

## The GDPR: a practical overview

Fontosabb kifejezések:

Data subject - adatalany

Data controller - adatkezelő

Data processor - adatfeldolgozó

Hogyan véded a személyes adatokat?

Mikor dolgozhatsz személyes adatokkal?

Melyek az adatalany jogai?

Az Európai Unióban

A GDPR védi a személyes adatokat

Mit jelent ez a Te cégedre nézve?

Engedd, hogy megmutassuk Neked

A GDPR: egy hasznos áttekintés

1. dia

---

A személyes adatok nagyon értékes árukká váltak. A technológiai fejlődésnek köszönhetően a személyes adatok védelmének érdekében sok ország fogalmazott meg adatjogi törvényeket, abból a célból, hogy csökkentsék az egyre növekvő aggodalmat az emberekben a személyes adatok védelmével kapcsolatban. Az EU 1995-ben létrehozta a Data Protection Directive-t. Ezt azonban minden EU-s tagállam átültette a saját verziójú direktívájába, és az országok között így kialakult különbségek elkezdtek befolyást gyakorolni a kereskedelemre. Annak érdekében, hogy a különbségeket csökkenteni tudják, létrehoztak egy egységesebb törvényt. Az EU 2016-ban megfogalmazta a General Data Protection Regulation-t (a továbbiakban GDPR) a Data Protection Directive helyettesítésére. A GDPR minden tagállamban egységesen kerül alkalmazásra, aminek köszönhetően kisebb az esélye a különböző változatok kialakításának, valamint ennek eredményeképpen egy egységesebb adatvédelmi törvény alakult ki.

2. dia

---

A GDPR a személyes adatok tisztességes és felelősségteljes felhasználásának a megfogalmazása. Minden olyan szervezetre vonatkozik, amelyek:

- Az EU területén lettek alapítva
- Árukat és / vagy szolgáltatásokat kínálnak az egyéneknek az EU-n belül
- Monitorozzák a személyek viselkedését az EU-n belül

Minden szervezetet kötelez ugyanazon személyes adatok védelmére vonatkozó sztxenderdek betartására attól függetlenül, hogy az EU-n belül hol található az adott szervezet. Ez azt jelenti, hogy még azon szervezeteknek is meg kell felelniük a GDPR személyes adatok feldolgozására vonatkozó

szabályozásainak, amelyek Ausztráliában, vagy az Egyesült Államokban találhatóak meg, viszont az európai piacot célozzák meg.

### 3. dia

---

A GDPR szabályozásainak teljesítése érdekében a cégednek vannak szabályai a személyes adatok feldolgozási folyamataira vonatkozóan. A jobb megértés érdekében tudnod kell a választ az alábbi kérdésekre:

- Melyek a GDPR kulcskifejezései?
- Melyek a GDPR főbb alapelvei?
- Mit kell tudnod a személyes adatok feldolgozásáról a GDPR szabályozásai alatt?

### 4. dia

---

A GDPR a személyes adatok feldolgozásának folyamataira vonatkozik. De mik pontosan a személyes adatok? A GDPR szerint személyes adatnak minősül minden olyan információ, amely egy azonosított vagy azonosítható természetes személlyel kapcsolatos. Ez azt jelenti, hogy a GDPR egyedül természetes személyekre vonatkozik, vagyis cégekre, kormányokra, és egyéb szervezetekre nem. Így az üzleti titkok, valamint a bizalmas kormány információk annak ellenére, hogy védelemre szorulnak, nem minősülnek személyes adatnak, így nem vonatkoznak rájuk a GDPR szabályozásai.

