Szolgáltatási Szerződés Instant Honlap vagy Instant Webshop szolgáltatás igénybevételére

amely létrejött egyrészről

SZOLGÁLTATÓ ADATAI

Szolgáltató neve: **Magyar Telekom Távközlési Nyrt.**

Székhely: **1097 Budapest, Könyves Kálmán krt. 36.**

Postacím: **1519 Budapest Pf. 434**

Adószám: **10773381-2-44**

Cégjegyzékszám: **01-10-041928**

Bankszámla szám: **10700024-04021609-51100005**

Értékesítő értékesítési kód:

Szolgáltató kapcsolattartási elérhetőségei:
Név: **Központi Ügyfélszolgálat**
Postacím: **1276 Budapest Pf. 1400**
E-mail cím: **uzleti@telekom.hu**
Internetes honlap címe: **www.telekom.hu**
Telefonos Ügyfélszolgálat, hibabejelentő: **1400**
(a hét minden napján, 0-24 óráig a Magyar Telekom vezetékes és mobil hálózatából díjmentesen hívható)

a továbbiakban **Szolgáltató**

másrészről

ELŐFIZETŐ ADATAI

Előfizető MT azonosító:

Előfizető neve:

Székhely:

Adószám:

Cégjegyzékszám:

Technikai kapcsolattartó neve:

Technikai kapcsolattartó e-mail címe:

a továbbiakban **Előfizető**

a továbbiakban együtt **Felek** között az alábbi feltételek mellett:

Előfizető köteles a Szolgáltatót a szerződéskötéskor megadott adataiban bekövetkezett változásokról 8 napon belül tájékoztatni. Ennek elmulasztása esetén, pl. amennyiben esetleg az esedékes számla küldésére hibás címre/névre kerül sor, a fizetési késedelemből eredő jogkövetkezményekért a Szolgáltató nem felel.

Szolgáltató az Előfizető részére a jelen szerződés keretében az alábbi Instant Honlap, valamint Instant Webshop szolgáltatást (kérjük, jelölje a megfelelőt) biztosítja.

A választott szolgáltatás:

Szolgáltatás neve	Havidíj (nettó)
◯ Instant Honlap	5 990 Ft
◯ Instant Honlap Prémium	7 990 Ft
◯ Instant Webshop	9 990 Ft
◯ Instant Webshop Prémium	14 990 Ft

A szolgáltatáscsomagok tartalma

Instant Honlap
- Domain regisztráció és fenntartás (.hu, .eu, .com, .org, .info, .net, .biz végződéssel az 1. számú melléklet szerint)
- Reszponzív (számítógépre és mobil eszközökre is optimalizált) honlap elkészítése
- SSL tanúsítvány
- 2 GB webtárhely
- 30 perc videótárhely
- Magyar nyelvű támogatás a szolgálatás igénybevételéhez

Instant Honlap Prémium
- Domain regisztráció és fenntartás (.hu, .eu, .com, .org, .info, .net, .biz végződéssel az 1. számú melléklet szerint)
- Reszponzív (számítógépre és mobil eszközökre is optimalizált) honlap elkészítése
- SSL tanúsítvány
- 50 GB webtárhely
- 30 perc videótárhely
- Magyar nyelvű támogatás a szolgálatás igénybevételéhez
- Szakértői támogatás a honlap szerkesztésében
- Riport funkciók elérhetősége
- Közösségi média és marketing funkciók elérhetősége, összeköttetés Előfizető meglévő fiókjával (Instagram és Facebook összekötési lehetőség)
- Google My Business összeköttetés Előfizető meglévő fiókjával

Instant Webshop
- Domain regisztráció és fenntartás (.hu, .eu, .com, .org, .info, .net, .biz végződéssel az 1. számú melléklet szerint)
- Reszponzív (számítógépre és mobil eszközökre is optimalizált) honlap és webáruház elkészítése
- SSL tanúsítvány
- 50 GB webtárhely
- 30 perc videótárhely
- Magyar nyelvű támogatás a szolgálatás igénybevételéhez
- Webáruház létrehozása
- Elhagyott kosár visszaállítása funkció elérhetősége
- Termékértékelések

Instant Webshop Prémium
- Domain regisztráció és fenntartás (.hu, .eu, .com, .org, .info, .net, .biz végződéssel az 1. számú melléklet szerint)
- Reszponzív (számítógépre és mobil eszközökre is optimalizált) honlap és webáruház elkészítése
- SSL tanúsítvány
- 50 GB webtárhely
- 30 perc videótárhely
- Magyar nyelvű támogatás a szolgálatás igénybevételéhez
- Webáruház létrehozása
- Elhagyott kosár visszaállítása funkció elérhetősége
- Termékértékelések
- Szakértői támogatás a honlap szerkesztésében
- Riport funkciók elérhetősége
- Közösségi média és marketing funkciók elérhetősége, összeköttetés Előfizető meglévő fiókjával (Instagram és Facebook összekötési lehetőség)
- Google My Business összeköttetés Előfizető meglévő fiókjával
- Facebook Marketplace összeköttetés Előfizető meglévő fiókjával

A szolgáltatás létesítése

A szerződéskötést követően a Szolgáltató az Előfizetőnek a megadott kapcsolattartói e-mail címére elküldött online űrlapon keresztül kéri a honlap, illetve webshop elkészítéséhez szükséges adatokat elküldeni. (Szöveges leírásokat, fényképeket, fájlokat, stb.) Az űrlap kitöltéséhez egy online portálon, való regisztráció szükséges, melyhez az Előfizető a kapcsolattartói e-mail címére kap meghívást. A regisztrációra azért van szükség, mert ez a portál szolgál kommunikációs felületként a honlap, ill. webshop publikálásáig, ahol a Szolgáltató az Előfizető részére elküldi elkészített oldal előnézeti

képét is, és itt lesz lehetősége az Előfizetőnek visszajelezni arról, hogy szeretne-e a publikálás előtt további módosításokat kérni.

Ezen a portálon keresztül lesz lehetősége a Szolgáltatónak és az Előfizetőnek arra, hogy a honlap, illetve webshop elkészítésével kapcsolatos további kérdéseiket, kéréseiket egymás felé jelezzék a honlap, illetve a webshop publikálásáig.

A honlap, illetve webshop publikálása az Előfizető jóváhagyását követően történik meg. A Szolgáltató ezt követően az Előfizető kapcsolattartó e-mail címére küldi meg a honlap, illetve webshop szerkesztéséhez szükséges felhasználói adatokat, valamint a szerkesztő felület elérhetőségét.

A szolgáltatás üzemeltetése a Wix.com Ltd. (továbbiakban Wix) tulajdonát képező, felhő-alapú platform segítségével történik. Előfizető jelen szerződés aláírásával a Wix igénybevételi feltételeit, valamint adatkezelési feltételeit is elfogadja, melyek az alábbi címen érhetők el: https://www.wix.com/about/privacy , https://www.wix.com/about/terms-of-use. Felek rögzítik, hogy a Terms of Use, valamint a Privacy Policy elfogadása az Előfizető és a Wix között hoz létre jogviszonyt, azok megszegése esetén Előfizető Szolgáltatóval szemben nem léphet fel.

