blancco

Törölni kötelező

Útmutató informatikai adathordozók törléséhez
munkáltatók és informatikai szolgáltatók számára

www.blancco.hu

A Blancco termékeit Magyarországon
a V-Detect Antivírus Kft. képviseli,
amely viszonteladói segítségével
szolgálja ki a végfelhasználókat.

Bevezetés

Európában az egyik legfontosabb alkotmányos érték az emberi méltóság. Minden alapjogot, így a személyes adatok védelméhez való jogot is ebből vezetünk le.

A digitális korszakba történő átlépéssel azonban ez a jogunk számos új módon került veszélybe. Egy munkavállaló böngészési előzményeiből például munkáltatója következtethet a betegségeire, vallási hovatartozására és politikai nézeteire. Ilyen adatok folyamatosan keletkeznek az általunk használt informatikai eszközökön – számítógépeken és okostelefonokon –, és könnyű belátni, hogy magánéletünkre veszélyt jelent, ha ezek az eszközök úgy kerülnek át másokhoz, hogy azok adatmentesítése, vagy más szóval „fertőtlenítése" nem történt meg.

A General Data Protection Regulation, azaz a GDPR, az Európai Unió új adatvédelmi rendelete egy hosszú jogalkotási folyamat után, 2016. május 24-én lépett hatályba, és kétéves türelmi időszak után 2018. május 25-től kell alkalmazni.

Ez a rendelet széles körben ír elő adattörlési kötelezettséget a piaci és az állami szektorok szereplői számára. Minden munkáltató esetében keletkezik ilyen kötelezettség, de olyankor is, ha egy gazdasági szervezet informatikai adathordozók, például mobiltelefonok vagy számítógépek, merevlemezek forgalmazásával vagy javításával foglalkozik.

Jelen útmutatónk kizárólag az adathordozók (például merevlemezek, notebookok, mobiltelefonok és tabletek, flashkártyák, USB-kulcsok) törlésének kötelezettségét taglalja, de nem tér ki mindazon esetekre, amelyek során a gazdasági szervezetnek adatokat (például egy bejegyzést egy adatbázisból, fájlokat vagy mappákat) kell törölnie.

Ezeket a törlési eseteket a Nemzeti Adatvédelmi és Információszabadság Hatóság NAIH/2019/2450. számú állásfoglalása segít értelmezni, amely a NAIH weboldalán elérhető.

Legfontosabb fogalmak

Adathordozó

Minden olyan informatikai eszközt adathordozónak tekintünk, amely adatokat képes tárolni. A leggyakoribb adathordozók a merevlemezek és SSD-meghajtók, a mobiltelefonok, az USB-kulcsok (pendrive-ok), valamint a például fényképezőgépekben és mobiltelefonokban is használt memóriakártyák.

Az adathordozókon folyamatosan keletkeznek adatok szándékosan és akaratlanul is. Utóbbira példa a böngészési előzmények mentése, amelyet a böngészők automatikusan elvégeznek, hogy felgyorsítsák az oldalak betöltődését.

Adattörlés vagy fertőtlenítés

Általánosságban elmondható, hogy a felhasználók rendelkezésére álló törlési lehetőségek nem tüntetik el helyreállíthatatlan módon az adatokat. A helyreállíthatatlan törlés kötelezettsége levezethető az alapelvekből (adattakarékosság elve, pontosság elve és a korlátozott tárolhatóság elve), illetve az érintettnek a törléshez való jogából, valamint az adatkezelés korlátozásához fűződő jogából is.

Amikor egy felhasználó töröl egy dokumentumot a gépéről úgy, hogy azt a kukába dobja, majd a kukát kiüríti, akkor nincs tisztában azzal, hogy a fájlt magát nem törölte, csak jelezte az operációs rendszer számára, hogy már nincs szüksége az adott dokumentumra, és alkalomadtán az operációs rendszer akár más dokumentumot is menthet annak helyére.

Olyan ez, mintha szeretnénk eltüntetni egy papíralapú jelentés tartalmát, de magát a jelentést nem semmisítenénk meg, csak annak a tartalomjegyzékét. Így ugyan valamivel nehezebb lesz kiigazodni a jelentés tartalmában, de korántsem lehetetlen, sőt, talán még nem is bonyolult.

