SZILÁGYI SZABOLCS 2018.02.22.

Így kell adatot törölni a GDPR szellemében

Nemzeti szinten eddig is szigorú rendelkezések vonatkoztak az érzékeny adatok megsemmisítésére, de az Európai Unió Általános Adatvédelmi Rendeletének hatályba lépése után senki sem kerülheti el az információtörlés folyamatos feladatát.

A GDPR (General Data Protection Regulation) egyik nagyon fontos eleme, hogy a személyes adat tárolását minden esetben arra az időtartamra korlátozza, amíg az információ megléte valamilyen okból elengedhetetlen. Amikor ezek az okok megszűnnek, az adatot törölni kell. A GDPR előírja, hogy az adatkezelőnek törlési vagy rendszeres felülvizsgálati határidőket kell megállapítania, és azok megtörténtéről nyilvántartást kell vezetnie.

Ez annyira fontosnak terület, hogy tavaly szigorítási kérelmet adtak be ennek kapcsán a GDPR-hoz. Az eredeti szöveg ugyanis lehetővé teszi, hogy a vállalatok azután is tárolják ügyfeleik személyes adatait (anonimizálva), ha a vállalat és az ügyfél között megszűnt a jogviszony. Az Európai Parlament bizottsága viszont azt javasolta, az adatkezelők legyenek kötelesek az adatokat végleges és helyreállíthatatlan törölni.

Felülírt történelem

A magyarországi vállalatok annyiban előnyben lesznek, hogy az adattörlést az Infotörvény (teljes nevén: 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról) meglehetős alapossággal szabályozza. Minden esetben törölni kell az adatot, ha 1. annak kezelése jogellenes; 2. az érintett (az adat tulajdonosa) kéri; 3. az hiányos vagy téves – és ez az állapot jogszerűen nem orvosolható –, feltéve, hogy a törlést törvény nem zárja ki; 4. az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt; 5. a törlést bíróság vagy a hatóság elrendelte.

A hatályos rendelkezések szerint az adattörlési feladatokat a magyar vállalkozásoknak az adott pillanatban rendelkezésre álló legbiztosabb technológiával kell végrehajtaniuk. Ahhoz, hogy meghatározható legyen, mi felel meg minősített adattörlésnek, ismerni kell az adott folyamat tanúsítását. Ilyen például a német BSI (Bundesamt für Sicherheit in der Informationstechnik) vagy az amerikai U.S. Army AR380-19.

Közös jellemzőjük, hogy a hagyományos, operációs rendszerből kiadott törlési módszerekkel ellentétben alkalmazásukkal garantált az adatok valódi megsemmisítése, tehát azokat törlés után semmilyen rendszer-vissza/helyreállítási módszerrel nem lehet kinyerni az adathordozóról. A gyakran katonai szintű algoritmusok segítségével számos alkalommal felülírásra kerül az adott adathordozó felülete, így az információ örökre elvész.

Lássunk egy példát arra, hogyan megy végbe a folyamat! A többek között a Blancco által is használt DoD 5220.22-M szabvány olyan eljárást határoz meg, amely az adathordozók felülírását egyesek és nullák mintáival végzi el, három felülírási ciklusban, melyeket az eljárás végén egy visszaellenőrzés követ. Ennek során minden elérhető terü-

let felülírásra kerül először (bináris) nullákkal, aztán egyesekkel, végül pedig véletlenszerű mintával. Ezt követően az utolsó felülírási ciklus visszaellenőrzése zajlik le.

Mi a helyzet az archívumokkal?

Óhatatlanul is felmerül a kérdés, hogy miként lehet két, egymásnak látszólag ellentmondó feltételt kielégíteni. A biztonsági mentések és az archívumok készítése ugyanis bizonyos tekintetben szembe megy a személyes adatok védelmének új európai direktívájával: ha az adott szolgáltatást használó ügyfél szerződése megszűnik, személyes adatainak nem csak az aktív adatbázisokból kell(ene) törlődnie, hanem a különböző másolatokból is.

Az IDC tavaly nyáron tartott GDPR-workshopján megpróbálták feloldani ezt az ellentmondást. Ahelyett, hogy rögtön a titkosítás eszközéhez nyúlnának a szolgáltatók – hiszen például törvényi előírások (adószabályok) szerint egyes adatokat akár hét évre visszamenőleg is tárolniuk kell –, érdemes hatástanulmányt készíteni.