Díjak

Az Instant Honlap Prémium és Instant Webshop Prémium csomagok havidíja tartalmazza a honlap, illetve a webáruház módosításában való szakértői segítségnyújtást is. A további csomagokban ezek a szolgáltatások külön díj ellenében vehetők igénybe. A beérkező módosítási igények (az alábbi táblázat szerinti mértékben) végrehajtására a Szolgáltató 3 munkanapos határidőt vállal.

A szakértői segítségnyújtás díjait a következő táblázat tartalmazza.
Az összegek egyszeri díjak és az ÁFA-t nem tartalmazzák!

Szolgáltatás		**Egyszeri díj csomagoknál**	**Egyszeri díj prémium csomagnál**
Webes tartalom szerkesztése	Legfeljebb 10 fotó módosítása, logó csere, kezdőkép módosítása. Szövegek módosítása vagy hozzáadása (legfeljebb 10 új szövegdoboz)	2 000 Ft	-
Webes riportok	Csatlakozás a Google Analyticshez - Dashboard létrehozása a felhasználó számára.	2 500 Ft	-
Közösségi média integráció, hírlevél	Közösségi média platformokkal való összekapcsolás (Instagram és Facebook). Hírlevél beállítása.	1 000 Ft	-
Webshop plusz termékek, max. 10	További 10 termék hozzáadása a webshophoz.	550 Ft	-
Webshop plusz termékek, max. 50	További 50 termék hozzáadása a webshophoz.	2 000 Ft	1 500 Ft

A kiegészítő szolgáltatások külön rendelhetők meg.

Díjazási/számlázási rendelkezések
Az Előfizető a Szolgáltató által havonta megküldött számlán szereplő összeget a számlán feltüntetett határidőben köteles kiegyenlíteni. A havidíj számlázása a honlap, illetve webshop publikálásának napján, de legkésőbb a szerződéskötéstől számított 30. napon kezdődik.

Fizetési késedelemre irányadó rendelkezések
Amennyiben az Előfizető a díj megfizetésével késedelembe esik, és azt a Szolgáltató legalább 8 napos póthatáridőt tartalmazó fizetési felszólítására sem fizeti meg, a Szolgáltató jogosult a szerződés tárgyát képező honlap vagy webshop elérhetőségének felfüggesztésére. A felfüggesztésre okot adó, kiegyenlítetlen számla késedelmi kamattal terhelt

összegének teljes kiegyenlítését követően kerülhet sor a szolgáltatás visszaállítására. Az Előfizető 30 napot meghaladó fizetési késedelme esetén a késedelem egyéb jogkövetkezményein kívül Szolgáltató jogosult a jelen megállapodás azonnali hatályú felmondására, és egyben a szerződés tárgyát képező honlap vagy webshop megszüntetésére, valamint a kapcsolódó domain cím delegálásának megszüntetésére. Fizetési késedelem esetén Szolgáltató a mindenkori Polgári Törvénykönyv szerinti késedelmi kamatot jogosult érvényesíteni.
A másik félhez címzett, teljesítésre felhívást tartalmazó fizetési felszólítás az igények elévülését megszakítja.

Ügyfélkapcsolat, hibaelhárítás, rendelkezésre állás
A szolgáltatás kapcsán felmerült esetleges hibákat, kérdéseket az Előfizető az instanthonlap@telekom.hu címen, vagy a 1400 telefonszámon jelezheti (az ügyfélszolgálat munkanapokon 8-20 óráig, a hibabejelentő a hét minden napján, 0-24 óráig díjmentesen hívható a Magyar Telekom helyhez kötött hálózatából).

Időtartam, megszűnés.
A jelen szerződés a felek általi aláírása napján lép hatályba és a szolgáltatás létesítéstől számított 24 hónapig tart.
A határozott idő lejárata előtti megszűnése esetén a Szolgáltató jogosult kötbért érvényesíteni. A kötbér összege a határozott időtartamból a hátralevő időszakra vonatkozó díjak egy összegben. A határozott időtartam lejártával a szerződés újabb egy-egy éves határozott időtartamra meghosszabbodik, a Szolgáltató honlapján publikált díjon, kivéve, ha valamely fél a határozott idő lejártát legalább 15 (tizenöt) nappal megelőzően arról értesíti a másik felet, hogy nem kívánja a szerződés meghosszabbodását.

Jelen szerződést mindkét fél kizárólag akkor jogosult azonnali hatályú rendkívüli felmondás útján megszüntetni a másik félhez címzett, indokolással ellátott írásbeli nyilatkozattal, ha a másik fél:

a) bármely fizetési kötelezettségének teljesítésével 30 (harminc) napot meghaladó fizetési késedelembe esik,
b) a fél szerződéses kötelezettségének teljesítését a fél írásbeli felszólítása ellenére magatartásával vagy mulasztásával akadályozza, feltéve, hogy a szerződésszegő fél a fél írásbeli felszólításában megjelölt póthatáridőben sem orvosolta a felszólításban megjelölt szerződésszegést,
c) egyedüli tagja, illetve többségi, minősített többségi vagy meghatározó befolyással rendelkező tagja vagy részvényese személyében közvetlen vagy közvetett változás történt,
d) megszegi a titoktartási kötelezettségét,
e) megsérti a szerződés korrupcióellenes rendelkezéseit,
f) fizetésképtelenné válik, vagy vele szemben jogerősen elrendelésre kerül a felszámolás, vagy végelszámolást kezdeményez, vagy nála csődeljárás indult és a csődeljárásban a fizetési haladék lejárt.

Megszűnik továbbá a szerződés, ha az Előfizető és a Wix között létrejött jogviszony megszűnik.

A jelen megállapodás megszűnése esetén az Előfizető kötelessége gondoskodni arról, hogy a szerződés megszűnéséig a honlapon, illetve webáruházban található adatokat (fényképek, ügyféladatok, stb.) mentése megtörténjen. A megszüntetést követően Szolgáltató az Előfizető honlapjának, webáruházának adatait nem állítja vissza.

Kártérítési felelősség
A Szolgáltató szerződésszegéssel okozott károkért való felelőssége kizárólag a tapadó károkra (azaz a szolgáltatás tárgyában bekövetkezett károkra) terjed ki. Szolgáltató nem felelős a következménykárokért (korlátozás nélkül ideértve az adatvesztésből eredő károkat is).
A felek a Szolgáltató kártérítési felelősségének mértékét a jelen szerződés megszegésével okozott károkért káreseményenként legfeljebb a szerződés tárgyát képező szolgáltatás nettó havidíjának 3 hónapra számolt összegének 100%-ára korlátozzák azzal, hogy a szerződés teljes időtartama alatt a Szolgáltató szerződésszegésből fakadó kártérítési kötelezettségeinek összértékét a felek legfeljebb a szerződés tárgyát képező szolgáltatás teljes futamidőre számított ellenértéke teljes nettó összegének 100%-ára korlátozzák.
Szándékosan okozott, továbbá emberi életet, testi épséget vagy egészséget megkárosító szerződésszegésért való felelősségre a fenti felelősségkorlátozó rendelkezések nem vonatkoznak.
A kártérítési felelősség alól bármely fél mentesül akkor, ha úgy járt el, ahogy az az adott helyzetben általában elvárható.