### 5. dia

---

A személyes adat emberekre vonatkozó információt jelent. Mint például:

- Név
- Helyszín információk, például a lakcím vagy az aktuális GPS pozíció
- Telefonszám
- E-mail cím
- Mobil eszköz ID-a
- IP cím

Néhány adat, mint például a keresési előzmények, vagy a geolokáció is kapcsolódhatnak egy specifikus személyhez, amely így azt személyes adattá teszi. Így még a munkakör is (pl.: elnök) is személyes adatnak minősül. A személyes adatok direkt vagy indirekt módon is utalhatnak egy személyre. Például, ha leírsz valakit egy munkatársadnak, akkor:

- Ha azt mondod, hogy „Mateo Picard a könyvelésen”, akkor direkt módon azonosítottad őt
- Azonban, ha azt mondod, hogy „A magas, fiatalember rövid hajjal a könyvelésen”, akkor indirekt módon azonosítottad őt

Azon információk, mint például egy online profil, amely nem tartalmaz sem képet, sem nevet, viszont érdeklődési köröket igen, szintén indirekt azonosítási módnak minősülnek, így szintén személyes adatnak minősül, vagyis ezáltal szintén vonatkoznak rá a GDPR szabályozásai.

### 6. dia

---

Egyetlen egy adat önmagában még nem elég ahhoz, hogy beazonosítható legyen valaki általa. Egy adatbázisban például többen is szerepelhetnek ugyanazzal a névvel, többen is lakhatnak ugyanazon a lakcímen, illetve többen is osztozhatnak ugyanazon az IP címen, és így tovább. Annak érdekében, hogy valaki pontosan azonosítható legyen, a szervezetek több adatot kombinálnak, melyek különböző

forrásokból származnak. Ebbe beleértendők az online előzmények, a social media felületek, a vásárlási szokások, és a kérdőívek. Ezen adatokból több is nem specifikus adatnak tűnhet önmagában, azonban, ha mindezeket kombináljuk, egy személy azonossága könnyen azonosíthatóvá válhat.

## 7. dia

---

A személyes adatok néhány formája érzékenyebb adatnak minősül, és emiatt külön, speciális kategóriaként vannak kezelve a GDPR szabályozásai szerint. Ilyen speciális kategóriának minősül például:

- Rasz vagy etnikai hovatartozás
- Politikai vélemény
- Vallási vagy filozófiai hovatartozás, meggyőződés
- Szakszervezeti tagság
- Egészség
- Szexuális élet vagy szexuális orientáció
- Genetikai adatok
- Biometrikus adatok

Amikor bármilyen személyes adat feldolgozásra kerül, a szervezeteknek fel kell készülniük arra, hogy bizonyítékot tudjanak szolgáltatni, miért használják fel az adott adatot, illetve, hogyan védik azt. Ezen érzékeny személyes adatok feldolgozásának szignifikáns, negatív következményei lehetnek az egyénekre nézve, így a szervezeteknek szigorúbb feltételeknek kell megfelelniük, amikor ezeket feldolgozzák.

## 8. dia

---

Mit jelent a személyes adatok feldolgozása? A személyes adatok feldolgozása minden olyan folyamatra utal, amelyet a szervezetek tesznek meg a személyes adatokkal kapcsolatban. Be tudod azonosítani, hogy a következő szituációk közül melyik minősülhet adatfeldolgozásnak? Kattints az Igen vagy a Nem gombokra attól függően, hogy mit gondolsz a feldolgozásról.

1. Mateo kitölt egy papír alapú jelentkezést, és utána nem küldi be.	Igen	Nem
2. Mateo személyes adatai megosztásra kerültek az egyik szervezet által egy másik szervezet részére.	Igen	Nem
3. Mateo kitölt egy jelentkezést, amit utána beküld egy szervezethez.	Igen	Nem
4. Mateo adatai egy digitális fájlban „Tárolva” vagy „Inaktív” megjelölést kaptak	Igen	Nem
5. Mateo adatai törlésre kerültek egy számítógépről.	Igen	Nem

Válaszok és indoklás:

1. **Nem** – Amennyiben az adat nem került átküldésre, akkor nem került felhasználásra sem.
2. **Igen** – Egy adat megosztása azt jelenti, hogy mindkét cég feldolgozza azt.

3. Igen – Abban a pillanatban, amint egy szervezet megkapja a személyes adatot, az feldolgozásra kerül.

4. Igen – Még egy olyan adat is feldolgozásra kerültnek minősül, amelyik tárolásra került, vagy amelyik éppen nincs aktív felhasználás alatt.

