonsági előírások megsértésének naplózására, riasztására és jelentésére vonatkozó eljárásokat kialakítani,
   2. válságegységet létrehozni a biztonsági vészhelyzetekre vonatkozó tervek előkészítésének és végrehajtásának irányítására.

A SZOLGÁLTATÓ köteles felismerni a biztonsági incidenst vagy szabályzatsértést, és kezelni a helyzetet.

# Az üzletmenet-folytonossági menedzsment információbiztonsági szempontjai

Az információfeldolgozó létesítményeket és rendszereket a rendelkezésre állási követelmények teljesítéséhez szükséges kapacitással kell ellátni.

Az SZOLGÁLTATÓ köteles:

1. azonosítani a fenyegetéseket és sérülékenységeket;
2. stratégiákat kidolgozni a kockázatok minimalizálására; és
3. meghatározni az Üzletmenet-Folytonossági Tervet (ÜFT), amely részletezi a szolgáltatás folyamatos rendelkezésre állását biztosító megfelelő mechanizmusokat.

Az ÜGYFÉL kérésére:

1. a SZOLGÁLTATÓ köteles készíteni egy, a fennmaradó kockázatokra vonatkozó dokumentumot.

# Biztonsági megfelelés

A SZOLGÁLTATÓ köteles azonosítani valamennyi vonatkozó jogszabályi és szerződéses követelményt, és megfelelő eljárásokat bevezetni a szellemi tulajdonjogokkal és a tulajdoni joggal védett szoftvertermékek használatával kapcsolatos, de nem kizárólagosan ezekre korlátozódó jogszabályi, szabályozási és szerződéses követelményeknek való megfelelés biztosítására.

A SZOLGÁLTATÓ garantálja, hogy a szolgáltatások nyújtásához alkalmazott valamennyi eszközhöz/szoftverhez szükséges engedéllyel rendelkezik, és megfelel a helyi jogszabályoknak.

A SZOLGÁLTATÓ köteles:

1. garantálni az összes vonatkozó törvény és rendelet betartását, a rendellenességek, a jogosulatlan események vagy bűncselekmények felderítését;
2. megfelelőségi személyzet útján nyomon követni a szabályozási környezet, figyelemmel kísérni a belső szabályokat, biztosítva:
   1. a folyamatos megfelelést,
   2. a megfelelőségi auditok megkönnyítését, és
   3. az ÜGYFÉL megfelelési jelentéstételi kötelezettségeinek teljesítését.

Amennyiben a Szolgáltatások az Európai Parlament (EU) 2016/679 Rendelete (GDPR) szerinti személyes adatok kezelésével járnak, a SZOLGÁLTATÓ köteles:

1. biztosítani az Adatvédelmi Jogszabályoknak való megfelelést;
2. az Adatvédelmi Jogszabályokkal összhangban kezelni az Adatokat, és megfelelő technikai és szervezeti biztonsági intézkedésekkel minimalizálni a véletlen vagy egyéb megsemmisülés vagy elvesztés, a jogosulatlan hozzáférés vagy a jogellenes vagy az Adatgyűjtés céljaival összeegyeztethetetlen adatkezelési tevékenységek kockázatát;
3. az adatokat kizárólag az ÜGYFÉL-nek való Szolgáltatás nyújtása céljából használni;
4. az adatok EU területén kívüli feldolgozásától tartózkodni az ÜGYFÉL külön írásbeli engedélye hiáynában;
5. technikai segítséget nyújtani az ÜGYFÉL részére az adatvédelmi jogszabályi rendelkezéseknek megfelelően elkészítendő jogi dokumentáció elkészítése során.

Az ÜGYFÉL kérésére tanácsot adni az adatvédelmi jogszabályokkal kapcsolatban, és elkészíteni a szükséges dokumentációt.

## Biztonsági Tesztek

A SZOLGÁLTATÓ köteles:

1. rendszeres Sérülékenységi Értékelést és Behatolásvizsgálatot végezni a Szolgáltatás biztonsági szintjének ellenőrzése és az ügyféladatok jogosulatlan hozzáféréstől való védelme érdekében, illetve Auditálási jelentést készíteni az Ügyfélnek, és korrekciós tervet javasolni;
2. évente legalább egyszer Behatolásivizsgálat elvégzésére egy független harmadik felet kijelölni;
3. évente legalább egyszer a Sérülékenységi Értékelés és a Behatolásvizsgálat eredményét megosztani az ÜGYFÉLLEL.