Kapcsolattartás
A szerződésben az előfizetői adatok között a kapcsolattartásra, értesítésre alkalmas adatokat az Előfizető abból a célból bocsátotta a Szolgáltató rendelkezésére, hogy ezen elérhetőségeken a Szolgáltató az Előfizetőt szerződéssel

kapcsolatosan értesíthesse. Az értesítés ezen módját az Előfizető a jelen szerződés aláírásával elfogadja. A kapcsolattartási e-mail címre történő továbbítás esetén az értesítést közöltnek kell tekinteni az elektronikus levelezőrendszer által megjelölt sikeres elküldés időpontjában. Az Előfizető elfogadja, hogy a jelen előfizetői szerződés teljesítésével kapcsolatos kérdésekben a Szolgáltató választása szerint, elektronikus levélben vagy egyéb úton tájékoztathassa

Az adatok feletti rendelkezési jogosultság; a személyes adatok kezelése és feldolgozása
Az informatikai szolgáltatások igénybevételével az Előfizető által tárolt és előállított adatok felett az Előfizető a vonatkozó jogszabályi (így pl. a személyes adatok védelmére vonatkozó) rendelkezések keretei között rendelkezik. A Felek rögzítik, hogy az informatikai szolgáltatások igénybevételével kezelt személyes adatok tekintetében az Előfizető adatkezelőként, a Szolgáltató pedig adatfeldolgozóként jár el. A Szolgáltató a személyes adatokat az Előfizető írásbeli utasításai szerint kezeli, azzal, hogy a jelen Szerződésben és annak mellékleteiben foglaltak ilyen utasításnak minősülnek, az esetlegesen ezeken kívül adott előfizetői utasítások pedig nem lehetnek az előbbiekkel ellentétesek, illetve nem tehetik a Szolgáltató teljesítését nehezebbé. Az adatfeldolgozás részleteit, illetve a Felek ezzel kapcsolatos jogait és kötelezettségeit a jelen Szerződéshez csatolt és annak elválaszthatatlan részét képező 2. számú Melléklet („Adatfeldolgozási megállapodás") rendezi, azzal, hogy az adatfeldolgozás részleteit az Adatfeldolgozási megállapodás I. sz. Függeléke – a vonatkozó Szolgáltatást leíró mellékletekkel együtt – rögzíti.

Tartalom
Szolgáltató az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (DSA rendelet) szerinti bejelentés kivizsgálása alapján jogosult adott tartalmat eltávolítani, vagy az ahhoz való hozzáférést megszüntetni. Szolgáltató továbbá adott tartalom eltávolítására, vagy hozzáférés megszüntetésére felszólító hatósági rendelkezés esetén az adott tartalmat eltávolítja, vagy a hozzáférést megszünteti.

Bejelentéstől függetlenül, ha az Előfizető a számára nyújtott szolgáltatást felhasználva szerverén olyan adatokat, információkat tárol, vagy továbbít, amely:
- jogosulatlanul megszerzett szerzői jogokat, a személyes adatok védelméhez való jogot sért.
- a társadalmi értékekre és az emberi méltóságra nézve sértő, különösen a félrevezető, trágár, szexuális, erőszakos tartalmú, a törvényellenes cselekedetre felbujtó, illetve vallási, politikai ellentétet szító tartalom;
- az Alaptörvénybe vagy a hatályos törvényekbe, jogszabályokba ütköznek; vagy
- az általa kínált termék tulajdonságairól vagy szolgáltatás tartalmáról, illetve ezek áráról bárkit félrevezethetnek

az Előfizető részéről súlyos szerződésszegésnek minősül.

Ha a szolgáltatás a fentiek alapján szünetel, Előfizető teljes díjfizetésre kötelezhető.
Abban az esetben, ha a Szolgáltató eszközeinek használatával olyan közzététel valósul meg, amely a fenti szabályokba nem ütközik ugyan, de jelentős társadalmi ellenállást vált ki vagy jelentős mértékben sérti a Szolgáltató üzleti érdekeit, a Szolgáltató fenntartja magának a jogot, hogy a közzétevőt azonosítsa, s vele tárgyalásokat kezdjen a közzététel megszüntetésére, és ennek tényét nyilvánosságra hozza.

Előfizető felelőssége, hogy honlapon, webshopon keresztül nyújtott szolgáltatása, közzététel megfeleljen a vonatkozó jogszabályoknak (különösen, de nem kizárólag az adatvédelmi rendelkezéseknek). Szolgáltató nem tehető felelőssé a meg nem felelés miatt. Előfizető felelőssége, hogy más fiókkal való összekötés esetén azokhoz engedéllyel rendelkezik.

Előfizető továbbá tudomásul veszi, hogy Szolgáltató teljes hozzáférési, visszakeresési, módosítási, terjesztési, korlátozási, törlési joggal rendelkezik Előfizető jelen szerződés keretében – akár az Előfizető, akár a Szolgáltató által – létrehozott, módosított honlapja tekintetében, beleértve az ilyen honlapnak működésére és kezelésére vonatkozó információt, a honlappal, webshoppal kapcsolatos bármely adatot, ide értve a tranzakciós adatokat, fizetési adatokat, személyes adatokat, a honlap, webshop látogatóinak adatait, függetlenül attól, hogy ezeket az adatokat a Szolgáltató az Előfizető, vagy a honlap, webshop látogatói hozzák létre, töltik fel közvetlenül vagy közvetve Előfizető honlapára, webshopjára. Előfizető felelőssége, hogy jelen rendelkezéshez szükséges hozzájárulásokkal rendelkezzen.

Vis maior
Vis maior a fél ellenőrzési körén kívül eső, a szerződés aláírásának időpontjában előre nem látható és el nem hárítható olyan esemény, amely akadályozza vagy lehetetlenné teszi a szerződésszerű teljesítést, így különösen az alábbiak:
a) természeti katasztrófa (villámcsapás, földrengés, árvíz, hurrikán és hasonlók);
b) tűz, robbanás, baleset,
c) járvány, járványügyi hatósági intézkedés;
d) radioaktív sugárzás, sugárszennyeződés;
e) terrorcselekmény, háború vagy más fegyveres konfliktus;
f) nemzetközi kereskedelmi korlátozás, embargó;

g) zendülés, rendzavarás, zavargások,
h) harmadik fél részéről történő rongálás.

Önmagában nem minősül előre láthatónak az olyan esemény, amelyhez hasonló esemény már történt, amennyiben az esemény a szerződés aláírásának időpontjában nem áll fenn.

A vis maior annyiban mentesíti az érintett felet a teljesítési kötelezettsége alól, amennyiben akadályozza vagy lehetetlenné teszi a szerződésszerű teljesítést. A vis maior feltételeinek fennállását az erre hivatkozó fél köteles bizonyítani.

