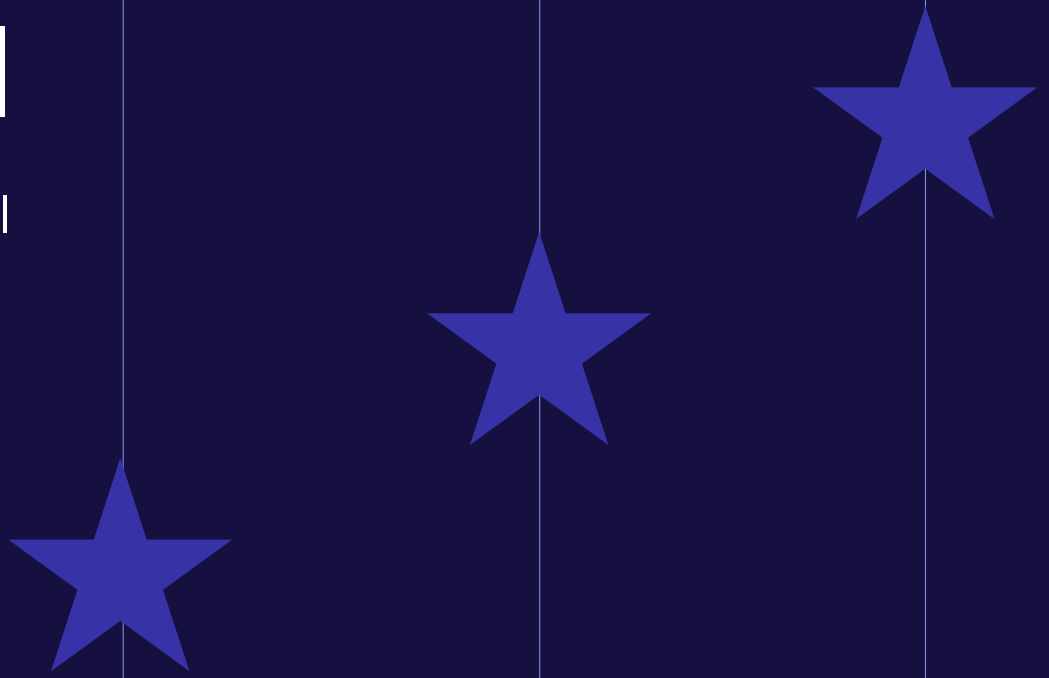
2022 a GDPR szemszögéből

Magyar és nemzetközi adatokkal



crosssec solutions

IMPRESSZUM

KIADJA

Crosssec Solutions Kft,
1052 Bp., Deák Ferenc tér 3.
–
Telefon: +36 20 666 7894
crosssec.com
info@crosssec.com

ÍRTA

Győri Aletta

KÖZREMŰKÖDÖTT

Gátos Eszter
Káldi Ivett
Kovács Marcell
Mátyus Lilla
Mezei Gréta

A kiadvány jelen változata készült:
2023. április

GDPR bírságok 2022-ben

BEVEZETÉS

Kiadványunkban a 2022-ben, a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) által kiszabott adatvédelmi bírságokat járjuk körbe, hogy az esetekből tanulva elkerülhesse a hiányosságokat és megelőzze a bírságolást.

Az Általános Adatvédelmi Rendelet (General Data Protection Regulation, röviden: GDPR) 2018. május 25-től alkalmazandó az Európai Gazdasági Térség területén, célja a személyes adatok védelmének jogi szabályozása. Ez a kötelezettség minden vállalatra, szervezetre, bizonyos esetekben magánszemélyekre is vonatkozik, amennyiben azok az Európai Unión belül élők személyes adatait üzleti célból tárolják és dolgozzák fel.

Az uniós országokban adatvédelmi hatóságok felelősek az adatvédelmi szabályok alkalmazásának biztosításáért, együttműködve az Európai Adatvédelmi Testülettel és az Európai Bizottsággal. Magyarországon ezt a feladatot a NAIH látja el.

