GDPR
kisokos

Felhívjuk a figyelmét, hogy jelen dokumentumban a GDPR aktuális szövegének és fogalmainak értelmezése olvasható, melyet a működő gyakorlat megváltoztathat.

A hatálybalépés 2018. május 25.-én esedékes, így a Rendelet jog alkalmazói gyakorlata még hiányzik, egyes kérdéskörök és módszertanok még nem kiforrottak.

Mi is az a GDPR?

A személyes adatok védelme, mint alapvető, de legfiatalabb emberi jog a XX. század közepén jelent meg és nőtt óriássá az informatikai csúcsfejlődés velejárójaként. A védelemre a századvég óta dolgoztak ki a nagyobb nemzetközi szervezetek, szerveződések iránymutatásokat, azonban a tagországok, egyes szuverén államok önmaguk alkották meg saját szabályrendszerüket. Az incidensek növekvő száma és egyre súlyosabb károkozási képessége arra késztette az Európai Uniót (is), hogy egy, minden tagállamra egységesen vonatkozó, modern és szigorú szabályrendszert hozzon létre, így 2018. május 25-i hatálybalépéssel létrejött az Általános Adatvédelmi Rendelet (General Data Protection Regulation).

Magyarországon a Nemzeti Adatvédelmi és Információszabadsági Hatóság (NAIH) felelős a GDPR betartatásáért, hatósági ellenőrzéseket folytathat le és a rendelkezések értelmében a nemmegfeleléseket szankcionálhatja.

A GDPR kulcselemei

FELDOLGOZÁS

Határozza meg adatkezelési, -feldolgozási, -gyűjtési, -rögzítési, -szervezési, -tárolási, vagy egyéb módon végzett tevékenységeinek törvényes alapját és frissítse adatvédelmi nyilatkozatát ennek magyarázása érdekében.

ELSZÁMOLTATHATÓSÁG

Biztosítsa, hogy hatósági audit során képes legyen bizonyítani megfelelését, mivel a GDPR kifejezetten előírja a felelősséget a vállaltok számára. Határozza meg, melyek azok a megfelelő technikai és szervezeti intézkedések, melyek biztosítják és bizonyítják a megfelelést.

BELEEGYEZÉS

A hozzájárulás az egyén szabadon választott, adott, konkrét és egyértelmű engedélye. Ügyeljen arra, hogy a hozzájárulások elkülönüljenek egymástól és azokat szabadon adják – hallgatás, inaktivitás és előre kipipált check-boxok már nem minősülnek opt-in-nek.

ÁTLÁTHATÓSÁG

A GDPR a magánszemélyek adatainak védelmére hivatott, vagyis fontos ügyelnie arra, hogy tevékenysége során az adatok tulajdonosai egyértelműen, világosan, könnyen és ingyenesen tudomást szerezhessek arról, pontosan mihez adták meg adataikat – ennek legjobb módja egy komplex adatkezelési tájékoztató.

Kire vonatkozik?

Uniós Rendelet lévén a GDPR-t közvetlenül alkalmazni kell valamennyi olyan vállalkozás esetén, mely az EU területén fejti ki tevékenységét és ez a tevékenység adatkezeléssel összefüggésben valósul meg.

Adatkezelő vagy adatfeldolgozó?

Az adatkezelés magába foglal szinte minden személyes adatokon végzett tevékenységet, így aki ezek valamelyikével foglalkozik, az Adatkezelőnek minősül.

- felvétel
- gyűjtés
- tárolás
- felhasználás
- továbbítás
- módosítás

Az Adatfeldolgozó az adatkezelő nevében és annak megbízásából dolgozik személyes adatokkal – tulajdonképpen csupán utasításokat hajt végre (üzemeltetés), de a célokat és a döntéseket az adatkezelő határozza meg.

PRIVACY BY DESIGN

Legyen Ön akár adatkezelő, akár adatfeldolgozó, tevékenységet úgy kell terveznie, hogy az adatvédelem és azok követelményei már kezdetektől részt vegyenek a rendszerek és folyamatok életciklusaiban.