Az adathordozó felülírással történő fertőtlenítése viszont azt jelenti, hogy az adathordozó teljes területe (beleértve a gyártó vagy az operációs rendszer által elrejtett területeket is) felülírásra kerül speciális algoritmusok segítségével. Ez pedig ahhoz hasonlítható, mintha a fenti papíralapú jelentés minden egyes sorát kihúzná valaki egy átláthatatlan különleges tinta segítségével, amely nem csupán letakar, hanem véglegesen kitöröl minden egyes sort.

A minősített adattörlés alatt pedig azt értjük, ha ez a felülírás egy olyan szoftver segítségével történik, amelyet külső szervezet – például a NATO vagy az adott ország nemzetbiztonsági szervezete – minősített, és megállapította, hogy az adattörlési eljárás valóban véglegesen és visszaállíthatatlan módon törli az adatokat.

A legismertebb és legelterjedtebb ilyen szoftver a Blancco, amely a világon a legtöbb biztonsági minősítéssel (például NATO, Common Criteria, CESG, BSI, DIPCOG) rendelkezik, és sztenderd megoldásnak számít az adattörlés területén.

Törlési jegyzőkönyv

Fontos megjegyezni, hogy a vonatkozó rendelkezések nem csupán az adathordozók fertőtlenítését (azaz visszaállíthatatlan és végleges törlését) írják elő, hanem a törlés igazolását is.

Ezért minden egyes adathordozó fertőtlenítését olyan jegyzőkönyvvel kell igazolni, amely tartalmazza az adathordozó azonosítóját (sorozatszámát), a törlés helyét, idejét, a törlést elvégző személy megnevezését, valamint a törlés eredményét (sikeres vagy sikertelen).

Ez jelentős adminisztrációs terhet jelent a gazdálkodó szervezetek számára, ugyanakkor a törlés ténye kizárólag ilyen tanúsító jegyzőkönyvekkel igazolható. Az adminisztrációs terhet pedig a modern törlőszoftverek tudják csökkenteni, amelyek a jegyzőkönyveket automatikusan létrehozzák.

A jegyzőkönyveket ezután visszakereshető módon szükséges tárolni, mivel hatósági ellenőrzés esetén ezekkel lehet igazolni a törlések megfelelő elvégzését.

Útmutató munkáltatók számára

Minden cégvezető számára egyértelmű, hogy a vállalat bizalmas adatait óvni kell, és mindent meg kell tenni annak érdekében, hogy azok ne kerüljenek nyilvánosságra. Azonban az már kevésbé egyértelmű, hogy az adathordozók törlésére nem csak ezért, hanem a munkavállalók személyes adatainak védelme érdekében is szükség van – és eme jogszabályi kötelezettség elmulasztása büntetéseket is vonhat maga után.

A GDPR és a hazai jogszabályok alapján az alábbi gyakran előforduló eseteket érdemes megkülönböztetni, majd ezekre megfelelő munkahelyi gyakorlatot kialakítani.

Gazdaváltás

Szervezeten belüli gazdaváltásnak hívjuk, ha egy céges adathordozót (tipikusan notebookot vagy mobiltelefont) az egyik munkatárs visszaad a vállalat számára, majd azt egy másik munkatárs megkapja használatra.

Nyilvánvaló, hogy amennyiben a két munkatárs beosztása és munkaköre más, az adathordozót megkapó munkatársnak valószínűleg nincs joga megismerni az adathordozót visszaadó munkatárs vállalati dokumentumait, ügyeit, feljegyzéseit.

De igaz emellett az is, hogy a vállalat kötelessége gondoskodni arról is, hogy az adathordozót visszaadó munkatárs személyes adatai (például családi fényképei és videói) semmiképpen se kerülhessenek az adathordozót megkapó munkatárshoz.

Ezért a szervezeten belüli gazdaváltás esetén egyszerre a vállalat érdeke, hogy védje a vállalati adatokat, és egyszerre kötelessége, hogy védje a munkatársának személyes adatait, és ezért a gazdát váltó informatikai eszközt fertőtlenítse az adatoktól.