# A. melléklet: Ellenőrzések

|  |  |  |
| --- | --- | --- |
| Azonosító | Terület | Követelmények |
| (A Szolgáltató kötelezettsége) |
| SP01 | Szolgáltató Kapcsolatok | Valamennyi érintett fél köteles kijelölni egy a biztonsággal kapcsolatos valamennyi feladatot (pl. Biztonsági incidensek, monitoring, biztonsági struktúra, biztonsági iránymutatások frissítése) ellátó biztonsági központot. |
| SP02 | Műveletbiztonság | A Szolgáltató köteles proaktívan figyelemmel kísérni az összes szoftver/hardver/alkalmazási komponenst, és minden biztonsági incidenst haladéktalanul jelenteni a STELLANTIS-nak. |
| SP03 | Műveletbiztonság | Az Alapszolgáltatási szerződésnek - felmerülő többletköltségek nélkül – tartalmaznia kell egy a STELLANTIS-szal egyeztetett, a biztonsági incidensek jelentésére, megválaszolására és megoldására vonatkozó időkeretet. |
| SP04 | Információbiztonsági Szabályzatok | A változáskezelési folyamatokat integrálni kell a STELLANTIS folyamatokba. |
| SP05 | Információbiztonsági Szabályzatok | A Szolgáltatónak a kritikus komponensek engedélyezésének, validálásának és ellenőrzésének kezelésére használható eszközökkel (pl. kulcskezelés, SW-fejlesztés) kell rendelkeznie.  Ezeket integrálni kell a STELLANTIS folyamatokkal és eszközökkel, ha a STELLANTIS felhasználói hozzáférnek a Szolgáltató eszközéhez. |
| SP06 | Eszközkezelés | A Szolgáltató a STELLANTIS előzetes engedélye nélkül nem teheti az internet számára hozzáférhetővé az alkalmazás/infrastruktúra bármely vagy egyes komponenseit. Valamennyi távoli alkalmazás/infrastruktúra hozzáférés csak biztonságos VPN-en keresztül engedélyezhető. |
| SP07 | Eszközkezelés | A Szolgáltató köteles biztosítani, hogy a rendszeradminisztrációs feladatokat dedikált "jump" szerver végezze, mivel a STELLANTIS felhasználói hozzáférnek a Szolgáltató alkalmazásaihoz. |
| SP08 | Műveletbiztonság | A szabványos eljárásokon (pl. CIS, NIST...) alapuló „keményítés“ minden komponens esetében kötelező annak biztosítása érdekében, hogy csak a szükséges és engedélyezett SW vagy szolgáltatások legyenek telepíthetők és aktiválhatók.  A szolgáltatásokat úgy kell konfigurálni, hogy azok csak engedélyezett kapcsolatokat fogadjanak.  Minden komponenst szabványos NTP-vel kell szinkronizálni. |
|
|
| SP09 | Műveletbiztonság | A Szolgáltatónak biztosítania kell, hogy minden Szolgáltatás / Eszköz rosszindulatú szoftverek elleni védelemmel és végponti biztonsággal (pl. IDS, APT) legyen ellátva, amennyiben ez technikailag megvalósítható. |
| SP10 | Műveletbiztonság | A Szolgáltatónak biztosítania kell, hogy valamennyi biztonsági javítás a lehető leghamarabb és indokolatlan késedelem nélkül megvalósulhasson. |
| SP11 | Műveletbiztonság | A Szolgáltató köteles:  -A STELLANTIS által azonosított valamennyi magas prioritású/kritikus biztonsági sérülékenység a javítás rendelkezésre állásától számított 1 napon belüli orvosolására.  -Valamennyi más sérülékenység 10 napon belüli orvosolására. |
|
|
| SP12 | Hálózatbiztonság | A Szolgáltató elkülönített Biztonsági Zónát határoz meg a homogén biztonsági és üzleti szolgáltatások számára. |
| SP13 | Hálózatbiztonság | A Szolgáltató elkülönítést biztosít (pl. FW, ACL Alhálózati) annak érdekében, hogy kizárólag az engedélyezett Felhasználók vagy Kapcsolatok számára engedélyezze a hozzáférést. |
| SP14 | Hálózatbiztonság | A Szolgáltató meghatározza az egy adott és ellenőrizhető Szolgáltatói engedélyezési folyamat hatálya alá tartozó FW szabályokat. Az ilyen FW szabályokat a Szolgáltatás-Felülvizsgálati Értekezletek során a STELLANTIS-szal közösen kell felülvizsgálni. |
| SP15 | Hálózatbiztonság | A Szolgáltatónak legalább évente valamennyi FW-szabályt hitelesítenie kell. |
| SP16 | Hálózatbiztonság | A Szolgáltatónak figyelemmel kell kísérnie a nem használt FW-szabályokat. A 6 havonta legalább egyszer nem aktivált szabályokat felül kell vizsgálni és el kell távolítani. |
