

BELSŐ ADATVÉDELMI SZABÁLYZAT

Gajdor Endre Attila egyéni vállalkozó belső működési és adatbiztonsági eljárásrendje

Jelen Belső Adatvédelmi Szabályzat (a továbbiakban: „Szabályzat”) célja, hogy rögzítse **Gajdor Endre Attila egyéni vállalkozó** (a továbbiakban: „Adatkezelő”) belső adatkezelési folyamatait, az alkalmazott informatikai és fizikai adatbiztonsági követelményeket, valamint az adatvédelmi incidensek kezelésének belső rendjét. A Szabályzat garantálja, hogy az Adatkezelő belső működése maradéktalanul megfelel az Európai Unió Általános Adatvédelmi Rendeletének (GDPR) és a hatályos magyar jogszabályoknak.

1. Az Adatkezelő hivatalos adatai

- **Név:** Gajdor Endre Attila egyéni vállalkozó
- **Székhely:** 2300 Ráckeve, Bajcsy Zsilinszky utca 98.
- **Nyilvántartási szám:** 62023591
- **Adószám:** 91863081-1-33
- **Közüsségi adószám:** HU91863081
- **Főtevékenység:** 741201 - Grafikai tervezés, vizuális kommunikáció

2. Belső adatkezelési folyamatok és eljárások

Az Adatkezelő egyedüli tagként, sole proprietor formában látja el tevékenységét, így közvetlenül felelős az adatok kezeléséért az alábbi belső folyamatok szerint:

2.1. Ügyféladatok rögzítése és egyeztetés

A megrendelőkkel történő kapcsolatfelvétel, e-mailes egyeztetések során keletkező adatokat az Adatkezelő kizárólag a szerződés előkészítése és a grafikai koncepciók kidolgozása céljából tárolja. Ha a megkeresést követő 1 éven belül nem jön létre szerződés, az adatokat tartalmazó elektronikus üzeneteket véglegesen törölni kell.

2.2. Szerződéses adatok kezelése

Az elfogadott árajánlatok és létrejött egyedi szerződések adatait az Adatkezelő a polgári jogi elévülési időn belül (5 év) biztonságos digitális környezetben tárolja a jogviták megelőzése és a teljesítés igazolhatósága érdekében.

2.3. Számlázási és pénzügyi folyamatok

Mivel az Adatkezelő alanyi adómentes (AAM) státuszú, a kiállított számlák nem tartalmazznak ÁFA-t, de a számviteli törvények alapján a kibocsátott bizonylatok a könyvviteli elszámolást támasztják alá. A bizonylatokat a kiállítás évét követő legalább 8 évig kötelező megőrizni.

3. Informatikai és fizikai adatbiztonsági intézkedések

Az Adatkezelő köteles a tőle elvárható legmagasabb szintű technikai és szervezési intézkedéseket fenntartani a személyes adatok védelmében:

3.1. Digitális biztonság

- **Eszközök védelme:** A tervezéshez, ügyfélkapcsolathoz és adminisztrációhoz használt számítógépeket, mobil eszközöket erős jelszóval, biometrikus azonosítással és automatikus képernyőzárral kell védeni.
- **Fiókok védelme:** Minden olyan online szolgáltatásban (levelezés, számlázó program, felhőalapú tárhely), ahol személyes adatokat kezelnek, kötelező a kétlépcsős azonosítás (2FA) bekapcsolása.
- **Hálózati biztonság:** Nyilvános, nem védett Wi-Fi hálózatokról az ügyféladatokat vagy levelezést tartalmazó rendszerekbe történő belépés tilos.

3.2. Fizikai biztonság

- A papíralapú szerződések, bizonylatok, jegyzetek kizárólag az Adatkezelő székhelyén, elzárt módon tárolhatóak, ahová harmadik, illetéktelen személy nem érhet el.
- A feleslegessé vált, személyes adatokat tartalmazó papírokat megsemmisítéssel (iratmegsemmisítő) kell kezelni, tilos azokat sértetlenül a kommunális hulladékba helyezni.

4. Adatfeldolgozók felügyelete

Az Adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe (könyvelő, számlázóprogram-szolgáltató, tárhelyszolgáltató), amelyek írásos nyilatkozattal vagy szerződési feltételeikben garantálják a GDPR-nak való megfelelést. Az Adatkezelő időszakosan ellenőrzi, hogy az adatfeldolgozók megfelelnek-e a biztonsági előírásoknak.

5. Adatvédelmi incidensek kezelésének belső rendje

Adatvédelmi incidensnek minősül a biztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi (pl. laptop vagy telefon ellopása, feltörése, vírusfertőzés).

5.1. Teendők incidens esetén:

1. Az incidens észlelésekor az Adatkezelő haladéktalanul megkezdi a kármentést (pl. jelszavak azonnali megváltoztatása, érintett fiókok felfüggesztése).
2. Az incidensről belső nyilvántartást kell vezetni, amely tartalmazza az incidens jellegét, az érintettek körét, az adatok számát, az incidens hatásait és a megtett elhárító intézkedéseket.
3. Ha az incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő köteles azt indokolatlan késedelem nélkül, de legkésőbb 72 órával azután, hogy az incidens a tudomására jutott, bejelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH).

6. Az érintetti kérelmek kezelése

Ha egy ügyfél vagy érintett személy élni kíván a GDPR-ban biztosított jogaival (hozzáférés, törlés, helyesbítés), a kérelmét az Adatkezelő köteles haladéktalanul, de legfeljebb a beérkezéstől számított 1 hónapon belül érdemben megvizsgálni és megválaszolni, a szükséges intézkedéseket díjmentesen végrehajtani.

Záró rendelkezés: Jelen szabályzatot az Adatkezelő magára nézve kötelezőnek ismeri el, és működése során folyamatosan biztosítja az abban leírtak érvényesülését.

Hatálybalépés / Felülvizsgálat kelte: Ráckeve, 2026. május 23.

Kiadta és jóváhagyta: Gajdor Endre Attila E.V.