Annak megértéséhez, hogy a személyes adatok védelméhez miért van szükség adattörlésre, gondoljon bele, hogy egy notebook tárolhatja használójának böngészési előzményeit. Ezekből pedig akár következtetéseket lehet levonni az adott munkatárs betegségeire, vallási hovatartozására és politikai nézeteire. Amennyiben a munkáltató ezeket az adatokat felhasználja arra, hogy profilozza a munkavállalóit, majd a létrehozott profil alapján döntsön azok előléptetéséről, úgy jogsértést követ el.

A másik oldalról a munkáltató hírnevét és vonzerejét növeli az, ha munkavállalói tudják, hogy személyes adataikat a munkáltató folyamatosan védelmezi, és számukra megnyugtató módon törli azokat a visszaadott informatikai adathordozókról, majd ezt a törlést a munkavállaló felé jegyzőkönyvvel igazolja.

Jogi háttér

A munkavállaló adatainak vonatkozásában a munkáltató tipikusan adatkezelői státuszban van, viszonylag ritkábban fordul elő az, hogy a munkáltató adatfeldolgozónak minősül. A munkáltató cég tulajdonában lévő eszközök esetében mindig a munkáltató felel az eszközökön található tartalmakért, ideértve a személyes adatokat is. Ezen ellenőrzési és törlési kötelezettsége alól akkor sem mentesül a munkáltató, ha a munkaszerződésben kiköti, hogy az adathordozó a munkavisszonnyal össze nem függő, azaz például magánjellegű célokra nem használható. A munkavállaló mint érintett kérésére a munkáltató köteles tájékoztatást adni a törlés megtörténtéről, mely akár egy jegyzőkönyv átadásával is megvalósítható.

Adathordozók szervizelése

A notebookok, mobiltelefonok szervizbe adása során ügyelni kell arra, hogy a szervizbe adott adathordozókon ne maradjanak vállalati adatok, de a munkatársak személyes adatait is óvni kell az illetéktelenektől.

Vezetett már adatvédelmi botrányhoz, hogy egy ismert politikus szervizbe adott notebookjáról kikerültek a politikus privát fotói.

Általánosságban javasoljuk, hogy az adattörlést az adatgazdához a legközelebb végezzük el. Így az adathordozót használó munkatárs először egy törlési jegyzőkönyvet kap, amely igazolja, hogy az általa átadott adathordozó már úgy kerül szervizelésre, hogy arról a személyes adatai törlésre kerültek.

Adathordozók leselejtezése

Az adathordozókat nem lehet leselejtezni, adományozni vagy a munkatársak részére eladni anélkül, hogy azok igazolható, jegyzőkönyvezett és visszaállíthatatlan módon törlésre kerüljenek.

A törlés tényét minden esetben jegyzőkönyvvel kell igazolni, és a jegyzőkönyveket visszakereshető módon kell tárolni.

Mindez azt jelenti, hogy a vállalatoknak az informatikai adathordozókról nyilvántartást kell vezetniük, és az egyes adathordozókat – különösen a számítógépeket és mobiltelefonokat – úgy kell leselejtezniük, hogy azokon a selejtezés előtt adattörlést végeznek egy olyan adattörlő szoftver segítségével, amely garantálja, hogy az adatok véglegesen és visszaállíthatatlan módon törlésre kerülnek.

Mindez természetesen költséggel járhat a vállalatok számára, amelyet a működési költségeikbe be kell építeniük. Néhány fős vállalkozások használhatnak ingyenes adattörlési megoldásokat (például DBAN), az ennél nagyobb vállalkozások számára viszont olyan megoldás használata javasolt, amely a törléseket a legnagyobb mértékben képes automatizálni, és a törlési jegyzőkönyveket is automatikusan létrehozza (például Blancco). Az ilyen automatizált szoftverek használatának licencdíja jellemzően kevesebb, mint a manuális adminisztrációval járó emberi erőforrás költsége.

A költségek kezelésére megoldást jelenthet, ha a vállalatok már az eszközök beszerzésekor kalkulálnak azzal, hogy az eszközöket leselejtezéskor törölni szükséges, és előfizetést kötnek adattörlési megoldás használatára.