5. Igen – Abban az esetben, amikor egy adat törlésre kerül, attól függetlenül még feldolgozás alatt van.

9. dia

---

Egy szervezet attól a pillanattól kezdve dolgoz fel egy személyes adatot, amikor egy adat begyűjtésre került, egészen addig, amíg ki nem törlik azt. Ebbe beletartozik a személyes adatok:

- Gyűjtése
- Felhasználása
- Adaptálása
- Megosztása
- Tárolása
- Korlátozása
- Törlése

A GDPR szabályozásai szerint amennyiben egy személyes adatot nem használunk, csak tároljuk azt, attól függetlenül az még adatfeldolgozásnak minősül.

10. dia

---

A GDPR szabályozásai szerint az alábbiak vesznek részt a folyamatokban.

- Data Subject – Adatalany: Azok a személyek, akik adatai begyűjtésre és felhasználásra kerülnek egy szervezet által
- Data Controller – Adatkezelő: Azok, akik gyűjtik az adatokat és döntenek arról, hogyan használják fel őket
- Data Processor – Adatfeldolgozó: Azok, akik az adatkezelők által lettek felvéve specifikus feladatok végrehajtásának céljából

Meg tudod határozni, hogy ki a adatalany / adatkezelő / adatfeldolgozó a következő forgatókönyv szerint?

**Fontos:** A példánál a neveket / személyeket jelölő köröket húzzátok át a szaggatott vonalas körökbe.

„Jean igényel egy bankkártyát egy ZYX bankon keresztül, amely Statement Co-t használ annak érdekében, hogy havi számlákat küldjenek a bankkártyát használó vásárlóiknak. A bank jóváhagyja a kártya kérelmet és küld egyet Jane-nek”

- Jane = adatalany
- ZYX Bank = adatkezelő
- Statement Co = adatfeldolgozó

„Amikor a WVZTek üzlet forgalma megduplázódott, a CEO felbérelt egy külső céget, hogy segítsenek előkészíteni és kiszállítani minden bejövő vásárlói megrendelést”

- Vásárlók = adatalany
- WVZTek = adatkezelő
- Külső cég = adatfeldolgozó

„Hanna a Call Center Inc-nek dolgozik, amelyik vásárlói hívásokat kezel a Trekket Chair részére. Hanna kap egy hívást Raj Patel-től és így hozzáfér a fájljaihoz.”

- Raj Patel = adatalany
- Trekket Chair = adatkezelő
- Call Center Inc = adatfeldolgozó

11. dia

---

Mind az adatkezelők, mint pedig az adatfeldolgozók személyes adatokat használnak, így pedig a GDPR szabályozásai vonatkoznak rájuk. Az adatkezelők azok, akik felelősséggel tartoznak az adatfeldolgozókért, akiket felbérelnek. Így a cégednek valószínűleg szüksége lesz további engedélyezési folyamatokra, mielőtt elkezdenének egy külsőssel együtt dolgozni. A cégednek azt is ellenőriznie kell, hogy a külsős cégnek lesz-e hozzáférése a személyes adatokhoz. Amennyiben igen, specifikus lépések megtételére lesz szükség, mielőtt a munka megkezdődik. Így legyél biztos abban, hogy tudsz és követsz minden szervezeti folyamatot, amikor egy külsős céggel együtt dolgozol, annak érdekében, hogy elkerülj minden potenciális kockázatot.

12. dia

---

Számtalan oka lehet annak, hogy a szervezetek miért dolgoznak fel személyes adatokat:

- Szolgáltatások vagy áruk nyújtása az egyének részére
- Piackutatás és elemzés
- Közbiztonság
- Üzleti kapcsolatok
- Foglalkoztatási célok

Ennek ellenére, a GDPR szabályozásai szerint egy szervezetnek képesnek kell lennie arra, hogy rámutasson egy olyan legitim indoklásra, amely alapján a személyes adatokat feldolgozhatja. Mint például:

- Szerződéses követelmények teljesítése
- A törvényeknek való megfelelés
- Vagy az adatalany beleegyezése

13. dia

---

A GDPR nagyon specifikus arra vonatkozóan, hogy mi határozza meg a beleegyezés fogalmát. A beleegyezés:

- Tisztán és világosan kell, hogy kifejezett legyen
- Szabadon adott, és nem kötelezően – A szervezetek csak akkor kérhetik az egyénet, hogy személyes adatokat vagy beleegyezést adjanak az adatok feldolgozásához, amennyiben ez szükséges a termék szállításához vagy a szolgáltatás teljesítéséhez

- Tiszta és pontos nyelven megfogalmazott kell, hogy legyen és könnyen elfogadható
- Könnyen megkülönböztethető kell, hogy legyen más beleegyezésektől
- A hallgatás nem beleegyezés

Fontos, hogy mindig legyél tisztában a céged beleegyezési folyamataival.

#### 14. dia

---

Az adatkezelőknek specifikus kötelezettségeknek kell megfelelniük a GDPR szabályozásai alapján, amikor feldolgoznak egy személyes adatot. Tudatában kell lenniük annak, hogy milyen személyes adatokat és miért, mi okból gyűjtenek. Az adatminimalizálás azt jelenti, hogy a szervezetek csak olyan adatokat gyűjtenek, amelyekre valóban szükségük van valamilyen specifikus üzleti célok okán, és kötelességük törölni vagy anonimizálni az adatokat, amint már nincs többé szükség az adott célból való felhasználásukra. A célkorlátozás értelmében kizárólag olyan célra használható a begyűjtött adat, amely okán az begyűjtésre került (és amibe az egyén beleegyezett).

#### 15. dia

---

Karl-nak meg kell változtatnia a KCF interaktív weboldalát. Jelenleg a vásárlók havonta hírlevelet kapnak, amely a következő információkat tartalmazza:

- Név
- E-mail cím
- Utca
- Város
- Ország
- Életkor
- Nem
- Mobil szám
- Fizetési információk

A KCF hírlevele a vásárlókat név szerint szólítja meg és néha országonként eltérhet attól függően, hogy néhány termék elérhető-e adott országokban az adott hónapban, vagy nem. Tudsz segíteni Karl-nak abban, hogy mely itemekre van szükség azoktól a vásárlóktól, akik szeretnének e-mailes hírlevelet kapni? (A helyes válaszok **zölddel** jelölve)

- **Név**
- **E-mail cím**
- Utca
- Város
- **Ország**
- Életkor
- Nem
- Mobil szám
- Fizetési információk

Amennyiben a céged személyes adatokat gyűjt a saját felhasználására, akkor adatkezelőnek minősül és köteles minimalizálni az adatgyűjtést és az adatok felhasználását.

## 16. dia

---

A GDPR adatalanyokat illető jogokat állapít meg. Az adatkezelőknek kötelességük tiszteletben tartani ezeket a jogokat és biztosítani, hogy az adatalanyoknak legyen lehetőségük gyakorolni őket. Az adatkezelőknek értesíteniük kell az adatfeldolgozókat az adatalanyok kéréséről.

Neked, mint munkavállalónak, fel kell ismerned ezeket a kéréseket és ismerned kell a céged adatkezelési folyamatait. A GDPR megköveteli, hogy bizonyosodj meg az adatalany személyazonosságáról, mielőtt teljesíted a kérését. Soha ne változtass vagy adj meg adatot anélkül, hogy követnéd a céged adatkezelési folyamatait, hogy ne hogy rossz személy kezébe kerüljenek a személyes adatok.

## 17. dia

---

Úgy gondolod, hogy tudod, milyen jogaik vannak az adatalanyoknak? Teszteljük a tudásod! Jelöld meg az alábbi kéréseket, **Igen**nel, ha teljesítened kell, **Nem**mel, ha nem vagy köteles teljesíteni vagy **Attól függ** válasszal, ha több adat szükséges.