Vis maior esemény felmerülésekor a fél köteles a másik felet erről haladéktalanul értesíteni, megjelölve azt is, hogy a vis maior esemény mely szerződéses kötelezettséget és mennyiben akadályoz vagy tesz lehetetlenné.

Ha a vis maior több, mint 6 (hat) hónapig folyamatosan akadályozza valamely felet a szerződésszerű teljesítésben, a szerződést bármelyik fél írásban, indokolással, azonnali hatállyal felmondhatja. A vis maior jogcímén történő felmondással összefüggésben a felek egymással szemben a felmondás előtt megvalósult részteljesítések elszámolásán felül semmilyen további igényt nem támaszthatnak.

Felek továbbá kifejezetten rögzítik, hogy járványok, valamint nemzetközi konfliktusok miatt a teljesítés során olyan problémák, akadályok keletkezhetnek akár harmadik félnél (pl. gyártó, szállító, egyéb közreműködő), amelyek akadályozhatják vagy késleltethetik a felek teljesítését. Az ilyen eset vis maiornak minősül és ennek megfelelően a kötelezett nem tehető felelőssé a késedelmes teljesítésért.

Felek szintén rögzítik, hogy a teljesítés során jogalkotói döntés alapján különleges jogrend került, vagy kerülhet kihirdetésre. A különleges jogrend miatt hatályba lépő intézkedések (beleértve bármely fél vagy a teljesítésbe bevont közreműködők által tett intézkedéseket) kihatással lehetnek a teljesítésre, akadályozhatják, késleltethetik a határidőben történő teljesítést. Az ilyen eset vis maiornak minősül és ennek megfelelően a kötelezett nem tehető felelőssé a késedelmes teljesítésért. Az ilyen intézkedések akkor is vis maiornak minősülnek, ha esetleg korábban már hasonló intézkedés került átmeneti időre bevezetésre.

Felek szintén rögzítik, hogy általánosan ismert világpiaci jelenség, hogy egyes gyártók alkalmanként nem vállalnak teljesítési határidőt, illetve alkalmanként a vállalt határidőt sem tudják tartani. A gyártó, kizárólagos disztribútor, forgalmazó miatt felmerülő késedelem, nem teljesítés esetén a jelen szerződés szerinti kötelezett mentesül a felelősség alól. A jelen szerződés szerinti kötelezett jogosult a szerződéstől egyoldalúan, külön jogkövetkezmények nélkül elállni vagy azt felmondani, amennyiben a gyártó, kizárólagos disztribútor, forgalmazó miatt felmerülő késedelemre tekintettel a szerződés fenntartása észszerűen nem várható el tőle.

Korrupcióellenes rendelkezés

Előfizető kijelenti, hogy tudatában van a Magyar Telekom Csoport etikus üzleti magatartási és korrupcióellenes szabályainak, valamint a jelen szerződésre alkalmazandó korrupcióellenes jogszabályoknak való megfelelőségi kötelezettségének, amelyet felek figyelembe vettek a jelen szerződés megkötése során.

Felek kijelentik és szavatolják, hogy az etikus és jogszerű üzleti magatartásnak megfelelően a szerződésben foglalt minden üzleti döntés, valamint a szerződéses feltételek kialakítása kizárólag jogszerű üzleti szempontok alapján történt.

A jelen szerződésre alkalmazandó korrupcióellenes szabályoknak való meg nem felelés esetén Szolgáltató jogosult a jelen szerződést azonnali hatállyal felmondani, vagy attól elállni.

Szankciós megfelelőség

Az Előfizető kijelenti és szavatol azért, (i) hogy sem az Előfizető, sem pedig az Előfizető tulajdonosi körébe tartozó, vagy az Előfizető felett befolyással rendelkező, vagy az Előfizető érdekkörébe tartozó, a jelen szerződés teljesítéséből gazdasági előnyre szert tevő más személy nem szerepel olyan, az Európai Unió, az Amerikai Egyesült Államok vagy a jelen szerződés alapján végzett gazdasági cselekményekre alkalmazandó más állam által elfogadott ellenőrzési vagy tiltólistán, illetve (ii) hogy a jelen szerződés alapján nyújtott szolgáltatások, illetve értékesített termékek Előfizető általi fogadásának, igénybevételének, a termékek birtokbavételének, illetve felhasználásának földrajzi helye nincs olyan országban, illetve területen, amelynek okán a jelen szerződés Szolgáltató által történő teljesítése – ideértve különösen de nem kizárólagosan a jelen szerződés alapján teljesített szolgáltatások nyújtását, illetve termékek értékesítését – gazdasági, kereskedelmi vagy pénzügyi szankció alá esne vagy jogszabályba ütközne. Az Előfizető kijelenti továbbá és szavatol azért, hogy a jelen szerződés alapján a Szolgáltató által nyújtott szolgáltatásokat, illetve az értékesített termékeket a teljesítés során és azt követően sem fogja oly módon használni, eltéríteni, tovább közvetíteni, értékesíteni vagy egyéb módon továbbadni, amely az Európai Unió, az Amerikai Egyesült Államok vagy a jelen szerződés alapján végzett gazdasági cselekményekre alkalmazandó más állam által elfogadott gazdasági, kereskedelmi, pénzügyi szankciós vagy exportellenőrzési szabályokba ütközne.

Az Előfizető vállalja és szavatol azért, hogy a fenti nyilatkozat a szerződés teljes időtartama alatt megfelel a valóságnak; ha pedig valószínűsíthető, hogy a körülmények megváltozása folytán az Előfizető az itt vállalt szavatosságnak már nem tud megfelelni, akkor erről a körülményről, az okok és a vonatkozó jogszabályi rendelkezések részletes bemutatásával együtt, köteles a Szolgáltatót haladéktalanul értesíteni. Kérésre az Előfizető észszerű időn belül részletes és szakszerű információt szolgáltat a Szolgáltatónak az Előfizető által igénybe vett szolgáltatások, illetve az általa megvásárolt vagy birtokba vett termékek felhasználásának körülményeiről, így különösen azok földrajzi helyéről, a felhasználás jellegéről és céljáról és a végfelhasználókról.

Ha az Előfizető bármely, a fenti pontokban foglalt kötelezettségét megszegi, az súlyos szerződésszegésnek minősül, amelynek alapján a Szolgáltató a szerződéstől részben vagy egészben azonnali hatállyal elállni vagy a szerződést azonnali hatállyal felmondani, a szerződésszegésből eredő kárát pedig Előfizetővel szemben érvényesíteni.

Átruházási és megterhelési tilalom
Szolgáltató előzetes írásbeli hozzájárulása nélkül Előfizető nem jogosult sem részben sem egészben harmadik személyre engedményezni vagy átruházni a szerződésből fakadó követeléseit, kötelezettségeit és jogait, továbbá azokat zálogjoggal vagy egyéb módon megterhelni.