Útmutató informatikai kereskedők és szolgáltatók számára

Informatikai beszállítók, notebook- és mobiltelefon-gyártók, mobilszolgáltatók, szervizek, valamint használt PC-kkel és GSM-ekkel kereskedők egyaránt kötelezettek adattörlést végezni az általuk kezelt informatikai adathordozókon, hogy biztosítsák, hogy azokon ne maradjanak személyes adatok.

A Blancco Technology Group 2019-es tanulmánya szerint a használt merevlemezek 42%-a tartalmaz még szenzitív és személyes adatokat, amikor újra forgalomba kerül. A kísérlet során felvásárolt használt merevlemezeken a szakértők többek között ilyen adatokat találtak:

- Egy magas nemzetbiztonsági minősítéssel rendelkező szoftverfejlesztő és családtagjainak útlevelei, születési bizonyítványai, önéletrajza és pénzügyi feljegyzései.
- Diákigazolványok, egyetemi tanulmányokkal kapcsolatos iratok, a velük társított e-mail-címekkel együtt.
- Egy nagyobb utazási iroda 5 GB méretű archivált irodai levelezése.
- Egy szállítmányozási cég 3 GB méretű adatállománya, amely tartalmazta a szállítmányok részleteit, időbeosztását és a kamionok adatait.
- Egy üzletlánc irodai adatbázisa 32 ezer fotóval együtt.
- Egy iskola adatai fotókkal, valamint a tanulók nevével, osztályzataival és dokumentumaival.

Amennyiben ilyen szenzitív adatok nyilvánosságra kerülnek, az jelentősen károsíthatja mind a kereskedő, mind az eredeti tulajdonos hírnevét.

Amennyiben egy vállalkozás informatikai adathordozók kereskedelmével, szervizelésével, bérbeadásával foglalkozik, úgy jogszabályok kötelezik az adathordozók fertőtlenítésére, azaz megfelelő és visszaállíthatatlan törlésére. Ezeket a vállalkozásokat jegyzőkönyvezési kötelezettség is terheli, minden egyes kezelt vagy értékesített adathordozó tekintetében.

A kereskedőknek emellett az alábbi két tényező miatt javasolt törölniük az adatokat az általuk forgalmazott számítógépek merevlemezéről:

1. Nem jogtiszta szoftverekkel kapcsolatos kockázatok elkerülése
A nem törölt adathordozókon olyan szoftverlicencek maradhatnak, amelyek felhasználására az adathordozó új tulajdonosának nincs jogosultsága.

2. Személyes adatok jogosulatlan kezelésével kapcsolatos kockázatok elkerülése
Jogvita alakulhat ki abból, ha a kereskedő által értékesített adathordozókról személyes adatok kerülnek ki.

Eszköz bérbeadása

Informatikai beszállítók foglalkoznak számítógépek és szerverek, storage-rendszerek lízingbe adásával, vagy biztosítanak ilyen eszközöket projektekhez ügyfeleik részére.

Egyes esetekben a lízing lezárásakor vagy a projekt befejezésekor ezek az eszközök visszakerülnek a szolgáltatóhoz, de nyilvánvaló, hogy az ügyfél vállalati adatai, valamint az ügyfél munkavállalóinak személyes adatai törlésre kell, hogy kerüljenek.

Ezért célszerű már a lízing- vagy a bérleti szerződésbe beépíteni az adattörlés díját, ellenkező esetben az ügyfél ragaszkodhat ahhoz, hogy a szolgáltató jegyzőkönyvvel igazolja az adatok törlését az eszközökről.

A fenti esetben az adattörlési kötelezettség az adatkezelőt (a lízingbe vevő céget) terheli, a szolgáltatót viszont ellenőrzési kötelezettség terheli.

Természetesen, itt is figyelembe kell venni a lízingszerződés idevonatkozó rendelkezéseit.

Garanciális csere és szervizelés

Amennyiben egy vállalkozás informatikai adathordozók javításával foglalkozik, rendszeresen találkozik személyes adatokat tartalmazó adathordozókkal.

Az esetek jelentős részében ilyenkor a vállalkozás feladata a személyes adatok lementése, majd az eszköz javítása után a személyes adatok visszatöltése.

