www.gazdagmami.hu

Adatvédelmi és GDPR tudnivalók
(a Vállalkozónői Kerekasztal 2018. május 11-i előadásának vázlata)

Mi számít személyes adatnak?

Minden, amiből közvetlenül vagy közvetetten beazonosítható az adott személy, például:

- név, email, telefon, lakcím, születési adatok – ezeket a legtöbben tudják,
- szakképzettség,
- nem,
- vallás,
- politikai nézetek,
- vagyoni helyzet,
- a böngészéshez használt eszköz adatai,
- vásárlási szokások

és még sorolhatnánk a példákat (a Wikipédiában részletesen megtalálhatod őket: https://hu.wikipedia.org/wiki/Személyes_adat)

Ha valamiről nem tudod biztosan, hogy személyes adat-e inkább kezeld úgy, mintha az lenne.

Különleges személyes adatok kezelése: pl. egészségügyi adatok, politikai hovatartozás
Ezeket nem szabad kezelni csak akkor, ha a munkához ez feltétlenül szükséges és csak annyit, amennyi feltétlenül kell a munkához.

Kire vonatkozik a GDPR?

Mindenkire, aki adatot kezel.
Nem csak cégek, szervezetek, egyéni vállalkozók, hanem magánszemélyek is!
Ha egy cég munkavállalója kezel adatot, ő a felelős érte (addig, amíg ő kezeli és rá van bízva)
Ha magánszemélyként blogolsz hobbiból és van egy blogértesítőd vagy egy Facebook oldalad, vagy egy statisztikád, vonatkozik rád a GDPR hatálya.

Magánszemélyek egymás közötti kapcsolattartására nem vonatkozik (a barátaid számát eltárolhatod a telefonodban – az nem számít adatkezelésnek)

A törvényszöveg nagyon általános, a gyakorlatban sokat segíthet a WP29-es iránymutatás, ez egy munkacsoport, akik a gyakorlatra ültetik át a törvényszöveget. (itt tudod megnézni, milyen iránymutatásokat adtak ki eddig: https://www.naih.hu/29-es-munkacsoport-iranymutatasai.html)

Milyen formában tárolt adat számít adatkezelésnek?

Minden forma ide számít. Ha egy noteszben tárolsz adatokat vagy felírod egy cetlire, az is adatkezelésnek minősül. A névjegykártya, szórólap is ide tartozik vagy a telefonodban elmentett számok (akkor is, ha a magántelefonodban üzleti partnerek adatait is tárolod).
De az e-mailben érkező adatokat is érinti (érdemes bizonyos időközönként a céges emaileket karbantartani, törölni a felesleges adatokat)

Hírlevélfeliratkozásnál, hírlevélküldésnél mire kell figyelni?

Mindenképpen tájékoztatni kell a feliratkozót, hogy marketing tartalmú hírlevelet fogsz neki

küldeni és el kell fogadnia az adatvédelmi szabályzatot (egy checkbox a feliratkozó űrlap alatt). A checkboxot nem szabad előre bepipálni!

Legyen leiratkozó link a hírlevélben, amivel le lehet iratkozni és ilyenkor valóban törölni is kell az adatokat (ne csak inaktív státuszba kerüljön)

Ha nem tájékoztattuk, hogy reklám tartalmú hírlevelet is kaphat, nem küldhetünk neki reklám tartalmú levelet, de a vásárlással kapcsolatos tájékoztatást igen (pl. használati utasítás, szállítási infók, a vásárlást követően véleménykérés)

Webáruházban a megrendelést követően csak az kaphat hírlevelet, aki ezt megrendeléskor bejelölte. A checkboxot nem szabad előre kipipálni.

A hozzájárulás 3 feltétele:

- önkéntes legyen
- megelőzte egy konkrét és megfelelő tájékoztatás
- félreérthetetlen cselekménnyel jelezte, hogy kéri a hírleveleket (rákattintott a gombra)

Csak annak szabad hírlevelet küldeni, aki előre feliratkozott.
Kivéve a céges email címek, amiknél egyértelmű, hogy cégről van szó, pl. info@cegnev.hu és nincs benne semmi, ami személynévre utal (pl. jolika@cegnev.hu, monogram sem lehet!)