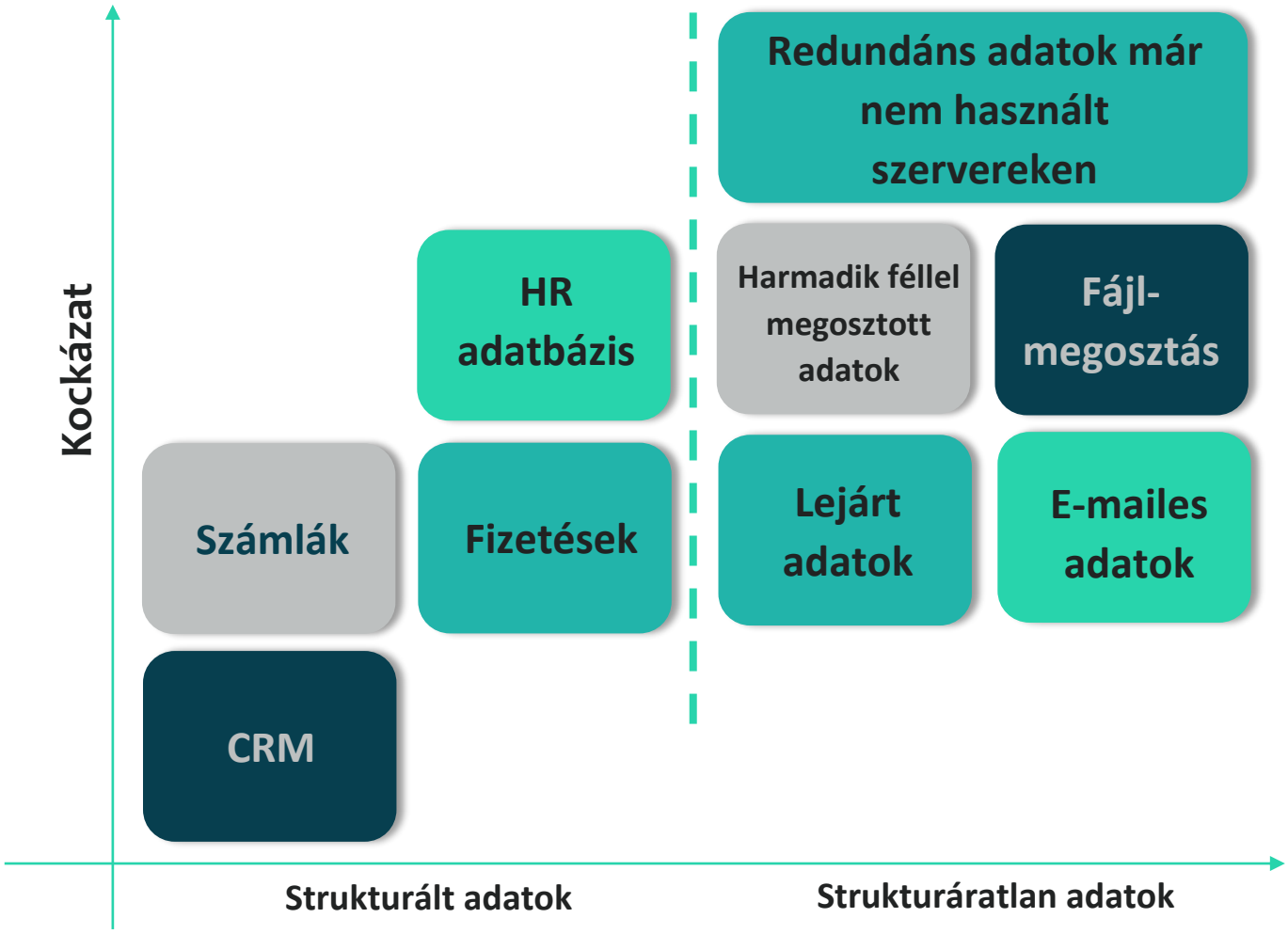
PRIVACY BY DEFAULT

Legyen Ön akár adatkezelő, akár adatfeldolgozó, tevékenységet úgy kell működtetnie, hogy az adatvédelem és azok követelményei alapértelmezett funkcióként vegyenek részt a rendszerek és folyamatok életciklusaiban.