Ezekben az esetekben fontos, hogy a lementett adatok (fájlok és mappák) törlését jegyzőkönyvvel kell igazolni az ügyfél felé, és az adatokat úgy kell törölni, hogy azok visszaállítása ne legyen lehetséges. Ilyen megoldást biztosítanak például a Blancco fájltörlési szoftverei, amelyek a jegyzőkönyvezés feladatát is automatizálják.

Az esetek egy más részében az adathordozót garanciálisan cserélik, így nem kerül vissza az ügyfélhez. Ilyen esetekben az átvett adathordozót fertőtleníteni kell az ügyfél adataitól. Amennyiben ez az adathordozó technikai meghibásodása miatt nem lehetséges, úgy az adathordozót lehetőleg a megsemmisítésére vonatkozó szabványok szerint meg kell semmisíteni. Nagyvállalatok esetében a megsemmisítésre célszerű speciális megsemmisítőberendezést használni, ilyen például a jegyzőkönyvezés feladatát is elvégző, NATO-minősített MAXXeGUARD berendezés, amely rögzített vágáshosszal az adathordozókat milliméteres csíkokra aprítja fel.

Felvásárlás

Az informatikai eszközök felvásárlásával foglalkozó vállalkozásoknak az eszközök felvásárlásakor meg kell győződniük arról, hogy azokon nem maradtak személyes adatok, vagy gondoskodniuk kell az adatok törléséről.

Amennyiben a felvásárlás során az eladó egyértelműen, törlési jegyzőkönyvekkel igazolja azt, hogy fertőtlenítette az adathordozókat, a vevőnek ellenőriznie kell, hogy a jegyzőkönyvek tartalma megfelel-e a valóságnak. Amennyiben a törlési jegyzőkönyvek nem állnak rendelkezésre, úgy a vállalkozásnak nagy valószínűséggel adattörlést is kell végeznie még akkor is, ha úgy gondolja, hogy az adathordozók nem tartalmaznak személyes adatokat.

Használt informatikai adathordozó nem hozható forgalomba anélkül, hogy az adatok törlését a kereskedő ne tudná törlési jegyzőkönyvekkel igazolni.

A Blancco adattörlési megoldásairól

A Blancco a világ vezető gyártója a menedzselt, megbízható és minősített adattörlés területén. A nemzetbiztonsági szervezetek, a rendőrség, a pénzügyi szolgáltatók és a számítógépek újrahasznosításával foglalkozó szervezetek első számú választása. 1997-ben alapított vállalatunk a legtöbb szakmai minősítéssel rendelkező adattörlési megoldásokat kínálja a világon.

Finn központú cégünk 14 saját irodát tart fenn Európában, Észak- és Dél-Amerikában, Ázsiában és Ausztráliában. Szoftvereink és hardveres megoldásaink segítségével ügyfeleink mindennap több tízezer számítógépről törlik az adatokat; a Blancco Asset Manager használatával pedig minden egyes nap több tízezer hardver- és szoftverleltárt készítenek.

Kiemelt termékeink:

1. Blancco Drive Erasure notebookok, számítógépek és szerverek törlésére.
2. Blancco Mobile Erasure és Mobile Diagnostics okostelefonok törlésére és diagnosztikájára.
3. Blancco Removable Media Erasure memóriakártyák és USB-kulcsok törlésére.
4. Blancco Management Console a törlési jegyzőkönyvek nyilvántartására.
5. Blancco LUN logikai meghajtók törlésére.
6. Blancco Virtual Hyper-V- és VMware-támogatással.
7. Blancco File Erasure Datacenter Edition fájlok és mappák menedzselt törlésére.
8. Blancco Degausser mágneses adathordozók megsemmisítésére (hardver).
9. Blancco hardverek (E800 és 24 Bay Eraser) szervermerevlemezek tömeges törlésére.

A Blancco termékeinek segítségével:

– Az automatizálható és irányított folyamatok révén a lehető leggyorsabb és legbiztonságosabb módon valósítható meg az adattörlés.

– Tanúsítható, auditálható jegyzőkönyv készül minden sikeres törlésről.

– A törölt adatok semmilyen technológiával nem állíthatóak helyre.