A NAIH érintettek, adatkezelők vagy más személyek kezdeményezésére vizsgálatot indíthat, és ha szükséges eljárást folytathat le, melynek vége a jogsértés mértékétől függően pénzbírság is lehet. A maximális kiszabható bírság – attól függően melyik nagyobb - az éves árbevétel 4%-a vagy akár 20.000.000 euró lehet.

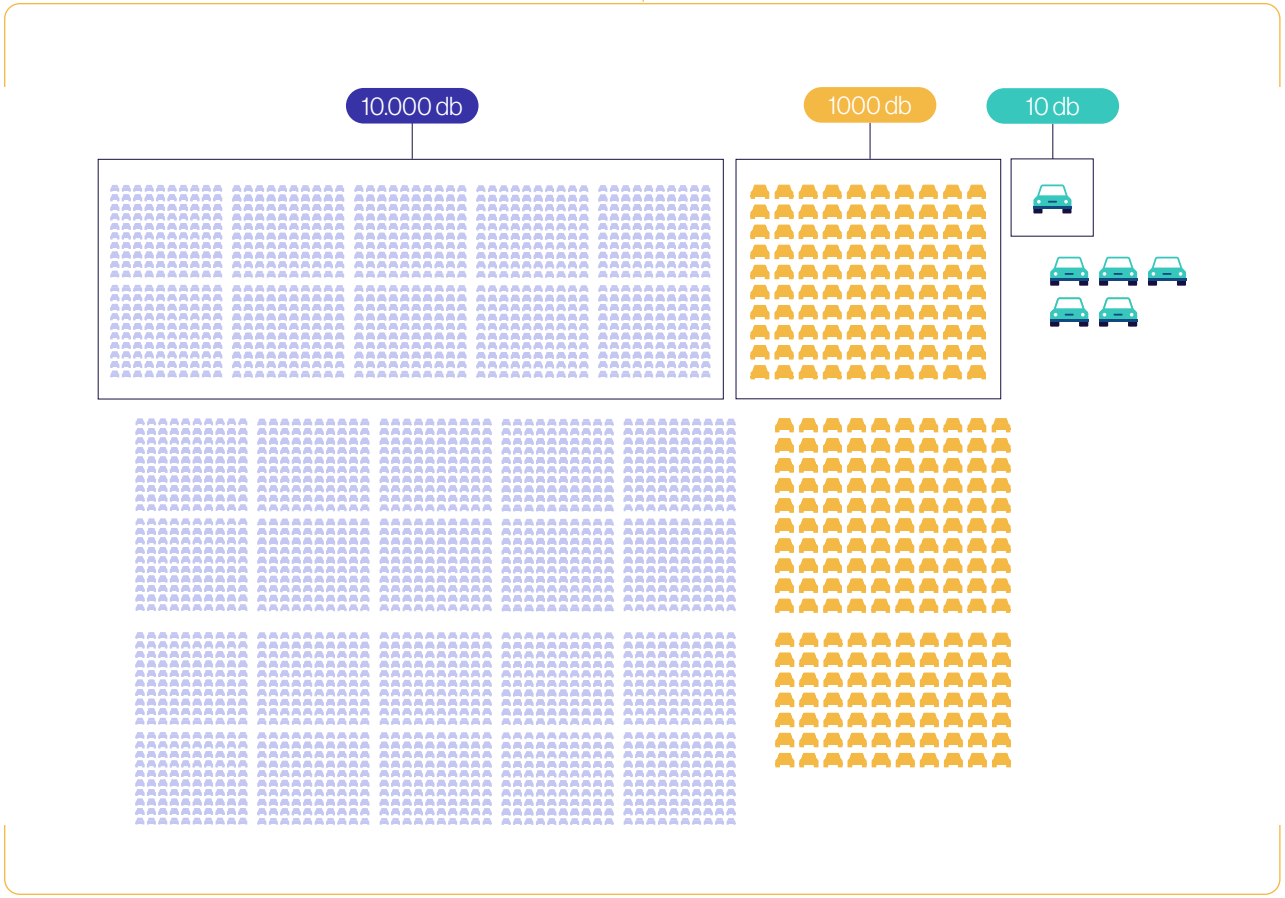
Egy korábbi kiadványunkban már bemutattuk az adatvédelmi bírságokat a rendelet megjelenésének kezdetétől 2020-ig, melyben a személyes adatok védelméhez szóló jog történelmét is körbejártuk. Jelen kiadvány tekinthető ennek folytatásaként is.