Teljességi klauzula
A jelen szerződés a mellékleteivel együtt tartalmazza a felek teljes megállapodását. Nem válnak a felek megállapodásának részévé a jelen szerződés megkötését megelőző tárgyalások és üzleti egyeztetések során készült dokumentumok, nyilatkozatok és feljegyzések. A felek minden korábbi azonos tárgyra vonatkozó megállapodása a jelen szerződés hatályba lépésével hatályát veszti. Felek a Ptk. 6:63. § (5) bekezdésének alkalmazását kizárják.

Fenntarthatóság
Előfizető további díj, költség felszámítása nélkül tűrni köteles, hogy Szolgáltató a fenntarthatósági követelményrendszerének körében Előfizetőnél auditot folytathasson (ez magában foglalhatja a webauditot is), továbbá vállalja, hogy kérés esetén információt ad.
Az audit igényét Szolgáltató köteles előre jelezni és azt saját költségén, Előfizető működésének ésszerűtlen mértékű zavarása nélkül végrehajtani.

Irányadó jog
A jelen szerződésre a magyar jog az irányadó.
A jelen szerződéssel kapcsolatban a felek között felmerülő jogviták esetére a felek alávetik magukat a magyar bíróságok kizárólagos joghatóságának és – hatáskörtől függően – a Budai Központi Kerületi Bíróság, illetőleg a Tatabányai Törvényszék kizárólagos illetékességének.

1. sz. melléklet: Domain megrendelő
2. sz. melléklet: Adatkezelési megállapodás

Kelt:

....

Méry Katalin Visky Dávid Előfizető

Magyar Telekom Nyrt.

1. sz. melléklet

DOMAIN NÉV REGISZTRÁCIÓS, ÉS FENNTARTÁSI ÉS MÓDOSÍTÁSRA VONATKOZÓ SZERZŐDÉS
Regisztrátor/Szolgáltató: Magyar Telekom Távközlési Nyrt. (továbbiakban Szolgáltató), 1097 Budapest, Könyves Kálmán krt. 36.) Bankszámla szám: 10700024-04021609-51100005, Adószám: 10773381-2-44, Cégjegyzékszám: Cg. 01-10-041928 Székhely: 1097 Budapest, Könyves Kálmán krt. 36., Postacím: 1519 Budapest, Pf. 434. Internetes honlap címe: http://www.telekom.hu/ Kapcsolattartásra alkalmas elérhetőség a Szolgáltató részéről: Név: Magyar Telekom Nyrt. Központi Ügyfélszolgálat Postacím: 1276 Budapest Pf. 1400 Telefonos Ügyfélszolgálat és hibabejelentő: 1400 (A hét minden napján, 0-24 óráig A Magyar Telekom vezetékes és mobil hálózatából díjmentesen hívható E-mail cím: **domain@telekom.hu** (uzleti@telekom.hu)
◯ **Új igény VÁLASZTOTT DOMAIN NÉV (.hu, .com, .eu, .org, .net, .info, .biz,):** _____ Kiterjesztést szükséges megadni. A domain regisztrációhoz szükséges csatolandó dokumentumok: aláírási címpéldány (elektronikus aláírás esetén nem szükséges), cégbírósági végzés, átadás-átvételi nyilatkozat (csak domain használó váltás esetén). A domain a DNS1, DNS2 névszerver által generált tárhelyre és levelező szerverre kerül beállításra, vagy az 1. sz. mellékletben megadottak szerint, vagy felek külön megállapodása szerint. ◯ szolgáltató váltás (DOMAIN NÉV: _____) Kérem a megjelölt domain név jelenlegi szolgáltatótól történő áthozatalát és a domain további fenntartását, továbbá megbízom a Szolgáltatót a fentnevezett domain névvel kapcsolatos regisztrátori teendők további ellátására.

IGÉNYLŐ ADATAI (kötelezően kitöltendő)	
Szerződő fél neve:	Tel.: +36-
Cégjegyzékszáma:	Adószáma:
Szerződő fél székhelye: _____ (ir.szám) _____ (város) _____ (közterület) _____ (házszám)	E-mail címe:

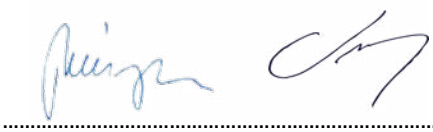
Kétfaktoros megerősítő eljárás adatai (.hu domain esetén kötelezően kitöltendő)
Tel.: +36-
E-mail címe:
Az Igénylő tudomásul veszi, hogy faktoros azonosítás keretében történő elfogadás esetén a jognyilatkozat megtettnek minősül. Tudomásul veszi továbbá a faktoros azonosítással járó kockázatokat, így azt, hogy az, aki az általa megadott faktorokkal rendelkezik, az a domainnel kapcsolatban korlátlanul rendelkezhet, akár a tudtán kívül. Igénylő tudomásul veszi, hogy a faktor adatok feletti rendelkezés megőrzésére különös figyelmet kell fordítania.