A BÍRSÁG MÉRTÉKE ELÉRHETI 20 MILLIÓ EURÓT, VAGY A TELJES VILÁGPIACI ÁRBEVÉTEL 4 % - ÁT.

Miért van erre szükség?

Egy közepes méretű vállalat Magyarországon 10 GB adatot, információt tárol, gyűjt, dolgozik fel, használ és kezel **dolgozónként.** Az alábbiakban összegyűjtöttük a leggyakoribb típusokat, továbbá diagrammunkon jól látszik a kockázat – strukturáltság összefüggése:



Mi a személyes adat?

Amikor egy entitás kapcsán felmerül a kérdés, hogy vajon személyes adat-e, a válasz nagy valószínűséggel igen. A Rendelet így fogalmaz: „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó *bármely* információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

A TOVÁBBIAKBAN A TELJESSÉG IGÉNYE NÉLKÜL MUTATJUK BE, MENNYIRE SZÉLESKÖRŰ A SZEMÉLYES ADAT ÉRTELMEZÉSE:

Azonosító adatok (név, titulus, cím, telefonszám), **kormány által kiadott azonosító adatok** (útlevél szám, engedély szám, nyugdíjszám, rendszám), **elektronikus azonosítási és lokációs adatok** (IP címek, cookie-k, GSM, GPS), **biometrikus azonosítási adatok*** (DNS adatok, ujj és hangnyomatok, arcfelismerés, retina kép), **pénzügyi források** (jövedelem, befektetések, megtakarítás, eszközköltségek), **adók, költségek** (kiadások, bérleti díjak, kölcsönök), **nyugdíj** (a nyugdíjrendszerben való részvétel időpontja, a rendszer jellege, a beérkezett és végrehajtott kifizetések) **személyes tulajdonságok** (kor, nem születési idő, születési hely, családi állapot, nemzetiség, katonai státusz, bevándorló státusz) **fizikai leírás** (méret, súly, hajszín, szemszín, megkülönböztető tulajdonságok), **családi állapot** (jelenlegi életforma, többi családtag adatai), **igazságügyi adatok** (a bejegyzett személy által, vagy ellen indított nyomozások vagy peres eljárások, büntetések és ítéletek, gondnokság, ideiglenes gyámság, fogva tartás, elhelyezés), **lakhatási adatok** (az ingatlan elhelyezkedése: a tulajdon tulajdonában lévő, vagy bérelt ingatlan jellege, ezen a címen való tartózkodás időtartama, bérleti díj, kulcstulajdonosok nevei), **egészségügyi adatok** (orvosi nyilvántartás, orvosi jelentés, diagnózis, kezelés, fogyatékosság vagy rokkantság, egyéb különleges egészségügyi paraméterek vagy egészségügyi státusz egy utazás vagy otthon kezelés során.) **képzési adatok** (képzési életút, a tanulmányok pénzügyi áttekintése, szakmai kompetencia, szakmai tapasztalat, szakmai szervezetekben való részvétel / részvétel) **munkahelyi adatok** (felvétel időpontja, felvételi mód, felvétel forrása, referenciák, a próbaidő részlete, korábbi munkahelyek és munkáltatók, távollétek, szolgáltatási kötelezettség, fizetések és kifizetések, jutalékdíjak, bónuszok, kiadások), **országos nyilvántartási szám, faji vagy etnikai adatok, szexuális életről szóló adatok, politikai hovatartozás, politikai kapcsolatok.**

* a kiemelt adatok a Rendelet alapján jellegükből és szenzitivitásukból adódóan **különleges / érzékeny** adatnak minősülnek.