- Kérdés: A hívó fél érdeklődik, hogy a céged hogyan tervezi felhasználni a személyes adatait.
- Válasz: **Igen** – Az adatalanyoknak joguk van tudni, hogy adataik miként kerülnek felhasználásra. A legtöbb szervezet adatvédelmi nyilatkozatot használ arra, hogy a GDPR szabályozásainak megfeleljenek és, hogy világos és tiszta legyen, hogy az adatkezelők hogyan használják fel a személyes adatokat.
- A hívó fél szeretne egy nyomtatványt a saját fájljairól.
- **Igen** – Az adatalanyoknak joguk van ahhoz, hogy lássák, milyen személyes adatokat tárol róluk az adatkezelő és joguk van ahhoz is, hogy másolatot kérjenek róla.
- A hívó fél informál téged, hogy a házzáma megváltozott, és kéri, hogy változtasd meg az adatot.
- **Igen** – Amennyiben valamely adat még nem teljes vagy hibás, az adatalany joga van ahhoz, hogy kérje annak javítását vagy kiegészítését. Az adatkezelőknek biztosítaniuk kell, hogy az adatok, amiket feldolgoznak, helyes.
- A hívó fél törli az accountját és kéri, hogy adatai legyenek törölve.
- **Attól függ** – Az „Elfeledtetéshez való jog”-ra vonatkozik. Az adatalanyoknak bizonyos körülmények között joguk van ahhoz, hogy adataikat kitöröltessék, beleértve azt, amikor az adatkezelő az adatalany beleegyezésére támaszkodott az adatok feldolgozását illetően és az adatalany visszavonja a beleegyezését. Azonban előfordulhatnak olyan esetek, amikor nem vagy köteles teljesíteni egy ilyen kérést, mert az adatok törlése csak az arra felhatalmazott munkavállalók által valósulhat meg. Legyél biztos benne, hogy tisztában vagy a céged adatok törlésére vonatkozó szabályaival és az arra vonatkozó megőrzési politikával, mielőtt eleget teszel egy kérelemnek.
- A hívó fél azt mondja, hogy az adat, amit róla tárolsz és egy harmadik féltől származik, nem helyes, így nem szeretné, ha azt feldolgoznád. A hívó fél és a harmadik fél egymásnak ellentmondó adatokról számolnak be.

- **Igen** – Korlátoznod kell az adatok feldolgozását addig, amíg megerősíted a vitatott adat hitelességét.
- A hívó fél arra kér, hogy töröld a levelező listáról és az adatai is legyenek törölve a megosztott marketing listáról.
- **Igen** – Az adatalanyoknak joguk van ahhoz, hogy tiltakozzanak az adataik direkt marketing célokra történő feldolgozása ellen. Tiszteletben kell tartanod az ilyen döntéseket.
- A hívó fél informál téged, hogy az accountját átviszi egy másik céghez és szeretné, ha az adatai átkerülnének hozzá.
- **Attól függ** – Bizonyos esetekben az adatalanyoknak joguk van ahhoz, hogy kaphassanak egy másolatot az adataikról, valamint, hogy azok átkerülhessenek egy másik céghez sztemderd, olvasható formátumban.

18. dia

---

A GDPR időkorlátokat határoz meg arra vonatkozóan, hogy a szervezeteknek mikor kell eleget tenniük a kötelezettségeiknek, tekintettel az adatalany jogainak tiszteletben tartására, annak érdekében, hogy a kéréseket megfelelő időben tudják teljesíteni a szervezeti irányelvekkel és eljárásokkal összhangban. Amennyiben bizonytalan vagy a szervezeti irányelvekkel kapcsolatban, vagy kérdéseid vannak, keresd fel a megfelelő személyt a szervezetben, aki információkkal tud szolgálni részedre.

19. dia

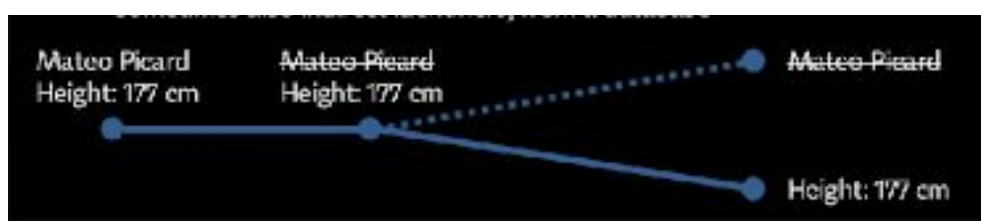
---

Az adatkezelőknek biztonságban és titokban / bizalmas adatként kell kezelniük a személyes adatokat, azok feldolgozásának teljes időtartama alatt. A szervezeteknek meg kell védeniük a személyes adatokat és korlátozniuk kell a hozzáférést, valamint kevésbé azonosíthatóvá kell tenniük őket.