Mi legyen a korábban gyűjtött adatbázisokkal?

Ha szabályosan gyűjtötted őket (feliratkoztak, volt adatvédelmi tájékoztató az oldalon és közölted velük, hogy reklám tartalmú emailt kapnak majd), akkor használhatod, a nem szabályosan szerzett listákat törölni kell.

Mit kell tenni, ha emailben vagy telefonon veszünk fel megrendeléseket és rögzítünk adatokat?

Ez is adatkezelésnek minősül, a másik beleegyezését kell kérni ahhoz, hogy rögzíthesd a telefonon felvett adatait.

Kinek kell adatvédelmi szabályzat a honlapjára?

Mindenkinek, aki bármilyen formában adatokat kezel (hozzászólások, honlap statisztika stb.)

Megrendelések felvételénél mire figyeljünk oda?

Ne kérjünk be felesleges adatokat, amire nincs szükség, csak annyit, amennyi a megrendelés teljesítéséhez szükséges.

Mi a helyzet a sütikkel? Mire figyeljünk?

A honlapon el kell fogadtatni a sütihasználatot és kell biztosítani a sütikről való leiratkozási lehetőséget is, ehhez az is elég, ha csak belinkelünk egy leírást arról, hogy az egyes böngészőkben hogyan lehet letiltani a sütiket.
A sütibe mostantól beletartozik a Facebook lájk gomb is, éppen ezért be kell kerülnie az

adatvédelmi szabályzatba annak is, hogy ezeket használjuk az oldalon.
Mivel sütihasználatkor továbbítjuk az adatokat a Google vagy a Facebook részére, ezért onnantól kezdve ők a felelősek az adatok felhasználásáért, éppen ezért az adatvédelmi tájékoztatóba célszerű belinkelni az ő adatvédelmi szabályzatukat is a felhasználók tájékoztatására.

Mit kell tudni a remarketing pixelek használatáról?

Nyugodtan lehet továbbra is használni csak be kell írni az adatvédelmi szabályzatba, hogy ilyeneket használunk és el kell fogadtatni a cookie kezelést az oldalon. A korábbi híresztelésekkel ellentétben a remarketing pixel használata nem számít tömeges megfigyelésnek, ezért emiatt nem kell adatvédelmi biztost alkalmaznia a cégnek.

Ha kérésre törölni kell a felhasználók adatait, hogyan tegyünk eleget annak a számviteli kötelezettségnek ami szerint meg kell őrizni a számlákat és a megrendeléseket?

Természetesen azokat az adatokat, amiknek a megőrzésére valamilyen törvény kötelez, továbbra is meg kell őrizni, viszont be kell írni az adatvédelmi tájékoztatóba, hogy ezeket az adatokat azért őrizzük, mert erre törvény kötelez.

Hogyan tájékoztassuk a felhasználókat az adatkezelésről?

Fontos a konkrét és megfelelő tájékoztatás az adatkezelésről:

- ki az adatkezelő (a te neved vagy a céged, szervezeted neve)
- mi az adatkezelés célja (miért kérem el azt a személyes adatot?)
- érthető jogi tájékoztatás,
- olyan helyen kell kihelyezni az adatvédelmi tájékoztatót, ahol könnyen elolvasható, megtalálható,
- ne legyen apróbetűs,
- bármikor tudja visszavonni a hozzájárulást a felhasználó (leiratkozik a hírlevélről, nem kéri a cookiekat, kéri, hogy töröld az adatait)

Az adatkezelés indoka mindig valamilyen félreérthetetlen cselekmény legyen:
- legyen ott gomb vagy jelölőnégyzet, amivel hozzájárult,
- szóbeli vagy írásbeli hozzájárulást adjon (pl. ha telefonon rendeli meg a termékedet, megkérheted, hogy küldjön egy emailt, amiben visszajelzi, hogy tényleg ő adta meg az adatait és hozzájárult, hogy kezeld azokat)

Típushibák:

- hallgatás nem egyenlő hozzájárulás („ha használod az oldalt azzal elfogadod, hogy...”,
- előre kipipált jelölőnégyzet
- automatikus pipa
- általános hozzájárulás (egyetlen gomb lenyomásával mindent elfogad)
- ha nincs előzetes tájékoztatás

Ha megvalósul a cél, már nem kell tárolni az adatot: pl. egy címre kiszállítottunk pizzát, már nem tárolhatjuk tovább a megrendelő adatait.