A vállaltok kötelezettségei

Minden vállalat – legyen az akármekkora – köteles megvédeni azon személyek adatait, akik megadják azokat bármilyen céllal.

KOMMUNIKÁCIÓ

Világosan és (akár gyerekek számára is) közérthetően mondja el, hogy ki is Ön, mivel foglalkozik és miért végez adatokkal kapcsolatos tevékenységet.

BELEEGYEZÉS

Az érintett akaratának önkéntes megnyilvánulása, mely konkrét és megfelelő tájékoztatáson alapul. Szerezze meg adatkezeléseihez a beleegyezéseket, amennyiben gyerekek is érintettek, úgy győződjön meg a szülői hozzájárulás meglétéről.

TÁJÉKOZTATÁS

Hívja fel az érintettek figyelmét az esetleges adatsértések kockázatára és annak mértékére.

MOBILITÁS

Önnek, mint adatkezelőnek, lehetővé kell tennie, hogy az érintettek hozzáférjenek adataikhoz és ezt más vállalatok számára is megadhassák azokat.

PROFILKÉSZÍTÉS

Amennyiben a személyes adatok kezelését bármely formában automatizálja (elemzések és előrejelzések), gondoskodnia kell arról, hogy ezt ne csupán gép végezze (manuális felülvizsgálat). Tájékoztassa az érintetteket az automatizált kezelésről.

MARKETING

Adja meg a lehetőséget az érintettek számára, hogy kimaradjanak a direkt marketingből (opt-out-lehetőségek).

ADATOK TÖRLÉSE

Adja meg a lehetőséget az érintettek számára, hogy adataikat rendszere „elfelejthesse”, amennyiben ők kifejezetten ezt kérik.

ÉRZÉKENY ADATOK VÉDELME

Biztosítsa, hogy azok az adatok, melyek a különleges kategóriák-ba tartoznak és szenzitív-nek minősülnek, további védelmi intézkedé-sekkel vannak ellátva.

UNIÓN KÍVÜLI ADATTOVÁBBÍTÁS

Azokban az esetekben, mikor az adattovábbítás az uniós hatóságok által jóvá nem hagyott országokba történik, biztosítsa, hogy további jogi intézkedéseket vezetett be.

Kötelező (?) elemek

Vizsgálja meg, hogy a GDPR egyes kötelező tartalmi elemei vonatkoznak-e az Ön vállalatára!

DPO – ADATVÉDELMI TISZTVISELŐ KINEVEZÉSE

Legyen Ön akár adatkezelő, akár adatfeldolgozó, az alábbi esetekben Adatvédelmi tisztviselőt szükséges kineveznie:

- közhatalmi vagy közfeladatot ellátó szerv;
- a tevékenység az érintetettek szisztematikus, nagymértékű megfigyelését teszik lehetővé;
- a kezelt adatok különleges, vagy bűnügyi kategóriába tartoznak.

NYILVÁNTARTÁS

Legyen Ön akár adatkezelő, akár adatfeldolgozó, az alábbi esetekben Adatvédelmi Nyilvántartást szükséges vezetnie:

- az adatkezelés rendszeres;
- veszélyezteti az egyének jogait és szabadságait;
- érzékeny vagy bűnügyi adatokat érint.

A nyilvántartásnak az alábbi paramétereket kell tartalmaznia:

- a vállalkozás alapinformációi (név és elérhetőség);
- adatkezelés indoklása;
- adatkategóriák ismertetése;
- adattovábbítás címzettjei;
- adattörlés határideje – megőrzési idő;
- végrehajtott biztonsági intézkedések.

DPIA – ADATVÉDELMI HATÁSVIZSGÁLAT

Legyen Ön akár adatkezelő, akár adatfeldolgozó, az alábbi esetekben Adatvédelmi Hatásvizsgálatot szükséges végeznie:

- magas kockázatú adatok feldolgozása;
- új technológiák bevezetése;
- profilalkotás és automatikus döntéshozatal;
- közterületek kiterjedt megfigyelése;
- érzékeny adatok.