SZERŐDÉSI FELTÉTELEK

1. Igénylő kijelenti, hogy a nyilvántartói szabályzatokat, előírásokat (különösen a Domainregisztrációs Szabályzatot) megismerte és elfogadja. A nyilvántartó az adott közdomain kezelője. A .hu domain esetében ISZT Nonprofit Kft. (továbbiakban: Nyilvántartó).
2. Igénylő kijelenti, hogy a domain regisztrálásával, delegálásával és fenntartásával kapcsolatban a Szolgáltató és a Nyilvántartó döntését elfogadja. Igénylő tudomásul veszi továbbá, hogy Domainregisztrációs Szabályzatnak való megfelelőségével kapcsolatos vita esetén a Szolgáltató és a Nyilvántartó álláspontja a döntő. A választott domain névvel kapcsolatos vitás kérdésekben aláveti magát az Alternatív Vitarendező Fórum döntésének, és tudomásul veszi, hogy a választott domain névvel kapcsolatosan ellene indult jogvitában jogorvoslati igényt kizárólag a Kérelmezővel szemben érvényesíthet. Továbbá, az alternatív vitarendezés során hozott döntés végrehajtásáért sem a Szolgáltató, sem a Nyilvántartó nem felel.
3. Az Igénylő tudomásul veszi, hogy a .hu domain nevek regisztrálásához, és egyes módosításához többfaktoros hitelesítés szükséges. Az Igénylő tudomásul veszi, hogy a megerősítő faktoros hitelesítéssel lehetséges a Domainregisztrációs Szabályzatban ekként előírt módosítások végrehajtása.
4. Igénylő tudomásul veszi, hogy ha eltér az igénylő és a faktor adatokban megadott elérhetőség, a .hu domain esetében a Nyilvántartó mindkét elérhetőségre küldhet értesítéseket.
5. Igénylő tudomásul veszi, hogy a megadott értesítési és faktor adatokat, a Szolgáltató a Nyilvántartónak továbbítja. Nyilvántartó az adatok kezelését az Adatkezelési Tájékoztatójában foglaltak szerint végzi.
6. A felek rögzítik, hogy a Nyilvántartónak történő adattovábbítás jogalapja az általános adatvédelmi rendelet (GDPR) 6. cikk (1) bekezdés f) pontja szerinti jogos érdek.
7. Igénylő tudomásul veszi, hogy a domain regisztrálást és delegálását saját kockázatára igényli, és sem a Szolgáltatót, sem a Nyilvántartót nem terheli felelősség sem a domain regisztrálásából, delegálásából, sem annak elutasításából, felfüggesztéséből, vagy visszavonásából esetlegesen keletkező károkért. Igénylő kizárólagosan felel az általa igényelt domain név megválasztásáért, jelentéstartalmáért, használatáért és ezek következményeiért. A Szolgáltató a választott név ellenőrzésére, jogszerűségének semmilyen vizsgálatára nem köteles. Az Igénylő részére delegált domainnel, a regisztrációs eljárással, a domain nevének megválasztásával, jelentéstartalmával vagy használatával kapcsolatos bármilyen jogvitából, kárból, követelésből következő költség alól tehermentesíti a Szolgáltatót. Domain fenntartásra vonatkozó szerződés hiányában, a domainhez tartozó tárhely/levelező szolgáltatás nem vehető igénybe
8. Nemzetközi domain név regisztráció szabályzata a GoDaddy UK Legal Agreements | Our TOS Agreement - GoDaddy UK, iDotz.Net Registrar Reseller Program (iRRP.Net) Agreement, iDotz.Net | Create a Professional Website, Blog, Portfolio or Online Store | Domain Name Registrar: Search.. Name.. Succeed! és a Document repository - EURid oldalakon érhetőek el.
9. A Szolgáltató szerződésszegéssel okozott károkért való felelőssége kizárólag a tapadó károkra (azaz a szolgáltatás tárgyában bekövetkezett károkra) terjed ki. A Szolgáltató nem felelős a következménykárokért (korlátozás nélkül ideértve az adatvesztésből eredő károkat is).
10. A felek a Szolgáltató kártérítési felelősségének mértékét a jelen szerződés megszegésével okozott károkért káreseményenként legfeljebb a szerződés tárgyát képező szolgáltatás éves díjának 50%-ára korlátozzák azzal, hogy a szerződés teljes időtartama alatt a Szolgáltató szerződésszegésből fakadó kártérítési kötelezettségeinek összértékét a felek legfeljebb a szerződés tárgyát képező szolgáltatás teljes futamidőre számított ellenértéke teljes nettó összegének 100%-ára korlátozzák.
11. Szándékosan okozott, továbbá emberi életet, testi épséget vagy egészséget megkárosító szerződésszegésért való felelősségre a fenti felelősségkorlátozó rendelkezések nem vonatkoznak.
12. A kártérítési felelősség alól bármely fél mentesül akkor, ha úgy járt el, ahogy az az adott helyzetben általában elvárható.
13. Jelen szerződés felek aláírásával lép hatályba a domain név delegálásától számított 12 hónapra. Felek a határidő leteltét legalább 30 nappal megelőző tett ellenkező tartalmú nyilatkozat hiányában jelen szerződés a 12 hónap lejártakor újabb 12 hónapos időtartamokra megújul. Felek a jelen szerződést 30 napos rendes felmondással bármikor felmondhatják, ebben az esetben a díj arányos részét Szolgáltató megfizeti Igénylő részére.
14. A Szolgáltató jogosult a szolgáltatás díját évente az előző évre vonatkozó – a KSH által hivatalosan kiadott – fogyasztói árindex-változásnak megfelelően módosítani a következő 12 hónapos időtartam kezdetétől.
15. A másik fél előzetes írásbeli hozzájárulása nélkül egyik fél sem jogosult sem részben sem egészben harmadik személyre engedményezni vagy átruházni a szerződésből fakadó követeléseit, kötelezettségeit és jogait, továbbá egyik fél sem jogosult azokat zálogjoggal vagy egyéb módon megterhelni. A jelen pont szerinti engedményezési és átruházási tilalom alól kivételt képez a Szolgáltató jelen szerződésből fakadó követeléseinek, kötelezettségeinek és jogainak a Szolgáltató kapcsolt vállalkozására történő engedményezése vagy átruházása, továbbá a Vállalkozó jelen szerződésből fakadó követeléseinek és jogainak harmadik személyre történő engedményezése vagy átruházása, melyhez jelen szerződés aláírásával igénylő előzetesen és visszavonhatatlanul hozzájárul.
16. A jelen szerződésre a magyar jog az irányadó.
17. A jelen szerződéssel kapcsolatban a felek között felmerülő jogviták esetére a felek alávetik magukat a magyar bíróságok kizárólagos joghatóságának és – hatáskörtől függően – a Budai Központi Kerületi Bíróság, illetőleg a Tatabányai Törvényszék kizárólagos illetékességének.

Igénylő kijelenti, hogy a jelen megállapodással kapcsolatban az általa megadott adatok a valóságnak megfelelnek. Abban az esetben, amennyiben az általa megadott adatokban változás következik be, arról a Szolgáltatót 15 napon belül írásban tájékoztatja. Igénylő továbbá tudomásul veszi, hogy amennyiben a megadott adatok nem valósak, vagy az adatok változását nem jelenti be, az a domain név visszavonását eredményezheti. Igénylő kijelenti továbbá, hogy Szolgáltató jogosult értesítéseket a megadott értesítési email címre küldeni.

Kelt:



Méry Katalin Visky Dávid

Magyar Telekom Nyrt.

Domain Igénylő (*cégszerű)* aláírása

2. számú melléklet

ADATKEZELÉSI MEGÁLLAPODÁS

az adatkezelők és az adatfeldolgozók közötti, az (EU) 2016/679 európai parlamenti és tanácsi rendelet 28. cikkének (7) bekezdése szerinti általános szerződési feltételekről (továbbiakban: SCC) alapján

Mellékletekkel és kiegészítésekkel

A SZERZŐDÉS TÁRGYA:

Az Európai Bizottság Általános Szerződési Feltételeket ("Feltételek") tett közzé a (EU) 2016/679 európai parlamenti és tanácsi rendelet (GDPR) 28. cikk (3) és (4) bekezdésének való megfelelés érdekében (https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj?locale=hu).
Felek megállapodnak, hogy a II. Mellékletben körülírt adatkezelésre ezen Feltételeket alkalmazzák az alábbi I-V Mellékletekben foglalt eltérésekkel és pontosításokkal.

A Feltételek módosítása nem megengedett.

I. MELLÉKLET

A felek jegyzéke

Adatkezelő

1.

Adatkezelő neve:	
Adatkezelő e-mail címe:	
Székhelye:	
Kapcsolattartó személy neve (operatív felelős):	
Pozíciója:	
E-mail címe:	
Adatvédelemért felelős kapcsolattartó személy (vagy ha van kijelölt adatvédelmi tisztviselő, az ő neve:	
Pozíciója:	
E-mail címe:	

Adatfeldolgozó:

1.