Ha szeretne naprakész híreket kapni a legfrissebb bírságokról, ajánljuk figyelmébe weboldalunkat (**gdprbirsagok.hu**), ahol minden nyilvánosságra hozott, bírsággal zárult esetről rövid összefoglalót talál.

32.760 db

TOYOTA COROLLA

lett volna megvásárolható a
832 millió eurós GDPR bírságból.



NEMZETKÖZI KITEKINTÉS

Az évben összesen 832 millió euró GDPR bírságot szabtak ki az adatvédelmi hatóságok. Ebből az összegből az év legkeresettebb új autójából (Toyota Corolla), a márka árlistájában szereplő 10.055.000 Ft-os áron 32.760 darab lett volna megvásárolható. Összehasonlításként Magyarországon 2022-ben a statisztikák szerint 3.416 darabot adtak el ebből a típusból. Az összes adatvédelmi bírság 80%-át a Meta (korábbi nevén Facebook) érdemelte ki, velük szemben több vizsgálatot is kezdeményeztek a hatóságok.*

Ennek tudatában nem meglepő, ha az év legmagasabb bírságát is a Meta Platforms kapta, 405 millió euró (a kiadvány szerkesztésekor 396 Ft-os árfolyam mellett 160,5 milliárd Ft) értékben. Az eset súlyossága fiatalkorúak érintettsége miatt volt kiemelkedő, az influenszer karriert tervező 13-17 év közötti fiatalok az Instagram profiljuk üzleti célúra váltásával automatikusan nyilvánossá tették email címüket és telefonszámukat is.

** forrás: autoszektor.hu*

HAZAI ESETEK

A NAIH sem restelkedett, 2022-ben 29 bírsággal végződő határozatot tettek közzé. Ezek száma nem fedi az összes vizsgálatot és nem tartalmazza az összes bírsággal zárult esetet sem, csupán az érdekesebb, tanulságos eseteket hozzák nyilvánosságra, informáló és intő szándékkal. A Hatóság éves beszámolójából tudhatjuk, hogy 991 alkalommal indítottak eljárást adatvédelmi ügyben, mely 79%-a érintetti kérelemmel kezdődött.

Az ismert 29 eset 32 megbírságolt Kötelezettet takar, hisz előfordul, hogy egy ügyben nem csak egy adatkezelő vagy adatfeldolgozó hibázik, sérti a GDPR rendeletet. **A bírságok összértéke 560.400.000 forintot ért el, ami közel 8-szor több mint 2021-ben volt.** *A több mint félmilliárdos értékhez nagyban hozzájárultak a dobogós helyezettjeink 425.000.000 fortint részesedéssel.*

#1

250 000 000

BUDAPEST BANK ZRT.

A bank 2017 óta alkalmazott hangelemző szoftvert, hogy mesterséges intelligencia segítségével elemezzék az ügyfélszolgálati telefonhívásokat. A szoftverrel egyrészt a munkavállalók teljesítményét értékelték, a várakoztatás, a csendben töltött idő és az egymásra beszélés alapján. Emellett adatokat gyűjtöttek az elégedetlen telefonálókról, hogy felmérjék, milyen sorrendben hívja őket vissza egy magasabb képzettséggel rendelkező munkatársuk. A rangsoroláshoz minden hívást rögzítettek, majd a szoftver kulcsszavak (például trágár szavak) és érzelmi, hangulati elemek azonosításával állította ki a listát – bár utóbbit csak az esetek 8%-ában ismerte fel.