– Csökken a szervezet jogi mulasztásának kockázata, a hírnév sérülésének veszélye, valamint a vállalat számára értéket jelentő adatok kiszivárgásának esélye.

– A Blancco termékei teljes mértékben eleget tesznek a biztonsági és titoktartási előírásoknak.

– A Blancco teljesen automatizált adattörlési folyamata a létező leggyorsabb törlési folyamatot nyújtja az iparágban.

Előnyünket a következő tényezőknek köszönhetjük:

– A hardver teljes írási sebességét kihasználjuk.

– Egyidejűleg több merevlemezt is tudunk törölni (akár több százat is egyszerre).

– Minden ügyfelünknél teljes mértékben személyre szabjuk az adattörlési folyamatot.

– Rendszeres termék- és driverfrissítéseket nyújtunk, a törlési sebesség és a hatékonyság maximalizálása érdekében.

– Lehetővé tesszük vásárlóink számára, hogy extra mezőket adjanak hozzá a riportoláshoz, mint pl. a projekt ID, a vásárló ID, a hely vagy a költségelszámolás helye.

– A Blancco Management Console használatával a riportolás és auditálás könnyűszerrel menedzselhető.

100%-os törlési biztonság

A Blancco garantálja a 100%-os adattörlést minden kompatibilis adathordozóról, beleértve a szervereket, a hagyományos PC-merevlemezeket, az SSD-meghajtókat, az okostelefonokat vagy flashmemóriákat. A Blancco törlési megoldásai teljesen biztonságosak, és a törölt adatok semmilyen technológiával nem állíthatóak vissza.

Riportolás és auditálás

Egyetlen törlés sem biztonságos, ha nincs bizonyíték annak sikerességéről, a törlést bizonyítandó dokumentumok előállítását pedig bizonyos esetekben törvény is előírja. A Blancco olyan részletes jegyzőkönyvet készít a törlésekről, amelyek tökéletesen megfelelnek minden adattörlésre vonatkozó előírásnak és jogszabálynak. Minden egyes törlésről digitálisan aláírt, a hamisítás ellen védett, ellenőrizhető jegyzőkönyv készül – teljesen automatikusan.

Nemzetközileg tanúsított törlési szabványok

A Blancco széleskörűen támogatja a nemzetközi felülírási szabványokat:

HMG Infosec Standard 5, Baseline/Lower Standard
HMG Infosec Standard 5, Enhanced/Higher Standard
BSI (German overwrite standard by Federal Office for Information Security/ Bundesamt für Sicherheit in der Informationstechnik)
U.S. Department of Defense Sanitizing (DOD 5220.22-M, DOD 5220.22-M ECE)
Bruce Schneier's algorithm
Navy Staff Office Publication (NAVSO P-5239-26)
National Computer Security Center (NCSC-TG-025)
Air Force System Security Instructions 5020
U.S. Army AR380-19
OPNAVINST 5239.1A
NSA 130-1
Peter Gutmann's algorithm
NAVSO P-5239-26 TOP SECRET (FEPROM)
NAVSO P-5239-26 SECRET or CONFIDENTIAL (FEPROM)
U.S. Army AR380-19 (FEPROM)
Firmware-based secure erase—ATA
Firmware-based secure erase—SCSI
NIST 800-88 ATA
Extended NIST 800-88 ATA
Extended NIST 800-88 SCSI
Blancco SSD Erasure

Minősítések

A Blancco a világ legtöbb minősítésével rendelkező adattörlési megoldása, amely sztenderdnek számít az adattörlés világában. A Blancco megoldásait használja a NATO, az Európai Unió különböző szervezetei, a legtöbb tagállam fegyveres szervezetei, bankok és más pénzintézetek.

A szoftvereink rendelkeznek többek között a NATO, Common Criteria, CESG, BSI, DIPCOG minősítésekkel.

Adatvédelmi alapfogalmak

Személyes adat: Azonosított vagy azonosítható természetes személyre (Érintett) vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító, vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

Különleges személyes adat: A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Adatkezelés: A személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Adatkezelő: Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Adatfeldolgozó: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

Érintett: Az adatkezelés alanya, bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.