Adatfeldolgozó neve és elérhetősége:	Magyar Telekom Nyrt.
Székhelye:	1097 Budapest, Könyves Kálmán krt. 36.
Kapcsolattartó személy neve, pozíciója és elérhetősége (operatív felelős):	
Adatvédelemért felelős kapcsolattartó személy (vagy ha van kijelölt adatvédelmi tisztviselő, akkor az ő) neve, pozíciója és elérhetősége:	dr. Esztervári Adrienn, Data Protection Officer dpo@telekom.hu

II. MELLÉKLET

Az adatkezelés leírása

A. Az érintettek azon kategóriái, akiknek a személyes adatait kezelik (annak jelzése, hogy ügyfelek, munkavállalók vagy más személyek (ideértve például a beszállítókat) adatai)

Az adatkezelő regisztrált felhasználói, kapcsolattartói. A szolgáltatás részeként összeállított honlapon tárolt személyes adatok érintettjei.

B. A kezelt személyes adatok kategóriái

A szolgáltatás részeként összeállított honlapon tárolt személyes adatok és a regisztrált felhasználói, kapcsolattartói.

C. Kezelt különleges személyes adatok (amennyiben releváns, pl. egészségügyi adatok, szakszervezeti tagság, biometrikus adatok stb) és az alkalmazott korlátozások vagy garanciák, amelyek teljes mértékben figyelembe veszik az adatok jellegét és a kapcsolódó kockázatokat, így például szigorú célhoz kötöttség, hozzáférési korlátozások (ideértve ha kizárólag speciális képzésben részt vett személyzet kap hozzáférést), az adatokhoz való hozzáférés nyilvántartása, az adattovábbításra vonatkozó korlátozások vagy további biztonsági intézkedések:

Nem történik ilyen adat kezelése.

D. Az adatkezelés jellege (Milyen szolgáltatások kerülnek nyújtásra? Hogyan fogják az adatokat kezelni, pl. továbbítják/módosítják is):

A Szolgáltató az Előfizető részére a választott díjcsomag szerint honlapot, vagy webshopot készít a Wix.com Ltd. platformján. A szerződés szerint az Előfizetői adatokat a honlap,illetve a webshop szerkesztéséhez használják fel, illetve a szolgáltatás nyújtásának érdekében továbbítja a Wix.com Ltd. részére.

E. Az Adatkezelő nevében végzett adatkezelés célja(i) (milyen célból kerül kezelésre az adat):

A szolgáltatás nyújtása.

F. Az Adatfeldolgozó általi adatkezelés időtartama:

A szolgáltatás nyújtásának időtartamával egyezik meg.

G. MEGÁLLAPODÁS OPCIONÁLIS RENDELKEZÉSEKRŐL

5. feltétel, a dokkolási mechanizmusról szóló rendelkezés alkalmazandó

III. MELLÉKLET

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

Felek az I. számú Függelékben részletezett intézkedésekben állapodnak meg azzal, hogy az I. számú Függelékben található rendelkezések közül, az abban meghatározott, az alább kiválasztott változathoz tartozó rendelkezések alkalmazandók:

1. Változat:

- Az Adatfeldolgozó a saját (vagy egy al-adatfeldolgozó) IT infrastruktúráját (szerver/kliens/applikáció) vagy a saját végberendezését használja kizárólagosan vagy kiegészítésképpen
  vagy

Az adatkezelés megszervezésével kapcsolatos biztonsági intézkedéseket az Adatkezelővel közösen kell megállapítani.

IV. MELLÉKELT

További adatfeldolgozók (al-adatfeldolgozók) jegyzéke (ideértve a további al-adatfeldolgozókat is)

A) Adatkezelő az alábbi al-adatfeldolgozók alkalmazását engedélyezi:

1.

Az al-adatfeldolgozó neve és kapcsolattartási adatai:	Atlassian Corp.
Székhelye:	350 Bush Street, Floor 13, San Francisco, California, 94104
Kapcsolattartó személy neve, pozíciója és elérhetősége (operatív felelős):	
Adatvédelemért felelős kapcsolattartó személy (vagy ha van kijelölt adatvédelmi tisztviselő, akkor az ő) neve, pozíciója és elérhetősége:	privacy@atlassian.com
Az adatkezelés leírása (beleértve a felelősségi körök egyértelmű elhatárolását amennyiben több al-adatfeldolgozó engedélyezésére került sor):	Az adatfeldolgozó szerződése szerint, a regisztrált felhasználók személyes adatainak kezelése történik a szolgáltatói szerződés teljesítése céljából.
Adatok továbbítása (ideértve az onnan történő hozzáférést is) harmadik országba (az EU-n kívülre):	igen/nem
Harmadik ország:	Egyesült Királyság, USA

Az alábbi jóváhagyási folyamat alkalmazandó további al-adatfeldolgozók és al-al-adatfeldolgozók alkalmazásához (7.7. feltétel):

ÁLTALÁNOS ÍRÁSOS ENGEDÉLY: Az Adatfeldolgozó jelen szerződés aláírásával rendelkezik az Adatkezelő általános engedélyével ahhoz, hogy az elfogadott listáról további Adatfeldolgozó(ka)t vegyen igénybe. Az Adatfeldolgozó írásban kifejezetten tájékoztatja az Adatkezelőt az említett lista bármely tervezett módosításáról a további adatfeldolgozók hozzáadása vagy lecserélése révén, legalább 15 nappal korábban, elegendő időt biztosítva az Adatkezelőnek arra, hogy az érintett további adatfeldolgozó(k) megbízása előtt kifogást emelhessen az ilyen változtatásokkal szemben. Az Adatfeldolgozó megadja az Adatkezelőnek azokat az információkat, amelyek szükségesek ahhoz, hogy az Adatkezelő a tiltakozáshoz való jogát gyakorolhassa

V. MELLÉKLET

További megállapodások

1. Nemzetközi adattovábbítások

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 vagy az (EU) 2018/1725 rendelettel összhangban kell végrehajtani.

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 által 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.

I. Függelék

Technikai és szervezési adatvédelmi intézkedések

Tartalomjegyzék

1. Bevezető rendelkezések

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

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

Az alábbi táblázatban az adott változatok esetén alkalmazandó rendelkezések találhatók:

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

1.1 A jelen dokumentumra vonatkozó felhasználói utasítások

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

1.2 Fogalom-meghatározások

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

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

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

2. Technikai és szervezési intézkedések

1. Adatvédelmi cél - Rendelkezésre állás

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

1.1. Követelmény Fizikai védelem a külső fenyegetésekkel szemben

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

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

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

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

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

1.3. Követelmény A rendszer megerősítése

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

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

1.4 Követelmény Backup koncepció

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

1.5. Követelmény A védelmi célok biztosítására vonatkozó személyzeti koncepció

Az adatfeldolgozó olyan személyzeti koncepciót vezetett be, amely az alábbi intézkedésekkel támogatja az adatvédelmet:

- Csak olyan szakértő személyeket alkalmaznak, akik bizonyíthatóan részt vettek a szükséges adatvédelmi képzéseken, és megfelelő titoktartási kötelezettség alatt állnak.
- A személyes adatok minden feldolgozásához felelős kapcsolattartó kerül kijelölésre. Rendelkeznek érvényes helyettesítési protokollal.

