GDPR

Alapok KKV-k számára

GDPRlite

Útmutató a GDPR megfeleléshez a magyar kis- és középvállalatok számára a Security.hu ajánlásával

Jelen dokumentumban a GDPR hatályos szövegének és fogalmainak értelmezése olvasható, melyet a működő gyakorlat megváltoztathat. Mivel a kötelező érvényű alkalmazás 2018. május 25.-től lép életbe, így a Rendelet jogalkalmazói gyakorlata még hiányzik, egyes kérdéskörök és módszertanok még nem kiforrottak.

Tartalom

Mi is a GDPR?

Az internetnek köszönhetően az adatmegosztás robbanásszerűen megnövekedett az elmúlt évtizedekben. De Mialatt gondtalanul élvezzük ennek előnyeit, ez nagy mértékben fenyegeti személyes adataink biztonságát. Ennek orvoslása érdekében az Európai Parlament előterjesztett és elfogadott egy tervezetet, melynek fő célja a személyes adatok birtokosainak biztosítása adataik megfelelő kezeléséről és privát szférájuk biztonságáról.

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 szabály-rendszerüket.

Az incidensek növekvő száma és egyre súlyosabb károkozó hatása arra késztette az Európai Uniót (is), hogy egy, minden tagállamra egységesen vonatkozó, modern és szigorú szabályrendszert hozzon létre, így 2018. május 25-i alkalmazással életbe lép az Általános Adatvédelmi Rendelet (General Data Protection Regulation). A GDPR elsődleges célja, hogy egységesen magas szintű jogi és technikai védelmet biztosítson a személyes adatok számára az elszámoltathatóság elvét figyelembe véve.

Kikre vonatkozik?

Uniós Rendelet lévén a GDPR-t közvetlenül alkalmazni kell valamennyi olyan vállalkozás esetén, mely az EU területén tevékenységi hellyel rendelkezik és tevékenysége során személyes adatokat kezel. Tehát Magyarországon cégmérettől függetlenül minden olyan szervezetet érint, ami az Unió területén tartózkodó személy személyes adatait dolgozza fel.

Mi a személyes adat?

Mielőtt mélyebben beleásnánk magunkat a GDPR elvárásaiba, érdemes megismerni melyek is a fő szempontok, amelyek alapján mérhető a megfelelés.

A szabályozás fő célja a személyes adatok biztosítása, annak garantálása, hogy a cégek és vállalatok mindent elkövetnek annak érdekében, hogy az alkalmazottaik, meglévő, illetve potenciális ügyfeleik személyes adatait csak az előre ismertetett célból, a szükséges mértékben kezelik.

A GDPR személyes adatnak tekint minden olyan információt, amely közvetlen vagy közvetett módon képes utalni vagy mutatni egy állampolgár kilétére. 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 GDPR igen részletesen belemegy abba, hogy mit is tekint azonosítóknak. A továbbiakban a teljesség igénye nélkül mutatjuk be, mennyire széleskörű lehet a személyes adat értelmezése:

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

Kik szerepelnek egy adatkezelésben?

Most, hogy tisztáztuk mi is a személyes adat, tovább léphetünk, hogy kiknek is lehet birtokában és milyen célból. A GDPR három fő entitást különböztet meg egymástól; mind valamilyen ponton érintettek a személyes adatok kezelésében.

ADATALANYOK

Olyan állampolgárok, akik személyes adataikat megosztották cégekkel és vállalatokkal valamilyen szolgáltatásért cserébe, ők az adatkezelések érintettjei.

ADATKEZELŐK

Az adatkezelés magába foglal szinte minden személyes adatokon végzett tevékenységet, így aki ezek valamelyikével foglalkozik és dönt az adatkezelés céljairól és eszközeiről, az adatkezelőnek minősül.

ADATFELDOLGOZÓK

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

Mik a jogok, jogalapok és a kötelezettségek

Ezt követően nézzük meg, mit is vár el pontosan a GDPR a cégektől és vállalatoktól. Ez két fő kategóriába sorolható – Az adatkezelésben érintettek jogaira; és a kezelők, feldolgozók kötelezettségeire. Mind a jogok biztosítása, mind a kötelezettségek betartatása az adatkezelőkre és -feldolgozókra hárul.

JOGOK

- **Adat helyesbítés (korrekció):** Amennyiben az adatalany hibát, hiányosságot észlel a begyűjtött személyes adatokban, a cég, vállalat adjon lehetőséget azok módosítására, javítására.
- **Hozzájárulás:** Az adatkezelők és -feldolgozók csak az alany önkéntes és egyértelmű, olykor kifejezett beleegyezését követően férhetnek hozzá annak személyes adataihoz, valamint csak az előre tisztázott módon és mértékben.
- **Adathordozhatóság:** Abban az esetben, ha az alany más szolgáltatóval szeretne a továbbiakban üzleti kapcsolatban állni, az aktuális vállalat köteles a személyes adatokat továbbítani.
- **Adatok törlése:** Az adatalany kérvényezheti személyes adatainak törlését az adatbázisból. Ez, ha jogos igénynek minősül, az adatkezelő, -feldolgozó köteles teljesíteni.
- **Tájékoztatás:** Világosan és közérthetően mondja el, hogy Ön, mint adatkezelő, mivel foglalkozik és miért végez adatokkal kapcsolatos tevékenységet.