| SP17 | Hálózatbiztonság | A Szolgáltatónak minden vonatkozó(iparági szabvány szerinti) biztonsági funkciót alkalmazni kell a valós idejű biztonsági ellenőrzés garantálása érdekében (pl. IDS/IPS, WAF, anti DDOS). |
| SP18 | Hozzáférési szabály | A Szolgáltató köteles garantálni, hogy a STELLANTIS szolgáltatásaiban használt/alkalmazott összes UID-t STELLANTIS hitelesítő lépcsőin keresztül hitelesít (pl. Active Directory, RedHat IDM, Gigya,...).  A helyi Felhasználói azonosítókat a STELLANTIS engedélyezi. |
|
| SP19 | Hozzáférési szabály | A műszaki okokból indokolt és a STELLANTIS-szal megfelelően egyeztetett különleges esetekben a Szolgáltató köteles:  - erős jelszóval és adott esetben erős hitelesítéssel konfigurálni a helyi UID-ket;  - az ilyen Helyi Azonosítók használatát a STELLANTIS-szal megfelelően egyeztetett vészhelyzeti vagy jelentős változtatási konfigurációs tevékenységekre korlátozni;  - kérésre haladéktalanul a STELLANTIS rendelkezésére bocsátott biztonsági naplók segítségével számontartani és nyomon követni valamennyi tevékenységet. |
|
|
|
| SP20 | Hozzáférési szabály | A Szolgáltató köteles elfogadni a STELLANTIS Azonosító- és Hozzáféréskezelő Rendszerét ("HFKR") a STELLANTIS Felhasználói azonosítói (pl. alkalmazottak, vállalkozók...) által használt bármely szolgáltatói szolgáltatásra vonatkozóan. |
| SP21 | Hozzáférési szabály | A Szolgáltató kizárólag a STELLANTIS hitelesítési lépcsőit alkalmazza, mivel:  - A Szolgáltató felhasználói a STELLANTIS rendszereit használják (a STELLANTIS UID-ket rendel a Szolgáltató Felhasználóihoz).  - A STELLANTIS Felhasználói azonosítói (pl. alkalmazottak, vállalkozók) a Szolgáltató rendszereit használják (ebben az esetben SAML vagy OAuth 2.0 alapú föderációra van szükség). |
|
|
| SP22 | Hozzáférési szabály | STELLANTIS erre irányuló igénye estén, a Szolgáltatónak erős hitelesítést kell alkalmaznia (pl. Adaptív Hitelesítés, egyszeri PIN-kód, 2. lépcsős hitelesítés), melynek technikai részleteit a STELLANTIS rendelkezésére kell bocsátania. |
|
| SP23 | Hozzáférési szabály | A Szolgáltatónak olyan alkalmazásspecifikus felhasználói szerepköröket és profilokat kell kialakítania a szükséges ismeretek alapján (pl. admin, csak olvasás...), amelyeket a Szolgáltató gyakorlatába implementálnak, és ennek megfelelően leképeznek a STELLANTIS Azonosító- és Hozzáféréskezelő Rendszerében. |
| SP24 | Az információbiztonság szervezése | A Szolgáltatónak a fő szerepkörök (pl. IKT-Szerkezetek vs. fejlesztők vs. biztonságiak...) feladatmegosztása alapján kell megterveznie a Szolgáltató gyakorlatában alkalmazandó jogosultsági szabályokat, melyeket megfelelően le kell képezni a STELLANTIS Személyazonosság- és Hozzáféréskezelő Rendszerébe. |
| SP25 | Biztonsági megfelelés | A Szolgáltatónak meg kell felelnie a STELLANTIS SOX-konform Felhasználókezelési Folyamatainak annak érdekében, hogy garantálja:  - a Felhasználó-engedélyezést és  - a Felhasználó-érvénytelenítést.  Lásd: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx |
|
|
|
|
| SP26 | Hozzáférési szabály | Amennyiben 6 hónapig nem használják vagy nem férnek hozzá, úgy a Szolgáltatónak le kell tiltania:  - minden ICT-hozzáférést (rendszer- és alkalmazásszinten),  - minden Végfelhasználót (az üzleti igényekből adódó kivételeket dokumentálni kell, azok felülírhatják ezt a szabályt), |
|
|
| SP27 | Hozzáférési szabály | A Szolgáltatónak úgy kell konfigurálnia a Szolgáltató Fiókokat (pl. DB adminisztrációs fiókok, FTP Felhasználók, Szervező felhasználók...), hogy megakadályozza a jogosulatlan emberi hozzáférést és használatot. |
| SP28 | Eszközkezelés | A Szolgáltatónak a STELLANTIS megfelelő Eszközkezelési Megoldását (pl. SCCM, MDM AirWatch, ...) kell használnia vagy integrálnia. |
| SP29 | Kriptográfia | A Szolgáltatónak el kell fogadnia a vonatkozó STELLANTIS nyilvános kulcsú infrastruktúra által biztosított és kezelt Ügyféltanúsítványokat. |
| SP30 | Eszközkezelés | A Szolgáltatónak meg kell felelnie a STELLANTIS vonatkozó Eszközkezelési Gyakorlata (pl. SCCM, MDM AirWatch,..) által meghatározott szabályoknak az eszköz engedélyezett képességeinek alátámasztása és nyomon követése érdekében. |