A bank honlapján lévő adatkezelési tájékoztató nem tartalmazott érdemi információt a hangelemzésről, csak a minőségbiztosítást és panaszmegelőzést jelölték meg célként. A mesterséges intelligencia alkalmazásának adatvédelmi veszélyeire a hatásvizsgálat során is kitértek, de az érdekmérlegelési teszt nem tartalmazott megoldást ezek kezelésére.

A MEGSÉRTETT JOG

GDPR 5. cikk (1) bekezdés a) és b) pont, 6. cikk (1) és (4) bekezdés, 12. cikk (1) bekezdés, 13. cikk, 21. cikk (1) és (2) bekezdés, 24. cikk (1) bekezdés, 25. cikk (1) és (2) bekezdés

#2

95 000 000

KISKERESKEDELMI ÜZLETLÁNC

Több panasz érkezett a Hatósághoz a kiskereskedelmi üzletlánc alkoholtartalmú italok kapcsán kialakított adatkezelési gyakorlatára vonatkozóan.

Az üzletlánc alkoholtartalmú italok vásárlása esetén bemondásra – más bejelentések szerint fényképes igazolvány átadására kötelezve – rögzítette a vásárló születési idejét. Az adatkezelés céljáról, időtartamáról és jogalapjáról a pénztáros nem tudott tájékoztatást adni. A Hatóság előzetes értesítés nélküli szemle során igazolta a panaszba foglaltakat.

Az adatkezelő jogalapként a fogyasztóvédelemről szóló 1997. évi CLV. törvény 16/A. § (1) és (4) bekezdéseit hivatkozta meg, amely szerint alkoholtartalmú italok vásárlását megelőzően „a vállalkozás vagy annak képviselője kétség esetén felhívja a fogyasztót életkorának hitelt érdemlő igazolására", azonban az üzletlánc általános jelleggel – egy bejelentő 70 éves volt – minden alkoholos italt vásárló életkorát 180 napig tárolta a kasszarendszerben.

A MEGSÉRTETT JOG

GDPR 5. cikk (1) bekezdés a) és c) pont, 6. cikk, 12. cikk, 13. cikk, 32. cikk (1) és (4) bekezdés

#3

80 000 000

AMPLIFON MAGYARORSZÁG KFT.

A Hatósághoz több bejelentés érkezett, miszerint a Kötelezett postai úton ingyenes szűrővizsgálatra történő invitálást küldött részükre, a hozzájárulásuk nélkül. A Kötelezett az érintettek nevét és címét a Belügyminisztérium nyilvántartásából rendszeresen kérelmezte, először direkt marketing majd piackutatási célú kapcsolatfelvételre hivatkozva. A Hatóság által vizsgált időszak alatt 300.000-400.000 érintett adataihoz jutottak így hozzá.

A Hatóság megállapította, hogy a piackutatás mint cél nem fedte a valóságot, mivel továbbra is az újabb ügyfelek elérése volt a cél. A Kötelezett az érintetteket és a Belügyminisztériumot is megtévesztette, célját elfedte, ezzel megsértette a tisztességes eljárás elvét.

Jogalapként önkéntes hozzájárulást jelöltek meg, mivel álláspontjuk szerint az érintettek korábban jelezhették volna a Belügyminisztérium felé, hogy nem kívánják adataikat rendelkezésre bocsátani piac- és közvéleménykutatás céljából. A Hatóság szerint a hozzájáruláshoz az érintettnek megfelelő tájékoztatást követően önkéntesen és egyértelműen kell a beleegyezésüket kinyilvánítani. A kiküldött értesítőkön lévő adatkezelési tájékoztatás hiányos volt, többek közt nem tartalmazta az adatkezelő adatait, a valós célt és helyes jogalapot, az igénybe vett adatfeldolgozókat.