JOGALAPOK

- **Hozzájárulás:** az érintett személy egyértelmű és önkéntes beleegyezése
- **Szerződés teljesítése:** már meglévő szerződés teljesítéséhez szükséges adatkezelés
- **Jogi kötelezettség:** adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges adatkezelés
- **Természetes személy létfontosságú érdeke**
- **Közérdekű adatkezelés**
- **Jogos érdek érvényesítése:** az adatkezelő jogos érdekét képviselő adatkezelési tevékenység

KÖTELEZETTSÉGEK

- **Elszámolhatóság és átláthatóság:** Egyértelművé kell tenni, hogy a begyűjtött személyes adatok milyen folyamatokban vesznek részt az adatkezelésben, ki férhet hozzájuk és milyen okból. Ezt az adatalany tudtára kell hozni, illetve a folyamat lépéseit megfelelően dokumentálni.
- **Mértékletesség:** A begyűjtött személyes adatokkal történő folyamatok semmilyen módon nem sérthetik az adatalanyok privát szféráját és biztonságát
- **Beépített és alapértelmezett adatvédelem:** Az adatkezelés tervezése és megvalósítása során megfelelő technikai és szervezési intézkedéseket szükséges bevezetni az adatok megfelelő védelme érdekében.
- **Érzékeny adatok védelme:** Biztosítsa, hogy azok az adatok, melyek a különleges kategóriákba tartoznak és szenzitívnek minősülnek, további védelmi intézkedésekkel vannak ellátva.

Mindez üzleti szemmel

Mindezek után tekintsük meg, mindez hogyan fest egy vállalati felépítésben.

Ön, mint adatkezelő szolgáltatásokért cserébe begyűjti és kezeli a meglévő és leendő ügyfeleinek adatait. Ugyanígy tesz a munkavállalóival is a munkaviszony fenntartása érdekében. Ezért cserébe biztosítja ezen személyek alanyi jogait és betartja a hozzá társuló adatkezelői kötelezettségeit.

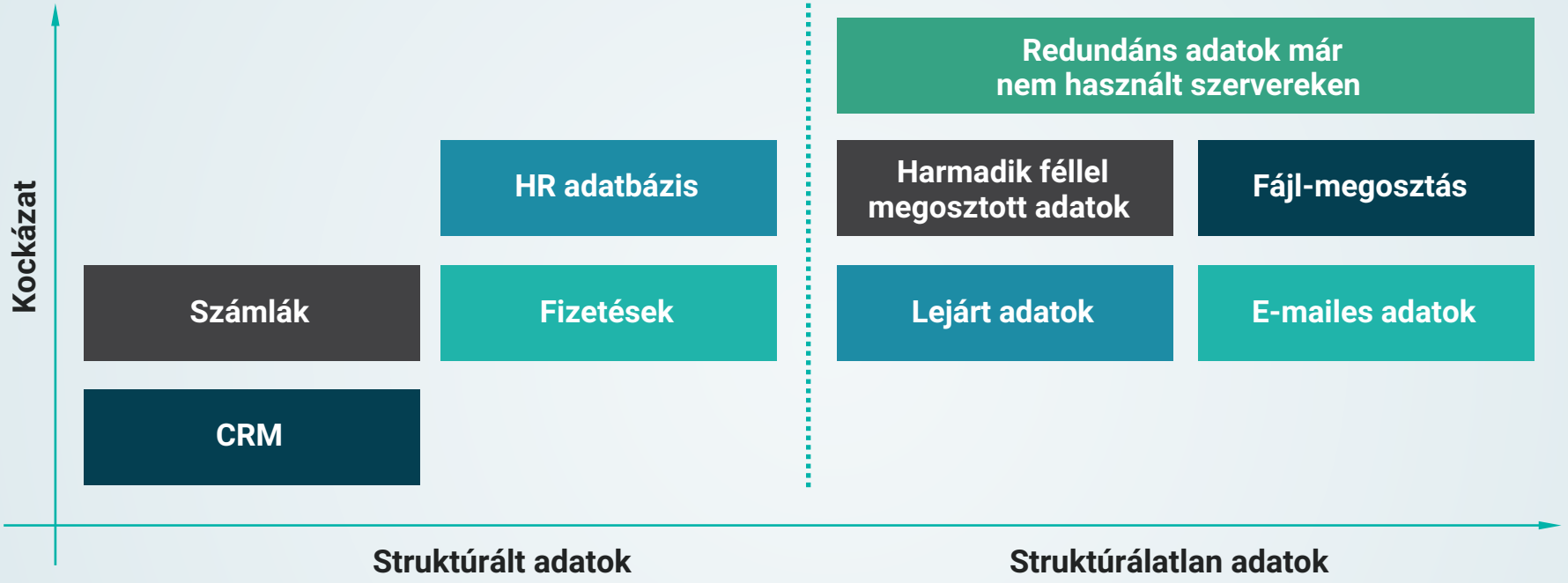
A begyűjtött és kezelt személyes adatokat átlátható és jól dokumentált folyamatokkal végzi, ügyelve a személyes adatok biztonságára, mint például adattitkosítás, vagy a jogosultságok szükséges minimumra csökkentése.