Mindig egyértelmű legyen, hogyan kezeljük az adatokat.

Online rendeléseknél:
- ÁSZF
- adatvédelmi tájékoztató
- adattakarékosság elve (feleslegesen ne táruljunk adatokat)
- célhoz kötöttség (ne tároljunk olyan adatot, aminek nincs célja pl. nem kell a megrendelés teljesítéséhez)
- a megrendelés nem egyenlő hírlevélre feliratkozás.

Kétféle szabályzatot kell megcsinálni:

Adatvédelmi tájékoztatás Ügyfél felé:
kedves X így és így kezelem az adataidat

Adatvédelmi szabályzat:
A cégben befelé magunk között:
- milyen adatokat kezelünk,
- hol kezeljük (notesz, telefon, email, hírlevélrendszer, CRM stb.)
- kinek adunk át adatokat, (pl. könyvelő, rendezvénynél a hostessek),
- mire használjuk az adatokat, mi a céljuk,
- hogyan védjük meg őket,
- mikor töröljük az adatokat.

Adatok védelme a cégben:
- legyen jelszó a laptopon, mobilon (ha van ujjlenyomatfelismerés, használjuk),
- ne legyen látható helyen tárolva a papír alapú adat (pl. a mappára ráírva az ügyfél neve, faliújságra kitűzve a partnerek elérhetőségei)
- a munkaügyi iratokat biztonságos helyen őrizzük,
- levelezőrendszereknél és más adatkezelő felületeknél, ha van rá mód, használjunk kettős azonosítást,
- a munkavállalókat, alvállalkozókat készítsük fel az adatkezelésre, ő a felelős azért az adatért, amit kezel addig, amíg rá van bízva (pl. kiszervezett ügyfélszolgálatos az ügyféladatokért)

A felkészülés menete:

1. Személyes adatok feltérképezése: hol kezeljük az adatokat, miért kezeljük, mi a célja? mettől meddig, kinek adjuk át? (ki fér hozzá a személyes adatokhoz a cégben) hogyan védjük? a jogalapok közül melyik szerint kezeljük az adott adatot

2. Döntés arról, hogy kell-e adatvédelmi tisztségviselőt alkalmazni?\
csak akkor kell, ha a főtevékenység során nagy számban megfigyelünk embereket\
(pl. térfigyelő kamera)

3. Munkavállalók (alvállalkozók, kisegítő családtagok stb.) felkészítése\

4. Adatvédelmi tájékoztatók elkészítése\

5. Honlap ellenőrzése\

6. Előzetes hozzájárulások felülvizsgálata\l

7. Adatfeldolgozói szerződések elkészítése, felülvizsgálata\l
minden céggel, akihez adatokat továbbítasz, le kell szerződni az adatkezelésről (pl. CRM szolgáltató, hírlevélszolgáltató, Facebook, Google, futárcég, könyvelő stb.)

8. Biztonsági intézkedések\l

9. Marketing eszközök ellenőrzése\l

10. Belső szabályozások elkészítése, felülvizsgálata (nem kötelező csak akkor, ha nagy szervezet van)\l

11. Nyilvántartások (adatvédelmi incidens nyilvántartást kell vezetni pl. ha elvész a notesz stb.)\l
adatvédelmi incidens bejelentési rendje: NAIH felé kell bejelenteni 72 órán belül, ha adatfeldolgozó vagy, az adatkezelőnek kell bejelenteni)

Hogyan lesznek ezek az ellenőrzések? Igaz a pletyka, hogy már a nyáron mindenkit ellenőrizni fognak és indulnak a bírságolások?

Ezt senki nem mondhatja biztosra, csak rémhírkeltés. Valószínűleg először csak figyelmeztetés lesz, nem bírságolnak rögtön. A nyár folyamán kiderül majd. A lényeg, hogy az alapszabályokat tartsd be és akkor nincs mitől félned.