Egy adatot úgy lehet titkosítottá tenni, hogy megváltoztatják azt olvasható formából egy random karakterekből álló szimbólummá, amelyet nem lehet elolvasni a dekódoló kulcs nélkül. Ez megvédi az adatot a jogtalan hozzáféréstől vagy felhasználástól.



Emellett egy adat lehet pszeudonimizált. Ez az eljárás megköveteli a direkt, valamint alkalmanként az indirekt azonosításra is szolgáló adatokat az adatbázisból. Ezáltal egy jogtalan felhasználó nem lesz képes arra, hogy a fennmaradt adatot hozzákösse a megfelelő személyhez. Az eltávolított adatot így külön kell, hogy kezeljék a pszeudonimizált adattól.





## 20. dia

---

Adatszégés: a GDPR szabályozásai szerint adatszégésnek minősül minden olyan esemény, amely során egy személyes adat véletlenül vagy jogszerűtlenül került törlésre, megváltoztatásra vagy elveszett; vagy amennyiben egy jogtalan közzététel vagy hozzáférés történt. Bizonyos esetekben az adatkezelőknek biztosítaniuk kell, hogy 72 órán belül értesítik a megfelelő felügyeleti hatóságokat. Ráadásul az értesítést annak az adatalanyoknak is meg kell kapnia, aki érintett az ügyben. Amennyiben úgy gondolod, hogy adatbiztonsági probléma történt, például:

- Egy dekódoló kulcs egy jogtalan személyhez jutott
- Elvesztett egy számítógépes fájl
- Idegen személy jutott be az épületbe
- Adatok nem a megfelelő személy részére lettek eljuttatva

Ilyen esetekben azonnal jelentsd a problémát az adatvédelmi tisztviselőnek.

## 21. dia

---

A GDPR megköveteli az adatok védelmét a szervezetektől a személyes adatok feldolgozásának teljes időtartama alatt. Erre általában 'Beépített adatvédelemként' szoktak utalni. A beépített adatvédelem egy termék, egy szolgáltatás vagy egy üzlet megtervezésének pillanatától, a fejlesztésén át, egészen az üzembehelyezésig tart.



A szervezeteknek demonstrálniuk és bizonyítaniuk kell, hogy megfelelnek ennek. Ezen kötelezettség teljesítéséhez dokumentálni kell az adatvédelmi megfontolásokat, kockázatokat és enyhítő megoldásokat a projekt fejlesztési folyamatának részeként.

## 22. dia

---

A szervezeteknek nem csak arra kell bizonyítékot nyújtaniuk, hogy megfelelnek a beépített adatvédelemnek, hanem arra is, hogy a GDPR többi feltételének is megfelelnek. Ehhez kapcsolódóan dokumentálnod kell, hogy:

- Milyen dokumentumaid vannak
- Hogyan kerülnek a dokumentumok felhasználásra
- Kivel kerültek megosztásra
- Hol kerülnek tárolásra és milyen hosszú időre

- Mikor és hogyan kerülnek törlésre

A pontos nyilvántartások vezetése segít a szervezetek számára a kérdések gyors megválaszolásában.

23. dia

---

A személyekhez kapcsolódó információk értékesek a szervezetek számára és emiatt olyan gondosan kell kezelni őket, amennyire csak lehet. Olyan módon kell kezelned mások adatait, ahogyan elvárnád, hogy a szervezeted a te adataidat kezelje. A GDPR megadja a szervezetek számára a minimum követelményeket, hogy teljesíthessék az elvárásokat. Az adatalanyok jogainak és a szervezeti kötelezettségek megértésével, valamint a céged irányelveinek és eljárásainak betartásával hozzásegítheted a szervezetet a GDPR követelményeinek betartásához, a büntetések elkerüléséhez, valamint a fogyasztók bizalmának növelését is elősegítheted.