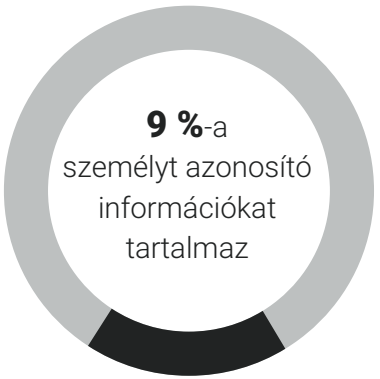
Olyan folyamatok esetén, melyeket egy különálló adatfeldolgozóra bíz (például könyvelő iroda, marketing felmérések, külső IT cégek) biztosítja, hogy egyértelműen mettől meddig terjed az egyes cégek hatásköre és jogosultsága az adatok kezelése kapcsán. Fontos, hogy ezen adatfeldolgozók képesek legyenek elszámolni és ledokumentálni az egyes tevékenységeket, melyeket a személyes adatokkal végeznek.

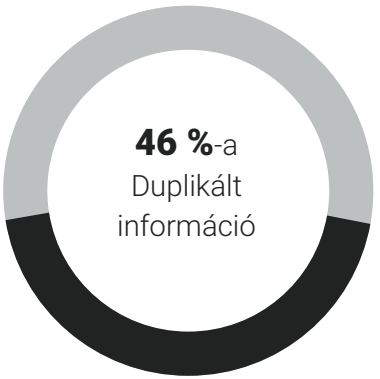
Mindezek fényében a cég biztosítja GDPR megfelelőségét.

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:







Hogyan kezdjük a felkészülést?

Felmérés és tervezés

Adatok feltérképezése: Megismerni és ledokumentálni, hogy az Ön vállalkozása milyen típusú személyes adatokat gyűjt, milyen célból és megőrzési időkkel.

Adatvédelmi hatásvizsgálat*: Bármilyen új vagy meglévő folyamat, amely személyes adatok kezelésével függ össze (pl: gyűjtés, tárolás, titkosítás, elemzés), felülvizsgálatot igényel .Az adatvédelmi hatásvizsgálat célja felmérni a folyamatok biztonsági szintjét és minimalizálni a személyes adatokra mért kockázatokat.

Megfelelés biztosítása

Hiányfelmérés és intézkedési terv: Az adatkezelések kockázatainak felmérése után, csökkentő intézkedések szükséges azokban az esetekben, amelyekben a fenyegetettség mértéke nagy. A jogosulatlan és / vagy lejárt adatkezelések felszámolása mellett

Adatvédelmi tisztviselő (DPO) kijelölése*: Hasonlóan egy munkavédelmi biztoshoz a GDPR elvárja, hogy legyen egy kinevezett adatvédelmi szakember minden vállalatban, akinek szerepköre a GDPR megfelelés kiértékelése és javaslattétel esetleges módosításokra. Ezen szerepkör betölthető egy, a cégen belüli személy vagy egy külsős által.

Folyamat dokumentálása, (tréning): Minden személyes adatot érintő tevékenységről részletes folyamatleírás kell, hogy készüljön, melyről az alkalmazottak átfogó tájékoztatást kapnak.

Kommunikáció és tájékoztatás: Adatkezeléseit megfelelő részletességgel szükséges dokumentálnia, közérthető nyelvezettel és bárki számára elérhetően.

GDPR-ral kapcsolatos fontos információk:

Felügyeleti hatóság

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

GDPR életbelépésének határideje

2018. május 25.

Szankciók

A nem megfelelés esetleges felszólításokat követően szankciókat von maga után, amely a vállalat éves nettó árbevételének 4% is jelentheti, vagy akár 20 millió eurót is.

HOL TALÁL HIVATALOS INFORMÁCIÓT A GDPR-RAL KAPCSOLATBAN?

Az Európai Unió hivatalos GDPR oldala:

https://www.eugdpr.org/

NAIH GDPR útmutató:

https://naih.hu/felkeszueles-az-adatvedelmi-rendelet-alkalmazasara.html

Ismerje meg a A **GDPRlite**-ot a kisvállalatok GDPR nyilvántartóját

Egy könnyen kezelhető, felhőalapú software, ami segítséget nyújt vállalkozása számára, hogy adatkezelésének folyamatai a GDPR által előírt paraméterek mentén legyenek dokumentálva.

- **Modern, biztonságos webes felület**
- **Jogszabályoknak megfelelő GDPR dokumentáció**
- **Irányítópult, GDPR megfelelés nyomonkövetése**
- **Egyszerűsített beállítások, cég tevékenységi körökre szabott template-k segítségével**
- **Automatikus figyelmeztetések közelgő határidő vagy fontos elvégzendő feladat esetén**

TUDJON MEG TÖBBET!