

Adatkezelési folyamatok végén: személyes adat megsemmisül-e vagy csak átalakul?

Krüpl Zsolt
2021. május 25.



Előzmény

A törlés nem törlés előadás – <https://www.cert.hu/huncert-workshop-2019>

- költséges visszaállíthatatlan módon törölni az adatot
- gyakorlatban „inaktív” jelölést adunk az adatnak

Érzékeny kérdések:

- biztonsági másolatok
- egyéb átmeneti célokra használt másolatok
- tesztrendszerbe áttöltött adatok sorsa
- archiválás

További érzékeny kérdések:

- adathordozó csere (rendszerből kikerül), szolgáltatás költöztetés esete
- szolgáltatás leállítása után mi lesz az adathordozó sorsa?

Törlés a gyakorlatban

Milyen szinten töröljük az adatokat? /* tetszőleges adatot */

- a) Az adat mellé odaírjuk, hogy „ne használd”
- b) Megjelöljük az alkalmazásban, hogy „inaktív”, ezáltal meg sem jelenítjük.
- c) „Eltávolítjuk” az adatsort az adatbázisból
- d) Felülírjuk az adatot vagy „lesikáljuk” a háttértárolóról – költséges, nehézségekbe ütközik

Biztonsági másolat, incidens utáni visszaállítás kérdése

- Biztonsági másolatból is törölni kellene?
- Esetleg elég valahol jelölni, hogy visszaállítás folyamán inaktívvá kell tenni? /* hol? */

További kérdés: biztonsági másolatok között eltelt időben levő törlések hogyan követhetőek nyomon?

Adat törlés **vagy** információ törlés?

- 1) Adatok törlésénél a cél az adat fizikai törlése, netán megsemmisítése (lásd: A törlés nem törlés c. előadást)

- 2) Információ törlésénél a cél
 - ha megjelöljük „ne használd”-ra, akkor a továbbiakban ne használjuk.
 - a „ne használd” jelzést **senki ne vegye le többé róla**
 - ha kikerül a kontroll a kezeink közül (adat más kezelésébe kerül, adathordozó átadásra kerül), akkor
 - vagy szerződéssel védendő. Valójában milyen mértékben védhető? Elegendő önmagában?
 - vagy az átadás előtt az adathordozón levő adatot meg kell semmisíteni

A **technika** és az érintettek által **betartott folyamat** **együttesen** képes csak szavatolni.

Példa: webshop

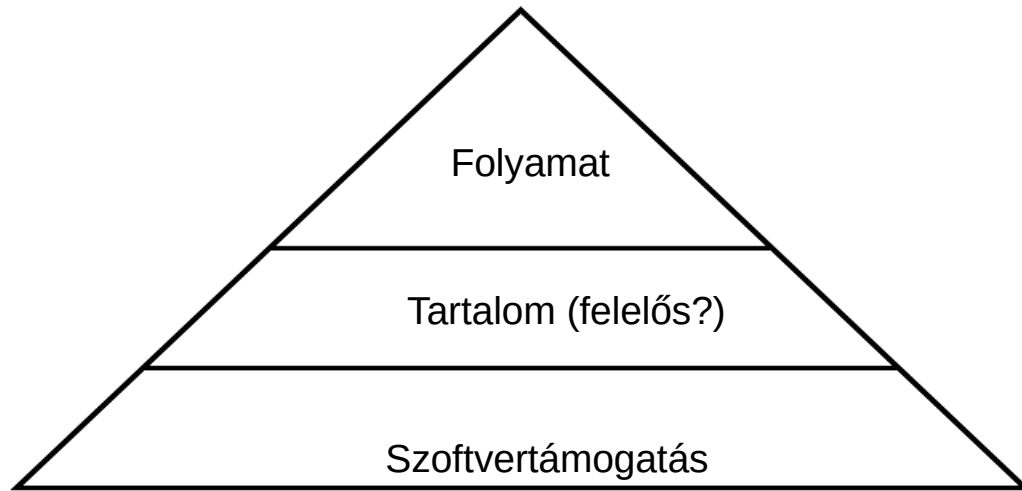
Folyamat:

1. Regisztráltunk egy webshopba
2. Később kérjük, hogy töröljék a személyes adatainkat
3. Visszaigazolják, hogy a rendszerből törölték a személyes adatainkat
4. Megnyugodhatunk, törölték.