A MEGSÉRTETT JOG

GDPR 5. cikk (1) bekezdés a) és b) pont, 6. cikk (1) bekezdés, 12. cikk (1) bekezdés, 14. cikk

#4

30 000 000

MAGYAR ÉREMKIBOCSÁTÓ KFT.

Az ügy bejelentője a Magyar Éremkibocsátó Kft. adatkezelési gyakorlatát kifogásolta, mivel weboldalukon vásárolva a rendeléskor megadott személyes adataival egy felhasználói fiókot regisztráltak neki, amiről csak utólag tájékoztatták.

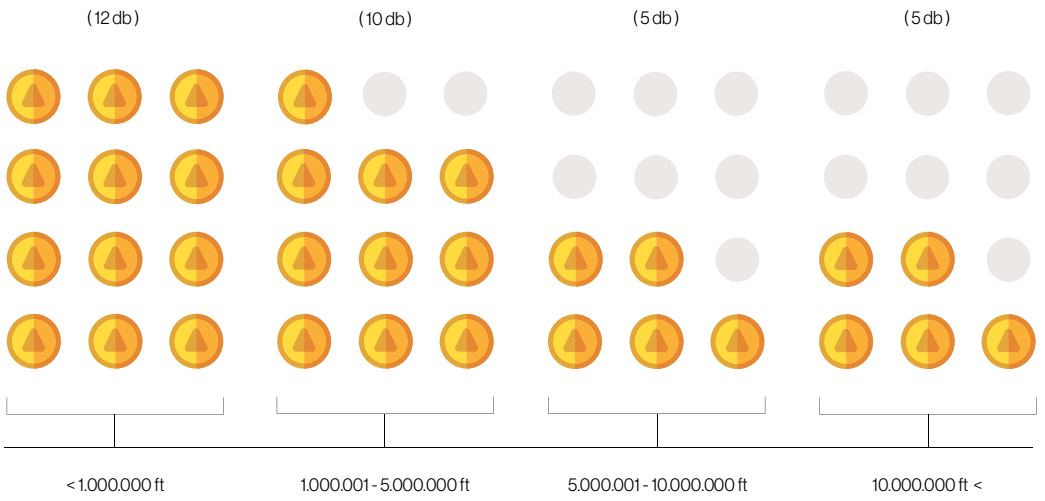
Az esettel kapcsolatban a Hatóság főként azt vizsgálta, hogy a személyes adatok megszerzése hogyan történik az új ügyfeleknél. Az új ügyfelek online, postái úton (más újság előfizetésekhez mellékelt formanyomtatvány visszaküldésével) vagy telefonon rendelhettek. Utóbbi két mód esetében az adatok kezeléséhez való hozzájárulás megfontolásához nem megfelelően vagy nem biztosították a szükséges minimális információkat. Ezen felül a Hatóság kifogásolta, hogy a begyűjtött email címeket célzott Google és Facebook hirdetésekhez is használták, ehhez viszont nem biztosítottak külön hozzájárulási lehetőséget.

A Kérelmezett megsértette az előzetes tájékoztatás nyújtásának kötelezettségét, a jogszerű, átlátható adatkezelés elvét, a célhoz kötöttség elvét, és megfelelő hozzájárulás nélkül kezelte több ezer érintett adatait.

A MEGSÉRTETT JOG

GDPR 5. cikk (1) bekezdés a) és b) pontja, 6. cikk (1) bekezdés, 7. cikk (2) bekezdés, 12. cikk (1) bekezdés, 13. cikk

Az összértéken túl az átlagos bírságérték is nőtt, méghozzá több mint 10-szeresére, 17.512.500 forintra. Ez a szám elsőre sokkolóan magas, viszont a csúcstartók eseteit ismerve a valóságot jobban tükrözi a medián érték, ami ellensúlyozva a kirívóan magas összegeket 2,5 milliót forintot tett ki. Azonban a legkisebb bírság is elérte a 200.000 forintot.



