blancco technology group

12 LÉPÉSES AKCIÓTERV

Felkészülés az EU adatvédelmi rendeletének (EU GDPR) való megfelelésre **Határidő: 2018**

1 Belső audit megtervezése

Tervezzen meg és folytasson le egy belső auditot, mely számba veszi a szervezet által jelenleg kezelt összes adatot és adathordozót. Azonosítsa és analizálja mindazon sérülékenységeket, melyek veszélynek tehetik ki a szervezetet, és az EU új adatvédelmi szabályainak megsértéséhez vezethetnek.

2 Írott dokumentáció készítése

Készítsen egy részletes listát mindazon fizikai, virtuális és logikai helyekről, melyeken vállalati, valamint az ügyfelekre, a vevőkre, az alkalmazottakra, a beszállítókra és a partnerekre vonatkozó adatokat tárol. Az elkészült listát vitassa meg minden belső osztállyal és érintettel, majd tartsa naprakészen.

3 Vezessen be biztonságos adatmegsemmisítési eljárást

Az elektronikus és informatikai adathordozókról olyan minősített módon távolítsa el a szükségtelenné vált adatokat, amely megfelel az olyan a jogilag előírt felülírási szabványoknak, mint a HMG Infosec vagy a DoD 5220.22.M. Ellenőrizze, hogy az eljárást elfogadják-e a nemzetvédelmi hatóságok, és megfelel-e az olyan szervezetek előírásainak, mint a NATO, a CESG, a TUV SÜD vagy a DIPCOG.

4 Minden adattörlést igazoljon

Az ügyfelek és vevők, a jelenlegi és volt alkalmazottak, valamint a beszállítók és partnerek korábbi adatokkal kapcsolatos kérdéseire írásban kell válaszolnia. Ennek során fel kell tudni mutatnia fizikai bizonyítékot (jegyzőkönyvet) arról, hogy az érintett elavult vagy irrelevánssá vált adatait mikor és milyen módszerrel, milyen eredménnyel semmisítette meg.

5 Tájékoztassa az érintetteket

Az ügyfeleket rendszeresen és ismétlődő módon tájékoztatnia kell az adataik feldolgozásának módjáról. Írásban kell tájékoztatnia az ügyfeleket arról, hogy milyen módon vonhatják vissza az adataik kezeléséhez adott hozzájárulásukat. Ha az adatok feldolgozásának vagy kezelésének módjában változás történik, erről írásban kell tájékoztatnia az ügyfeleket.

6 Menedzselnie kell a mobileszközöket

Ha az alkalmazottak mobileszközöket használnak a munkájuk során (például BYOD program), készítsen szabályzatot arra, hogy mi történik az eszközökön tárolt adatokkal az eszköz eladásakor vagy a munkaviszony megszűnésekor. Biztosítsa, hogy külön terv készüljön a vállalat saját tulajdonában lévő eszközökre és az alkalmazottak tulajdonában lévő eszközökre.

7 Felelősen gyűjtse az adatokat

Készítsen útmutatást arra, hogy milyen típusú és szintű profilozást (adatgyűjtést) végez a szervezete.

8 Segítse az együttműködést a részlegek között

Működjön együtt a szervezet más részlegeivel a cég minden szintjén, hogy támogatni tudja az egyedi adatgyűjtési, adattárolási és adatmegsemmisítési üzleti igényeiket és céljaikat.

9 Szervezzen oktatást és tréningeket

Készítse el a megfelelő oktatási anyagokat az alkalmazottak számára a teljes szervezetben, melyek leírják a különböző adatvesztési forgatókönyveket és okokat, az adatok védelmére és integritásának monitorozására vonatkozó legjobb gyakorlatokat, valamint az adatok megsemmisítésének helyes (és helytelen) módjait. Juttassa el ezeket az anyagokat minden munkavállaló számára, tekintet nélkül beosztásukra és munkakörükre.

10 Nevezzen ki adatvédelmi felelőst

Egy belső embert nevezzen ki adatvédelmi felelősnek. Ennek a személynek a feladatai közé tartozik, hogy implementálja az adatkezelésre vonatkozó szabályozásokat, az informatikai és adathordozó eszközök menedzsmentjét megvalósítsa azok teljes életútján keresztül, beleértve a leselejtezés folyamatát is. Az adatvédelmi felelős feladatai közé tartozik az is, hogy naprakész maradjon az EU- és a nemzeti adatvédelmi szabályozások és ajánlások változásaival kapcsolatban.

11 Monitorozza a kockázatkezelést

Készítsen átfogó kockázatkezelési tervet, mely kiterjed az adatok kezelésének módjára azok keletkezésétől kezdve a tárolásukig és eltávolításukig az adathordozók adatoktól való fertőtlenítésének módjáig. A kockázatkezelési tervnek ki kell terjednie az olyan harmadik szervezetekre is, mint a beszállítók és a partnerek.

12 Készítsen incidenskezelési tervet

Foglaljon írásba egy incidenskezelési tervet, melyre a szervezet egy adatvédelmi incidens esetén a válaszreakcióit alapozza. A tervnek tartalmaznia kell az érintetteknek küldött mintaüzeneteket, a sajtónak küldött mintaüzeneteket, a maximális válaszidőt, az elvárt határidőket, az érintettek listáját, és a kríziskezeléssel megbízott csapat tagjainak szerepeit és feladatkörét.

A Blancco lehetővé teszi, hogy az adatokat jegyzőkönyvezett módon, minősített eljárás okkal törölje minden adathordozóról, az USB kulcsoktól és memóriakártyáktól kezdve a számítógépeken, SSD meghajtókon és mobiltelefonokon, táblagépeken keresztül egészen a szerverekig, adatközpontokig, VMware, Hyper-V és más virtuális környezetekig.

Az adatok eltávolítására és megsemmisítésére, valamint az adathordozók leselejtezésre való proaktív felkészülés segíti a közigazgatási szervezeteket és a vállalatokat abban, hogy megfeleljenek az EU adatvédelmi szabályainak és biztosítani tudják a feledéshez való jogot („right to be forgotten”). Emellett csökkentik a szervezet ellen indított hatósági eljárás valószínűségét és az esetlegesen kiszabott büntetések mértékét.

Bővebb információ: http://torles.hu