Fél évvel a GDPR bevezetés után

Kedves Partnereink!

A helyzetről Péterfalvi Attilával, a Nemzeti Adatvédelmi és Információszabadság Hatóság vezetőjével (NAIH) készült cikk ad kellő bizonyosságot nyújtó információkat.

https://www.napi.hu/magyar_vallalatok/gdpr-hamarosan-erkezhet-az-elso-magyarorszagi-birsag.673708.html

A természetes személyek adatainak kezelésével kapcsolatosan az új uniós adatvédelmi szabályozást (GDPR - General Data Protection Regulation) **már két éve elfogadták**, de csak 2018. május 25-e óta kell kötelezően alkalmazni. Mivel az új „Infó törvény" (Az információs önrendelkezési jogról és az információszabadságról szóló2011. évi CXII. törvény) kapcsolódó módosítása 2018. július 26-án lépett hatályba, addig csak a korábbi eljárási szabályokkal rendelkezett a szabályok betartatásáért felelős hatóság, a NAIH.

A személyes adatok szabályszerű kezelésével foglalkozni kell, mert az érintettek szinte teljes tevékenységében előfordulhatnak személyes adatok (munkavállalói adatok, munkakapcsolatok, névjegyek, telefonszámok, mail címek, beléptetés, kamera, céges rendezvények, marketing adatok, stb.) Nem elég csak a jelen viszonyait áttekinteni és szabályozni, mert a **korábbi sok éves működés** során keletkezett adatok **is** az adatkezelés, adatfeldolgozás tárgyát képezik.

A rendelet előírásainak megszegése esetén a **kiszabható bírság** költségvetési szerveknél 20 millió forint, azon kívüli szervezeteknél **akár 20 millió euró**, vagy a cégcsoport teljes, globális forgalmának 4 százalékát is elérheti. A kettő közül a magasabb összeg a felső határ.

„A GDPR-hez kapcsolódó általános jogszabályt már elfogadták, máig hiányoznak azok a jogszabályi rendelkezések, amelyek a szektorális adatkezeléseket szabályozzák. Akár több ezer jogszabályi rendelkezést kell módosítani a jövőben, ez vélhetően 2019 első felében fog megtörténni"

„Az első két hónapban 840 ügy érkezett a NAIH-hoz, melynek a fele konzultációs típusú megkeresés volt, a másik fele pedig vizsgálati ügy. Előbbihez olyan esetek tartoznak, amikor különböző megkeresésekre kiegészítő vagy értelmező állásfoglalást adnak, vagy ilyen anyagot tesznek közzé a honlapjukon, míg utóbbihoz azok, amikor a hatóság bár elindítja az eljárást, de az nem határozattal zárul, hanem egy állásfoglalással, amely bár kötelező érvényű, de nem kényszeríthető ki."

„Október 29-ig újabb 802 ügy érkezett be az adatvédelmi hatósághoz, ezeknek mindössze 17 százaléka volt konzultációs ügy … további 80 százaléka vizsgálati típusú volt. 25-26 eljárásnak a végén bírságolni is lehet."

Ma még *„a GDPR alapján **egyetlen ügy sem jutott el odáig, hogy tényleges bírságot szabtak volna ki**"… „Ugyanakkor arra*

nem kell számítani Péterfalvi szerint, hogy egyből a maximum bírságot szabnák ki, azonban az a cél, hogy az uniós hatóságok a bírság összegét is harmonizálják."

(Ha csak valamilyen arány alapján állapítják majd meg a bírságokat, az is lehet tetemes összeg!)

Adatvédelmi incidenseknél a vállalatoknak 72 órájuk van, hogy bejelentsék az ügyet, ezt többségük meg is teszi, mivel úgy gondolják, hogy "előbb-utóbb úgyis kiderül".

*„Az incidensbejelentésekből harmada **téves címre küldött küldemény** miatt érkezett be, 10 százaléknál **jogellenesen tettek közzé** valamit, hasonló arányban volt, hogy valaki jogellenesen ismert meg adatokat, de 3 százalékban különböző adathordozók elveszítése miatt is a hivatalhoz fordultak. … **az adatvédelmi incidensek legtöbbször emberi mulasztásra vezethetőek vissza**".*

*„A NAIH továbbra is elsődlegesen panaszbeadványok alapján folytat eljárásokat, azaz a beérkező jelzések alapján dönt: elindítja a hatósági eljárást vagy sem. **Nincs kiemelt ellenőrzési terv**, hogy például a kkv-kat vagy egy bizonyos szektort ellenőrizzünk"*

Számos esetben *„az adatait féltő panaszos fordul a NAIH-hoz … a munkahelyi és kamerás adatkezelés, illetve az adatvédelmi tájékoztatók elmaradása a leggyakoribb".*

A fentiekből is látszik, hogy komolyan kell venni a GDPR kérdéseket és – a jogszabály életbe lépését követő – kezdeti lendületből és aktivitásból nem lehet lejjebb adni.

Az ismertetett interjú sem utalt semmi olyan könnyítésre, amely vállalkozói körökben gyakran terjed, azaz, hogy a magyar kisvállalkozásokra nem vonatkoznának a GDPR szabályok. Tehát, a KKV szektor nem évez semmilyen előnyt az EU rendeletben foglaltak betartását illetően. A nemzetközi példákból, esetekből könnyen lehet következtetni a későbbi hazai szankciók nagyságára is.

Minden vállalkozásnak elemi érdeke a saját folyamatainak áttekintése, a nála előforduló személyes adatok számbavétele, rendszerezése, nyilvántartásba vétele, majd ezt követően a tudatos kezelése, illetve feldolgozása, feldolgoztatása.

Mivel a GDPR alatt lévő személyes adatok köre és jellege túlnő a vállalkozás számviteli keretein, éppen ezért a GDPR-ral kapsolatos feladatok sem tartozhatnak a könyvviteli szolgáltatást végző személyek kompetenciájába. A vonatkozó szabályok betartásáért, betartatásáért a vállalkozás vezetése a felelős.

Ott, ahol az előforduló személyes adatok köre, jellege megkívánja, **önálló adatvédelmi tisztviselőt** (DPO) célszerű megbízni a saját belső szabályozás elkészítésére, illetve a felmerülő ügyek szakszerű intézésére.

A számviteli szakemberek a management számára abban tudnak segítséget nyújtani, hogy kapcsolati rendszerükben működő GDPR specialistát ajánlanak, illetve a számvitel területén jelentkező személyes adatok számbavételében, majd kezelésében támogatják az adatvédelmi tisztviselő munkáját.

Budapest, 2018. november 26.

Tisztelettel:

dr. Sallai Csilla

Kamarai tag könyvvizsgáló