#1	Pénzintézetek	8 db
#2	Egyéb	6 db
#3	Telekommunikációs vállalat	4 db
#3	Egészségügyi szolgáltató	4 db
#4	Politikai párt	3 db
#4	Forgalmazó	3 db
#5	Szerelő	2 db
#5	Szálláshely	2 db

KIKET BÍRSÁGOLT A NAIH?

A Hatóság által nyilvánosan közzétett határozatok többségében nem nevezik meg a kötelezettet, akivel szemben az eljárás indult – ez alól általában nagy számú érintett esetében teszneк kivételt – viszont az esetek bemutatásából a kötelezettek foglalkozási köre egészen pontosan behatárolható.

2022-ben a legtöbb szabálysértést a pénzügyi szektorban tevékenykedők – bankok, hitelintézetek, követeléskezelők – követték el. Őket a szintén nagyobb vállalkozásméretű telekommunikációs szolgáltatók követték a sorban. Az adatvédelmi rendelet betartásának kötelezettsége azonban nem függ a cégmérettől, kisvállalkozások, mikrovállalkozások, sőt még egyéni vállalkozók is kerülhetnek a Hatóság célkeresztjébe mint például javítást-felújítást végző szolgáltató, szálláshely tulajdonos, szülész-nőgyógyász és autószerelő is kapott bírságot – itt ne felejtsük el, hogy a legalacsonyabb bírság is 200.000 Ft volt. A választások évében ahogy várható volt, néhány politikai párt is megsértette a GDPR rendelkezéseit.

LEGGYAKORIBB SZABÁLYSZEGÉSEK

A sértett rendelet cikkek szerint a legtöbb problémát az 5. – személyes adatok kezelésére vonatkozó elvek, 6. – az adatkezelés jogszerűségére vonatkozó jogok, 12. – tájékoztatásra és érintetti jogok gyakorlására vonatkozó intézkedések és a 13. – az érintettek részére rendelkezésre bocsátandó információkat (adatkezelési tájékoztató) érintő hiányosságok okozták.

A 9. cikkben szabályozott különleges személyes adatok kezelését is számos esetben sértették meg, ha azt is figyelembe vesszük, hogy az e fajta adatok (pl. faji, etnikai, politikai véleményre, vallási meggyőződésre utaló személyes adatok, egészségügyi adatok, szexuális irányultságra vonatkozó személyes adatok) kezelésére a működő vállalatok közül csak kevésnek van lehetősége, mivel bizonyos kivételeket leszámítva (pl. egészségügyi célzattal) tilos.

Ezek mellett a következő cikkeket sértették meg gyakran:

7. cikk: Hozzájárulással kapcsolatos előírások
14. cikk: Milyen információkat kell az érintett részére rendelkezésre bocsátani, ha az adatai nem közvetlenül tőle kerültek az adatkezelőhöz
15. cikk: Az érintett hozzáférési joga
17 cikk: Törléshez való jog
21. cikk: Tiltakozáshoz való jog
24. cikk: Adatkezelő feladataiban ejtett hiányosságok: technikai és szervezési intézkedések
25. cikk: Beépített és alapértelmezett adatvédelem
31. cikk: Együttműködés a felügyeleti hatósággal
32. cikk: Az adatkezelés biztonság

TANULSÁG, AJÁNLÁS

Az esetekből látható, leggyakrabban milyen területeket érintenek hiányosságok. A következőkben a legtöbbször problémát okozó rendeletrészeket vesszük számba, és szedjük pontokba mikre érdemes nagyobb figyelmet fordítani, a hibák elkerülése érdekében.