Kérdés:

- Biztosak lehetünk-e abban, hogy később nem fogják más célra felhasználni?
- A „törölt” személyes adatnak tuti nem lesz utóélete, biztosan nem kerül később **3. félhez?**

Nézzünk a dolgok mögé



Szükséges adatkezelői tevékenységek:

- 1) Személyes adat felvétele
(tárolás, másolatok, adatfeldolgozók)
- 2) Személyes adat módosítása,
(a már nem szükséges adatmezők törlése)
(tárolás, másolatok, adatfeldolgozók)
- 3) Személyes adat felszámolása
(tárolás, másolatok, adatfeldolgozók)

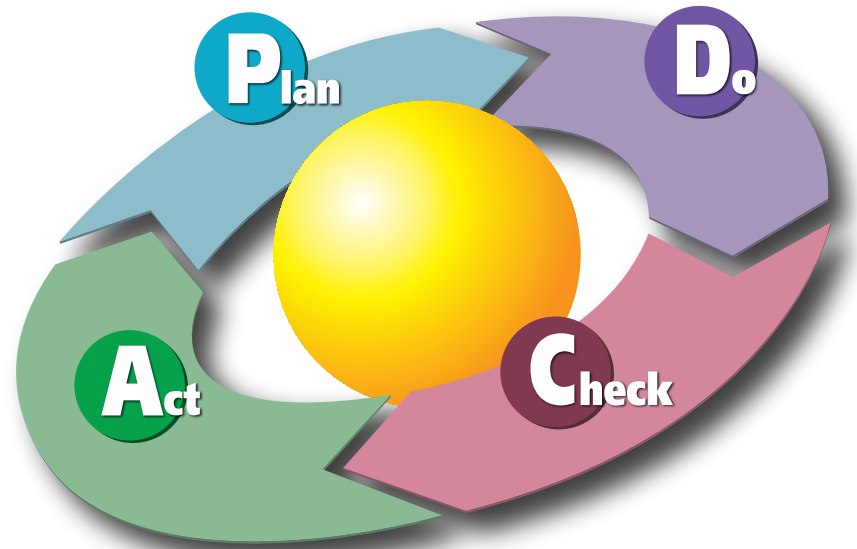
Szervezetnél alkalmazott adatkezelési folyamat (részletesen, előíró jelleggel):

- 1) Adatkezelési folyamat megtervezése (alapos, teljes életciklusra kiterjedő)
- 2) Bevezetés (oktatás)
- 3) Betartatás (**ellenőrzés**, kiegészítő oktatás)
- 4) Folyamat felülvizsgálata, módosítása

Amennyiben be van vonva adatfeldolgozó, akkor valójában arra is ki kell terjedni a folyamatnak.

Cég szabályozásban hihetünk?

- Amint látszik, valójában **nem technikai kérdés** az információ törlése
- Annál inkább a szervezet **szabályozási kérdése**
- Vajon hogy áll az adott szervezet
 - szabályozási folyamatokkal
 - betartásával
 - **vezetői elköteleződéssel**



A folyamat **mindig** be lesz tartva? **Amikor nem teljesül ...**

Tegyük fel, hogy a szándék megvan, de

- A) a folyamatban hiányosságok vannak
- B) a folyamat végrehajtásában hibák vannak.
- C) a folyamat nincs betartva
 - személy másban érdekelt
 - külső tényezők (incidens, időprés) hatására figyelmetlenség
- D) a vezető elköteleződése megvan, de lecserélik
 - más tényezők lesznek hangsúlyosabbak, a folyamatot megváltoztatja
- E) Incidens (informatikai, akár a tevékenység beszüntetése)

Nyitott kérdések

Kiadjuk a személyes adatainkat egy cégnek, mert anélkül nem érhető el részünkre a szolgáltatása.

- Van a cégnek egy publikált adatkezelési tájékoztatója, mert „kötelező” hogy legyen. Hihető?
- Elérhetőek lesznek-e a jövőben KKV-t segítő útmutatások, pl. folyamatszervezésről, mint segítség?
- Elérhető lesz a jövőben **adatkezelési folyamatokkal** kapcsolatos megfelelőségi tanúsítás, **audit jelentés**?
 - Enélkül jelenleg valóban mennyire bízhatunk az adott adatkezelő adatkezelési folyamataiban?
 - Adatkezelő által bevont adatfeldolgozóra ténylegesen kiterjed a megfelelő adatkezelési folyamat?
- Adatkezelő vagy adatfeldolgozó beszünteti a tevékenységét. Mi lesz az adathordozókkal, a személyes adattal?
 - Tevékenység felhagyásakor az ekkor esedékes megsemmisítési folyamatokat betartatja valaki?
 - Felszámolás esetén az adatvagyon megfelelő megsemmisítése a felszámoló részéről megvalósul-e?

A megfelelő személyes adat kezeléshez a személyes adat teljes életciklusát lefedő valós folyamatok szükségesek, amely folyamatnak ki kell terjednie az érintett szervezetek esetleges felszámolására is.

Köszönöm a figyelmet!