Nem árt tudni, hogy a mentés idején az adatok gyakran (újra)aggregálódnak, ami azt jelenti, hogy két vagy több forrás pszeudonimizált adatai vegyesen kerülhetnek a mentési adathordozóra. Adatbázis-szintű titkosítás hiányában a mentési adathordozók adatait ebben az esetben csak azután lehet deanonimizálni, ha több forrásból korrelálták őket, int körültekintésre a piackutató vállalat.

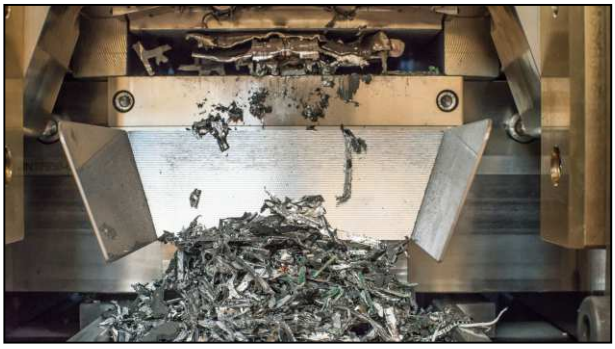
Amennyiben az információ titkosítatlanul kerül mentésre, olyan hozzáférés-szabályozást kell kialakítani, ami pontosan meghatározza, ki milyen adatokhoz férhet hozzá. Emellett a biztonsági mentésekért felelős személyeket a GDPR szellemiségének megfelelően monitorozni kell.

Konkrét számmal szolgált az általunk megkérdezett szakértő. *Gilincsek Szabolcs*, minősített GDPR-menedzser általános javaslata szerint a személyes adatokat tartalmazó mentéseket 28 napra érdemes beállítani (az üzleti adatokat pedig lehet hosszabb távon is). Véleménye szerint ennyi idő alatt olyan mértékben tud változni egy-egy ügyféladatbázis, hogy az archívumoknak nem sok haszna van.

És hogy honnan származik ez az egzakt szám? Mivel a törlési jog érvényesítésére (mint minden érintett jog érvényesítésére) egy hónap áll rendelkezésére az Adatkezelőnek, ez február hónapban történő kérés esetén csak 28 napot jelent, így biztosan nem tudunk mellélőni azzal, hogy a mentésekből nem törlődnek. Persze arra figyelni kell, hogy ha töröltünk egy adatot és valamiért vissza kellett állítani 28 napon belül egy mentést, erre vonatkozóan ki kell dolgozni egy stratégiát, hogy a visszaállított adatokból is eltűnjenek a már törölt adatok.

Meghajtók törlése, leselejtezése

Végül említést érdemel a komplett adathordozók dokumentált kivezetése is, amely szintén fontos követelmény a GDPR irányából. A leselejtezni tervezett adattároló eszközöket nem lehet pusztán kiszerelni az addig használt rendszerekből, majd értékesíteni, hanem gondoskodni kell a rajtuk levő információ jegyzőkönyvezett, minősített törléséről. Ezt sem feltétlenül a személyes adatokat kezelő cégnek kell végeznie, igénybe vehet külső adattörlési szolgáltatást is.



Amit nem lehet digitálisan törölni, azt meg kell semmisíteni. Munkában a MAXXeGuard

Ez utóbbi esetben a szolgáltató felel azért, hogy a számára átadott adathordozó médiumról véglegesen és visszaállíthatatlanul törlésre kerüljön a tárolt információ. Ha a tárolóegység hibás, és ezért nem végezhető el rajta a törlési művelet, akkor fizikai érdemes fizikailag megsemmisíteni, amihez olyan eszközök nyújtanak segítséget, mint a MAXXeGUARD. A kifejezetten adathordozók megsemmisítésére kialakított darabológép, amely NATO minősítéssel rendelkezik, képes az adathordozókat – jegyzőkönyvezett módon – akár milliméteres darabokra szétvágni.

Így az adatkezelő nyugodt lehet afelől, hogy rendszeréből nem szivárog ki semmilyen személyes adat. Ez a GDPR-nak való megfelelőség mellett a tetemes büntetések elkerülését is garantálja.

Forrás: **https://bitport.hu/eu-nak-kedves-adattorles**

Válogatta: Fonyó Istvánné