| SP31 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltató kizárólag a STELLANTIS projektjein dolgozó felhasználóknak engedélyezi a STELLANTIS fejlesztői környezethez való hozzáférést.  A STELLANTIS bármikor ellenőrizheti és/vagy nyomon követheti a Szolgáltató felhasználóinak jogosultságát.  Ez a fejlesztési környezet tulajdonviszonyaitól függetlenül alkalmazandó. |
|
|
| SP32 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltatónak időben biztosítania kell az önmagyarázó Forráskód dokumentációt a tervezett fejlesztés valamennyi egyeztetett szakaszában. |
| SP33 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltató köteles a STELLANTIS megoldások kifejlesztéséhez felhasznált SW/HW komponensek teljes és részletes listáját rendelkezésre bocsátani és naprakészen tartani, beleértve a harmadik féltől származó komponenseket is. |
| SP34 | Biztonsági Tesztek | A Szolgáltatónak minden egyes szoftverkiadáskor biztonsági kódvizsgálatot kell végeznie, amelynek eredményeit meg kell osztania a STELLANTIS-szal. |
| SP35 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltató a STELLANTIS megoldásokat a biztonsági és iparági szabványok szerinti legjobb szoftverfejlesztési megoldások (pl. OWASP MSP, OWASP ASVS stb.) szerint fejleszti. |
| SP36 | Hálózati biztonság | A Szolgáltató köteles egyeztetni a STELLANTIS-szal a külső környezetekhez való minden olyan hálózati kapcsolatot, amelyet a Szolgáltató a STELLANTIS számára nyújtott szolgáltatások/megoldások (pl. nyilvános felhőszolgáltatások) nyújtásához igénybe vesz. |
| SP37 | Kriptográfia | A Szolgáltató garantálja, hogy a hitelesítő adatokat vagy kriptográfiai anyagokat (pl. magánkulcsok, tokenek, ...) nem tárolja helyben az eszközön, és nem ágyazza be a forráskódba. |
| SP38 | Kriptográfia | A Szolgáltató biztosítja, hogy minden olyan adatot, amelyet helyben kell tárolni egy eszközön (pl. mobil, laptop, ...), a STELLANTIS-szal előzetesen egyeztetett, ipari szabványú algoritmusokkal titkosít. |
| SP39 | Hozzáférési szabály | A Szolgáltatónak úgy kell konfigurálnia a Közösségi Bejelentkezést az alkalmazásban, hogy a STELLANTIS hitelesítési infrastruktúrája is ellenőrizze a felhasználófiók érvényességét. |
| SP40 | Hálózati biztonság | A Szolgáltató minden hálózati kapcsolatot úgy konfigurál, hogy az a Transport Layer Security protokollon alapuljon. A TLS protokoll minimális verziója az 1.2, és úgy kell konfigurálni, hogy elkerülhető legyen az alacsonyabb verziókra való visszalépés.  A backend szervereknek el kell utasítaniuk minden olyan TLS-tárgyalási kérelmet, amely anonim kulcscsere-algoritmusokat tartalmaz. |
|
| SP41 | Kriptográfia | A Szolgáltatónak védenie kell a HTTP-munkamenetazonosítókat és a felhasználói hitelesítési információkat tartalmazó tokeneket a Man-In-The-Middle támadások és a munkamenet eltérítése ellen. |
| SP42 | Kriptográfia | A Szolgáltató úgy konfigurálja a szervereket és az ügyfeleket, hogy a tanúsítványok érvényességét széles körben ellenőrizni és igazolni tudja (pl. a CRL-ek és az érvényességi időszakok figyelembevételével).  A Szolgáltató a mobilalkalmazásokon az OWASP pinning elveit követve végrehajtja a tanúsítványok közzétételét. Lásd: <https://www.owasp.org/index.php/Pinning_Cheat_Sheet> |
|
|
| SP43 | Hozzáférési szabály | A Szolgáltatónak minden kapcsolatot (azaz a Szerver-Szerver, Ügyfél-Szerver kapcsolatot) erős hitelesítési módszerekkel (pl. kölcsönösen hitelesített TLS) ellátva kell konfigurálnia. |
| SP44 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltatónak a szoftver kiadása előtt olvashatatlanná kell tenni az alkalmazás forráskódját. |
| SP45 | Kriptográfia | A Szolgáltatónak a STELLANTIS és a Szolgáltató között létrejött szerződésekben meghatározottak szerint a titoktartás és az integritás garantálása érdekében védenie kell a hitelesítési tokeneket.  A Szolgáltatónak az ilyen tokeneket azt megakadályozva kell kialakítani, hogy azokat a létrehozó eszköztől eltérő eszközön lehessen használni. |