MEGFELELŐ JOGALAP

A GDPR előírásainak betartásához kulcsfontosságú, hogy az adatkezelők meghatározzák, az érintettek adatait mely jogalapra hivatkozva kezelik, hisz ezzel támasztható alá, miért is van birtokukban az adat.

Gyakran megesett, hogy a Hatóság nem tartotta a célhoz mérten megfelelőnek a választott jogalapokat, ezért érdemes szakértővel konzultálva megválasztani és megindokolni, ahelyett hogy mintákból dolgozva átmásoljuk, vagy az elsőre legnagyobb kört lefedő jogos érdekre rábökünk.

A nyilvánosságra hozott ügyekben jellemzően két jogalap okozott gondot, az említett jogos érdek és a hozzájáruláson alapuló adatkezelés.

SEGÍTÜNK!

Vegye fel a kapcsolatot szakértőinkkel, ha szeretné elkerülni a bírságot! Segítünk, hogy az adatvédelmi folyamatai a GDPR rendeletnek megfelelően, mégis vállalatára szabottan valósuljanak meg.

Kérjen ajánlatot kis- és középvállalkozóként, vagy akár nagyvállalatként, önkormányzatként, nonprofit szervezetként is, hisz gyakorlott csapatunk az Ön üzleti folyamataihoz igazítva támogatja az adatvédelmi megfelelését.

KÖZEPES- ÉS NAGYVÁLLALATI AJÁNLATUNK

Tanácsadási szolgáltatásunk már kifejezetten egyéni- mikro- és kisvállalatok számára is költséghatékonyan elérhető. Kérje szakértőink segítségét!

EGYÉNI- ÉS KISVÁLLALATI AJÁNLATUNK

TOVÁBBI INFORMÁCIÓ

crosssec solutions

gdprbirsagok.hu
tanacsadas.crosssec.com
info@crosssec.com

ÉRDEKMÉRLEGELÉS

Ahogy az imént körbejártuk, a jogos érdek az adatkezelők kedvelt jogalapja, azt viszont kevesen tudják, hogy ehhez tartozik a legtöbb adminisztráció is, például érdekmérlegelési tesztet kell végezni az alkalmazása előtt. Az érdekmérlegelés két fél érdekét állítja szembe, az adatkezelőét és az érintettét.

A közzétett esetekből tudjuk, hogy jogos érdek megjelölése esetén a Hatóság egyből kérni szokta az érdekmérlegelést is, azonban még nem volt olyan határozat, amiben nem lett volna hiányosság benne – de az előfordult már, hogy a dokumentum hiányzott, nem készült el. Legjellemzőbb hiba, hogy csak az adatkezelő érdekeit tartalmazza, az érintett ellenérdekeit nem, így a kettő nem kerül összevonásra, súlyozásra.

TÁJÉKOZTATÁS

Az érintetteket minden esetben tájékoztatni kell az adatgyűjtés tényéről és részleteiről, mielőtt az adatkezelést megkezdjük. Tudatni kell velük ki/kik, milyen adatait, milyen célból és jogalappal kezelik, mennyi ideig őrzik meg, vannak-e más adatkezelők vagy adatfeldolgozók, akik hozzáférnek az adatokhoz, továbbítják-e EU-n kívülre és milyen jogokkal élhetnek (pl. hozzáférés, visszavonás).

A hatósági esetekben sokszor előfordult, hogy az érintettek nem kaptak tájékoztatást, vagy a tájékoztatás tartalmi elemei nem feleltek meg a valós adatkezelésnek. Fontos, hogy az adatkezelési tájékoztatók naprakészen legyenek tartva és a valós üzleti folyamatokhoz igazítsuk. Lényeges tisztázni, hogy adatvédelmi tájékoztatóra nem csak a weboldal tulajdonosoknak van szüksége, hanem mindenkinek, aki üzleti célból személyes adatokat kezel, pl. kapcsolattartási adatok, számlázáshoz szükséges adatok esetében is, akár papír alapon ismertetve.