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

1.6. Követelmény Vészhelyzeti intézkedések az adatfeldolgozási tevékenység helyreállítása céljából

Az adatfeldolgozó vészhelyzeti tervet / koncepciót vezetett be az adatfeldolgozás helyreállítására. A koncepció célja a rendelkezésre állás helyreállítása egy esetleges incidenst követően. A vészhelyzeti koncepciónak meg kell felelnie a következő követelményeknek/kritériumoknak:

- Vannak olyan szabályok, amelyek egy incidenst követően meghatározzák az adatfeldolgozás helyreállításához szükséges időt.
- Az adatok helyreállításához szükséges erőforrások rendelkezésre állnak
- A felelősségi körök kijelölésre kerültek
- Meghatározták az incidens elleni védekezésre és a szabályos működés helyreállítására vonatkozó ellenőrzött intézkedéseket
- Megvannak az információs és eszkalációs láncok
- Meghatározták a megfelelő folyamatokkal és szabályokkal (backup tervvel, személyi koncepcióval stb.) való interakciókat

2. Adatvédelmi cél - Integritás

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

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

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

2.2. Követelmény Engedélyezési koncepció

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

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

2.3. Követelmény Identitáskezelés

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

2.4. követelmény Kriptográfia koncepció

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

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

A kriptográfiai koncepció célja:

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

2.5. Követelmény Az adatok naprakészségének biztosítására szolgáló folyamatok

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

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

3. Adatvédelmi cél - Bizalmasság

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

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

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

- A védelmi szint függvényében területeket határoznak meg; a szükséges biztonsági peremfeltételeket meghatározzák és végrehajtják. A védelmi szint besorolása a területeken található személyes adatok vagy információfeldolgozó rendszerek (beleértve a mobil munkaállomásokat is) alapján történik.
- Megfelelő beléptetési szabályokat határoznak meg és használnak, melyekkel biztosítják, hogy csak jogosult személyek lépjenek be a meghatározott területekre.
- A szervezetnél az adatvédelmi előírások és a biztonsági követelmények alapján rendszerhozzáférés szabályozási irányelvet kell kidolgozni és bevezetni. Ez az irányelv a személyes adatokhoz való hozzáférést a szükséges védelmi szint függvényében és a „szükséges ismeret" (need-to-know) alapelv szerint szabályozza. Ez különösen a személyes adatokat tartalmazó informatikai rendszerekhez, hálózatokhoz és adatbázisokhoz való hozzáférésre vonatkozik.
- Az adathordozók kezelésére vonatkozó eljárásokat a meghatározott védelmi szintnek megfelelően hajtják végre.
- Ha a személyes adatokat mobil adathordozókon tárolják, azokat hatékonyan kell titkosítani (lásd a 2.4. pontot).

- Az adathordozók szállítására vonatkozó szabályokat a személyes adatokra vonatkozó védelmi szintnek megfelelően hozzák létre. Ha a személyes adatokat nem titkosítják, megfelelő alternatív védelmi intézkedéseket kell hozni. Ha valamely területen magas szintű védelemre van szükség, különleges követelmények vannak a szállítás megbízhatóságára, az adatok titkosítására, valamint a dokumentációval, a naplózással és a bizonyítással kapcsolatos kötelezettségekre.
- Minden típusú kommunikációs berendezés (beleértve a mobil munkaállomásokat) esetében vannak irányelvek, biztonsági eljárások és ellenőrzések az információátvitel védelmére. A személyes adatok nyilvános hálózatokon keresztüli továbbítása esetén az adatokat mindig titkosítják.
- A szervezetnél a mobil eszközök (laptopok, külső adathordozók, mobiltelefonok) használatával kapcsolatosan beazonosított kockázatoknak megfelelően megfelelő iránymutatásokat és intézkedéseket hajtanak végre a személyes adatok bizalmas kezelésének és sértetlenségének biztosítására. Ezen szabályok célja a személyes adatokhoz való hozzáférés minimalizálása, tárolásuk és továbbításuk titkosítása, valamint a külső adathordozók használatának az abszolút minimumra csökkentése.

3.2. Követelmény Biztonságos hitelesítési eljárások

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

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

4. Adatvédelmi cél - Összekapcsolhatatlanság

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

4.1. Követelmény Az adatkezelés céljának meghatározása

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

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

4.2. Követelmény A célhoz kötöttség megvalósítását biztosító intézkedések

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

- A feldolgozás, felhasználás és továbbítás jogainak korlátozása az adatkezeléshez feltétlenül szükséges mértékig
- Szervezeti/területi határok szerinti elkülönítés

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

4.3. Követelmény Anonimizálási eljárások meghatározása, végrehajtása és alkalmazása

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

5. Adatvédelmi cél - Átláthatóság

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

5.1. Követelmény Az eljárások nyilvántartása

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

- Az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá - ha van ilyen - az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;
- Az egyes adatkezelők nevében végzetti tevékenységek kategóriái;
- Adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;
- Ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

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

5.2. Követelmény Az adatfeldolgozás dokumentálása

Az adatfeldolgozó a személyes adatok kezelését az alábbiak szerint dokumentálja:

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

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

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

5.4. Követelmény Az adatfeldolgozás naplózása

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

5.5. Követelmény Az információszolgáltatási kötelezettségek biztosítása

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

6. Adatvédelmi cél - Beavatkozás lehetősége

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

6.1. Követelmény Az érintettek jogaira vonatkozó folyamatok végrehajtása

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

- Kivéve, ha adatkezelő ezt már korábban bevezette, az adatfeldolgozónak folyamatot kell bevezetnie azon személyek azonosítására és hitelesítésére, akik szeretnék gyakorolni az érintettek jogait.
- Az adatkezelő és az adatfeldolgozó közösen határozzák meg azon jellemzőt, amellyel az érintettet a szervezeti határokon átnyúlóan egyértelműen azonosítani lehet.
- Az adatfeldolgozó olyan rendszereket, szoftvereket és eljárásokat vezetett be, amelyek lehetővé teszik a hozzájárulás, a hozzájárulás visszavonása és a tiltakozás differenciált lehetőségeit.
- Az adatfeldolgozó operatív lehetőségeket biztosított az egy adott személyre vonatkozóan tárolt összes információ összeállítására, helyesbítésére, zárolására és törlésére.
- Előnyben részesülnek azok az automatizált adatkezelési folyamatok (nem döntéshozatali folyamatok), amelyek a kezelt adatokhoz való hozzáférést elhagyhatóvá teszik, és a párbeszéd-vezérelt folyamatokhoz képest korlátozzák a befolyásgyakorlást.

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

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

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

7. Adatvédelmi cél - Adattakarékosság

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

7.1. Követelmény Operatív intézkedések az adatok minimalizálására

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

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

7.2. Követelmény Az adattakarékosságra irányuló technikai intézkedések

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

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

7.3. Követelmény Törlési koncepció meghatározása, végrehajtása és ellenőrzése

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

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