|
| SP46 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltatónak a szoftver telepítése előtt el kell távolítania a forráskódból a hitelesítő adatokat vagy kriptográfiai anyagokat (pl. magánkulcsokat). |
| SP47 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltatónak olyan mobilalkalmazásokat kell fejlesztenie, amelyek nem tárolnak adatokat külső cserélhető memóriatárolókon (pl. SD-kártyákon). |
| SP48 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltató az operációs rendszerek által rendelkezésre bocsátott valamennyi alkalmazandó biztonsági fokozatok (pl. sandboxing, engedélyezés, ...) használatával konfigurálja a mobilalkalmazást.  Az alkalmazásnak képesnek kell lennie a valós idejű támadások észlelésére és megelőzésére. |
|
|
| SP49 | Információbiztonsági szabály | A Szolgáltató szükség esetén kérésre segít a Macrodata osztályozásában. |
| SP50 | Hálózatbiztonság | A Szolgáltatónak minden olyan hálózati kapcsolatot, amely hitelesítő, bizalmas vagy érzékeny adatokat (azaz személyazonosításra alkalmas információkat, különleges adatokat) továbbít, úgy kell konfigurálnia, hogy az TLS protokollt használjon. |
| SP51 | Kriptográfia | A Szolgáltatónak úgy kell konfigurálnia az Alkalmazásokat, hogy a Man-In-The-Middle támadások megelőzése érdekében széles körben ellenőrizze és igazolja a tanúsítványok érvényességét (pl. beleértve a CRL-eket és az érvényességi időszakot). |
| SP52 | Hálózatbiztonság | A Szolgáltatónak minden adatcsere-folyamatot (pl. WS vagy FTP) úgy kell megterveznie és megvalósítania, hogy az TLS-csatornán keresztül történjen. |
|
|
|
| SP53 | Rendszer Beszerzése, Fejlesztése és Karbantartása | A Szolgáltatónak minden adatátviteli folyamatot úgy kell megterveznie és végrehajtania, hogy minden adat titkosítva kerüljön átvitelre.  A folyamat során a szolgáltató garantálja, hogy az összes érintett adat Titkossága, Sértetlensége és Rendelkezésre állása védett. |
|
| SP54 | Fizikai Biztonság | A Szolgáltató minden biztonsági másolatot Biztonságos környezetben készít és tárol.  Az ilyen környezetnek olyan fizikai és logikai hozzáférés-ellenőrzési eljárásokat kell biztosítania, amelyek csak az arra jogosult felhasználók számára teszik lehetővé a hozzáférést. |
|
| SP55 | Műveletbiztonság | A Szolgáltató rendszeresen (legalább negyedévente) elvégzi a biztonsági mentések visszaállításának tesztelését.  Az ilyen vizsgálatok eredményeit rendszeresen jelenti kell a STELLANTIS-nak.  A STELLANTIS minden sikeresen végrehajtott visszaállítási tesztet befejezett visszaállításnak tekint. |
|
|
| SP56 | Műveletbiztonság | A Szolgáltató köteles a STELLANTIS rendelkezésére bocsátani a STELLANTIS számára dedikált infrastrukturális és alkalmazási komponensek biztonsági naplóit. |
| A biztonsági naplókészletet (pl. bejelentkezési/kilépési tevékenység ...) a biztonsági tervezési tevékenységek során kell egyeztetni. |
| SP57 | Műveletbiztonság | A Szolgáltatónak proaktívan figyelemmel kell kísérnie valamennyi biztonsági naplót, és minden biztonsági incidenst haladéktalanul jelentenie kell a STELLANTIS-nak. |
| SP58 | Biztonsági Teszt | A Szolgáltató minden szerződéses évben legalább 2 alkalommal foganatosítja a STELLANTIS számára nyújtott szolgáltatások/megoldások teljes körű VA/PT-jét.  Minden eredményt javítási tervekkel együtt (adott esetben) további költségek nélkül meg kell osztani a STELLANTIS-szal. |
|
| SP59 | Biztonság Teszt | A Szolgáltató lehetővé teszi a STELLANTIS számára (vagy a STELLANTIS megfelelően felhatalmazott harmadik fél Szolgáltatójának), hogy a közösen megállapított időben és módon VA/PT-t végezzen. |
| SP60 | Információbiztonsági politika | A Szolgáltató lehetővé teszi a STELLANTIS számára, hogy a Felek által elfogadott szabályok szerint elvégezze a szolgáltatás körébe tartozó valamennyi infrastrukturális komponens és alkalmazás ellenőrzését. |

# B. melléklet: Felhő-ellenőrzések

|  |  |
| --- | --- |
| Fogalmak | Felhőszolgáltató (CP): A SZOLGÁLTATÓ. |
| Felfőügyfél (CC): Az ÜGYFÉL. |
| **Felelős és hivatkozás** | **Követelmény** |
| CP01 | A CP köteles a CC adataihoz hozzáférő és/vagy azokat kezelő rendszergazdák és üzemeltetők képességeinek és ismereteinek értékeléséhez megfelelő eljárással rendelkezni. |
| CP02 | A CP köteles legalább évente megfelelő, harmadik fél útján biztonsági értékelést végezni a szolgáltatásról és a szolgáltatásba bevont valamennyi rendszerről. |
| CP03 | A CP köteles megfelelni a szükséges legjobb biztonsági gyakorlatnak és egyéb minőségi szabványoknak. A CC köteles tisztában lenni ezekkel a gyakorlatokkal. |
| CP04 | A CP felelősséget vállal a CC-adatok bizalmas jellegének, rendelkezésre állásának és sértetlenségének biztosításáért. |
| CP05 | A CP köteles SLA-kat kell biztosítaniuk a fiókok létrehozására, felfüggesztésére és törlésére. |
| CP06 | A CP köteles megfelelő szolgáltatásminőséget biztosítani, más CC-k vagy azok CU-k intézkedései vonatkozásában is. |
| CP07 | A CP köteles elmagyarázni egy a CP-nél esetlegesen bekövetkező nagyobb üzemkiesés üzletre gyakorolt hatását. |
| CP08 | A CP köteles üzletmenet-folytonossági és katasztrófa-helyreállítási tervet készíteni.  A CP köteles biztosítani:  - Helyreállítási adatközpontok elhelyezését.  - DR és BC tervezési dokumentumokat.  - RTO-t és RPO-t. |
| CP09 | A szerződés időtartama alatt CP CC tudta és beleegyezése nélkül nem változtathatja meg az adatfeldolgozási műveletek feltételeit. Amennyiben CC nem fogadja el a módosításokat, úgy kapcsolódó költségek keletkezése nélkül jogosult a szerződés felmondására. |
| CP10 | A CC rendszereit el kell különíteni a többi CP-ügyfél rendszereitől. |
| CP11 | A szolgáltatás nyújtásához használt szerkezet részletes leírását meg kell adni, és azt jóvá kell hagyni. |
| CP12 | A CC jogosult sérülékenységi értékelések és behatolás-vizsgálat elvégzésére. |

# C. melléklet: Adatvédelmi ellenőrzések

"Adatok": személyes adatok.

|  |  |
| --- | --- |
| **Azonosító** | **Követelmény** |
| DP01 | Az Ügyfél mindig kizárólagos Adattulajdonos. |
| DP02 | A Szolgáltató felel az általa nyújtott szolgáltatásokkal kapcsolatos jogszabályok be nem tartása miatt kiszabott szankciókért. |
| DP03 | Az Ügyfelet haladéktalanul tájékoztatni kell az incidensről és a végrehajtott korrekciós intézkedésekről, ha az Adatfeldolgozásban vagy a szolgáltatások nyújtásához használt bármely rendszerben adatvédelmi incidenst vagy biztonsági rést észlelnek. |
| DP04 | A hitelesítéshez használt Adatokat hatékony kriptográfiai biztonsági intézkedésekkel kell védeni. |
| DP05 | Valamennyi Adatátvitelt a legújabb titkosítási eljárásokkal kell titkosítani. |
| DP06 | A bizalmas vagy fokozottan bizalmas adatok feldolgozása esetén, mint például a helymeghatározási adatok, személyazonosító okmányok, banki adatok, személyes adatok különleges kategóriái, azokat a legmodernebb titkosítási eljárások alkalmazásával nyugalmi állapotban kell titkosítani. |
| DP07 | Az Ügyfél köteles biztosítani az Adatok (többmenetes biztonságos törléssel való) megsemmisítését a tárolóeszközök eltávolítása, a hardver cseréje vagy a hardver újrafelhasználása esetén. |
| DP08 | A Szolgáltató köteles megadni az Adatok törlésének és megőrzésének ütemezését, beleértve az életciklusvégi megsemmisítést is. Ennek a szerződés felmondása esetén is érvényesnek kell lennie. |
| DP09 | A Szolgáltató erre vonatkozó igény esetén (pl. kérésre, vagy ha az Ügyfél úgy dönt, hogy eláll a szolgáltatástól) köteles az Adatok valamennyi másolatát megfelelő időn belül biztonságosan törölni. |
| DP10 | A Szolgáltató nem oszthatja meg az Ügyfél-Adatokat harmadik Felekkel vagy a Szolgáltató által esetlegesen kínált egyéb szolgáltatásokon keresztül.  A Szolgáltató csak a szolgáltatás nyújtásának céljával jogosult az Adatok feldolgozására.  A különböző célokra gyűjtött adatokat külön-külön szükséges kezelni. |
| DP11 | Ha a nyújtott szolgáltatás Adatvédelmi engedélyhez/hozzájáruláshoz kötött, úgy az ilyen engedélyekre/hozzájárulásokra vonatkozó naplókat a szerződés teljes időtartama alatt meg kell őrizni, illetve kérésre és a szerződés lejártakor az Ügyfél rendelkezésére kell bocsátani. |
| DP12 | A Szolgáltatónak meg kell határoznia, hogy milyen feltételek mellett férhetnek hozzá harmadik Felek az Ügyfél adataihoz, beleértve a hatóságokat is. |
| DP13 | A Szolgáltató kizárja vagy korlátozza az Adatok másolását (beleértve a nyomtatást is), és gondoskodik a használatot követő megfelelő megsemmisítésről. |
| DP14 | A Szolgáltató köteles ellenőrzési nyomvonalakat vezetni (az ellenőrzési nyomvonalnak hamisításbiztosnak kell lennie), és lehetővé tenni, hogy az Ügyfél nyomon követhesse őket annak a megállapítása érdekében, hogy ki olvasta/táplálta be az adatfeldolgozó rendszerekbe, módosította vagy törölte az Adatokat. A naplóknak tartalmazniuk kell a forrás IP-címet.  A naplóknak legalább egy évig rendelkezésre kell állniuk. |
| DP15 | A Szolgáltató köteles lehetővé tenni az Ügyfél számára, hogy kérésre elfogadott és használható formátumban valamennyi adatról másolatot kapjon. |
| DP16 | Az Adatokról legalább napi rendszerességgel biztonsági másolatot kell készíteni, és a Szolgáltató által az Adatfeldolgozáshoz használt szoftverekről naprakész biztonsági másolatot kell tartani. |
| DP17 | Megfelelő intézkedéseket kell elfogadni az Adatokhoz való hozzáférés meghatározott határidőn (de legfeljebb hét napon) belül történő helyreállítása érdekében. |
| DP18 | Az Adatokat olyan intézkedések alkalmazásával tárolják, amelyek védik azokat a jogosulatlan hozzáféréstől, megváltoztatástól, sérüléstől és megsemmisüléstől (pl. védik a véletlen megsemmisüléstől vagy elvesztéstől). |
| DP19 | Biztosítani kell a személyes Adatokra vonatkozó jogszabályoknak való megfelelést. Ha a szolgáltatás nyújtása érdekében az Adatokat az EU-n kívül dolgozzák fel (még ha csak hozzáférés szintén is), és erről a jogszabályok által megkövetelt adatvédelmi szerepköröknek és hozzájárulások megjelölésével megfelelően tájékoztatni kell az Ügyfelet. |
| DP20 | A Szolgáltató köteles támogatnia az Ügyfelet az esetlegesen szükséges jogi eljárások során. |
| DP21 | A Szolgáltató köteles meghatározni, hogy mely vállalatok (beleértve az alvállalkozókat is) és hol dolgozzák fel (még ha csak hozzáférés szintjén is) az Ügyfél-Adatokat, valamint azt, hogy mikor és miért továbbítják az Adatokat ezekre a helyekre.  A Szolgáltató köteles tájékoztatást adni arról, hogy az Ügyfél-Adatok milyen körülmények között továbbíthatók, akár ideiglenesen is, más országokba. A Szolgáltató köteles az Adatok továbbítását az Ügyfél által megfelelőnek tekintett országokra korlátozni. |
| DP22 | A Szolgáltató a következőket garantálja:  Adathozzáférést ellenőrző rendszert.  Beépített mechanizmust, amely valamennyi, az Adatokhoz hozzáférő személyt felszólít a jelszavak megújítására.  Egyedi bejelentkezési azonosítót ("Felhasználói azonosító") és jelszót (a "hitelesítő adat") minden egyes adatfeldolgozásban részt vevő személy (továbbá a Szolgáltató felhasználói) számára.  A kizárólag a hozzárendelt személy ("Felhasználó") által ismert jelszó, mely legalább a következő jellemzőkkel bír:   1. legalább 8 karakterből áll; 2. számjegyekkel vagy különleges karakterekkel kombinált kis- és nagybetűket tartalmaz; 3. nem tartalmazza a felhasználói azonosítót; 4. azt a felhasználónak önállóan és kötelezően módosítania kell az első csatlakozáskor és a jelszó visszaállítása után; 5. azt legalább 60 naponként módosítani kell.   A Felhasználóhoz rendelt felhasználói azonosító nem ruházható át egy másik, a feldolgozásért felelős személyre.  A hitelesítő adatokat deaktiválni kell, ha azokat legalább 6 hónapig nem használták (kivéve a műszaki irányítási célokra engedélyezetteket).  A hitelesítő adatokat akkor is haladéktalanul deaktiválni kell, ha a feldolgozásért felelős személyt az Adatokhoz való hozzáférésből kizárták.  A feldolgozásért felelős személyeket utasítani kell arra, hogy a feldolgozási munkamenetek alatt ne hagyják felügyelet nélkül és ne tegyék hozzáférhetővé az elektronikus berendezéseket. |
| DP23 | Engedélyező rendszer:   1. amennyiben az adatfeldolgozásért felelős személyek számára különböző szintű engedélyezési profilokat határoztak meg, úgy engedélyezési rendszert kell alkalmazni; 2. az adatkezelésért felelős minden egyes személy vagy személyek homogén csoportja számára az adatkezelés megkezdése előtt olyan jogosultságú profilokat köteles meghatározni és konfigurálni, amelyek csak az adatkezelési műveletek elvégzéséhez szükséges adatokhoz való hozzáférést teszik lehetővé; 3. rendszeresen, de legalább évente ellenőrizni kell, hogy a profilok fenntartásának feltételei továbbra is fennállnak-e. |
| DP24 | Szervezési intézkedések - A Szolgáltató garantálja, hogy:   1. az Adatokhoz való hozzáférés a "szükségesség" elve alapján történik; 2. korlátozza az Adatfeldolgozással kapcsolatos tevékenységek végzésére jogosult személyek számát; 3. képezi a felhatalmazott személyeket az adatvédelmi előírásokról, a Szolgáltató által hozott biztonsági intézkedésekről és a biztonsági vészhelyzetek esetén alkalmazott biztonsági politikákról; 4. az Adatfeldolgozó rendszer használatára jogosult személyek csak a hozzáférési joggal rendelkező Adatokhoz férnek hozzá, és az Adatokat a feldolgozás során és azt követően a tárolás során nem lehet jogosulatlanul olvasni, másolni, módosítani, eltávolítani vagy felhasználni; 5. naprakész listát vezet az Adatokhoz való hozzáférésre jogosult személyekről, és ezt a listát az Ügyfél indokolt kérésére az Ügyfél rendelkezésére bocsátja. |
| **Rendszergazdák**  Az Ügyfél megbízza a Szolgáltatót a "Rendszergazdák" mint szakavatott személyek kijelölésével. A Szolgáltató saját hatáskörének megfelelően a következő intézkedéseket vállalja (példálózóan és nem kizárólagosan): | |
| DP25 | A Rendszergazdához való Adathozzáférés ellehetetlenítése. Ha ez nem megvalósítható, erről tájékoztatni szükséges az Ügyfelet. |
| DP26 | A Rendszergazda szerepkörrel megbízott személy(ek) képzettségének gondos felmérése. |
| DP27 | A Rendszergazda egyedi kijelölése, és a Rendszergazda jogosultságszintjéhez kapcsolódóan ellátandó tevékenységek részletes listája. |
| DP28 | Egy a Rendszergazda személyes adatait tartalmazó belső dokumentum létrehozása és napra készen tartása. |
| DP29 | Az adatvédelmi hatóság ellenőrzése esetén és/vagy az Ügyfél kérésére a fent említett dokumentum DP28 formátumban való rendelkezésre bocsátása. |
| DP30 | A Rendszergazda tevékenységének legalább éves ellenőrzése annak megállapítása érdekében, hogy az megfelel-e az adatvédelmi jogszabályokban előírt szervezeti, technikai és biztonsági előírásoknak. |
| DP31 | A Rendszergazda az Adatfeldolgozó rendszerekhez és az elektronikus adatbázisokhoz való logikai hozzáférés-ellenőrzésének nyilvántartása. A nyilvántartásoknak (hozzáférési naplóknak) teljesnek és megváltoztathatatlannak kell lenniük. Lehetővé kell tenni az integritásuk tervezett ellenőrzési céloknak megfelelő nyomon követhetőségét. |
| DP32 | A DP31-ben meghatározott hozzáférési naplókat megfelelő ideig, de legalább egy évig meg kell őrizni. A hozzáférési naplóknak tartalmazniuk kell az időbélyegzőket és a kapcsolódó események leírását.  A naplókat kérés esetén az Ügyfél rendelkezésére kell bocsátani. |