Milyen adatbiztonsági intézkedéseket vár el a GDPR az adatkezelőktől?

GDPR már az alapelvek között is kiemeli az **"integritás és bizalmi jelleg" elvét**, amely azt az általános elvárást támasztja, hogy a személyes adatok

kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve

A Rendelet több helyen is világossá teszi, hogy az elvárás az adatkezelők felé, hogy a megfelelő technikai és szervezési intézkedéseket **a változó valószínűségű és súlyosságú kockázat figyelembevételével alakítsák ki.**

A DPC (ír adatvédelmi hatóság) az alábbi konkrét intézkedéseket ismerteti az útmutatójában:

a. **Adatok gyűjtésére és megőrzésére vonatkozó szabályozás:** Az adatok elvesztéséhez vagy ellopásához fűződő kockázatok csökkentésének legnyilvánvalóbb és leghatékonyabb eszköze nyilvánvalóan az, ha az adatok nem kerülnek kezelésére. Ez a gyakorlatban azt jelenti, hogy az adatok kezelésének mindig igazodnia kell az adatkezelés céljához és a szükséges minimumra kell szorítkoznia (lásd célhoz kötöttség, adattakarékosság, korlátozott tárolhatóság elvei). Fontos, hogy az adatkezelők tisztában legyenek azzal, hogy milyen adatokat, milyen célból kezelnek és azokra meddig van ténylegesen szükség a cél elérése érdekében.
b. **Hozzáférések szabályozása:** Szükséges biztosítani, hogy csak az férhessen hozzá az adatokhoz, akinek a feladatihoz ez szükséges ("*need to know*" elv). A hozzáféréseket időről-időre felül kell vizsgálni. A hozzáféréseknek célszerű személyre szólónak lennie (kerülve az azonos csoport által ugyanazon felhasználónév+jelszó páros használatát). Az adatok érzékenysége is meghatározó jelentőségű, amikor a hozzáférésekkel kapcsolatos részletszabályok kialakításra kerülnek (pl. egyes esetekben több faktoros azonosítás is indokolt lehet). Külön figyelmet kell fordítani az IT adminisztrátori hozzáférésekre, amelyek jellemzően széleskörű jogosultságot jelentenek. Olyan esetekben, amikor a rendszerből az adatok le is tölthetők, indokolt további intézkedéseket is megtenni, illetve adott esetben a letöltések technikai blokkolása is indokolt lehet. (Az ír hatóság anyaga további nagyon hasznos útmutatást ad a megfelelő jelszó kiosztási szabályok meghatározására és a jelszavak kezelésére vonatkozóan is.)
c. **Automatikus képernyővédők:** Alkalmasak annak biztosításra, hogy a felügyelet nélkül maradt eszközökhöz ne történhessen ellenőrzés nélküli hozzáférés.
d. **Titkosítás:** Az adatok biztonságos tárolásának eszköze. Különösen fontos lehet az alkalmazása például hordozható eszközökön vagy nyilvános hálózatokon keresztül történő adattovábbítás esetén. A technológiai fejlődésre tekintettel a titkosítási sztenderdek is folyamatosan változhatnak, így rendszeres felülvizsgálatra szorul az adatkezelők részéről az

alkalmazott titkosítási technológia. A DPC véleménye szerint jelenleg az adathordozó 256 bites titkosítással történő védelme megfelelőnek minősülhet.

e. **Anti-vírus szoftver alkalmazása:** A megfelelő szoftver telepítése mellett a rendszeres frissítés is kiemelten fontos, illetve a megfelelő belső szabályozás és a tudatosság növelése is (pl. a gyanús csatolmányok megnyitásának mellőzése).
f. **Tűzfalak:** Amennyiben a hálózatnak vannak külső kapcsolatai (akár más hálózatok, akár az internet irányába), akkor a tűzfalak alkalmazása is elengedhetetlen, megfelelő konfigurálás mellett.
g. **Szoftverek frissítése:** Az adatkezelőnek gondoskodnia kell arról, hogy az általa alkalmazott szoftverek megfelelően frissítésre kerüljenek, hiszen az újabb verziók olyan javításokat tartalmazhatnak, amelyek pl. külső támadások megelőzését is szolgálhatják.
h. **Távoli hozzáférés:** A távoli hozzáférések potenciális kockázatot jelenthetnek a rendszerre nézve, így azok biztosítása fokozott körültekintést és további biztonsági intézkedések bevezetését teheti szükségessé.
i. **Vezeték nélküli hálózatok:** Az ismeretlen, nem megbízható hálózatokra történő csatlakozást lehetőség szerint kerülni kell, illetve megfelelő szabályok szükségesek a használatára. Ezen túlmenően technikai biztonsági intézkedések is szükségesek (pl. megfelelő titkosítás alkalmazása).
j. **Hordozható eszközök:** Amennyiben a hordozható eszközökön (pl. USB, laptop, telefon, stb.) személyes adatok tárolása történik, akkor szükséges megfelelő titkosítás alkalmazása. A belépéshez pedig megfelelő erősségű jelszó megadását kell megkövetelni. A távoli törlés lehetősége alkalmas a kockázatok csökkentésére.
k. **Logolás és audit:** A hozzáférések logolása és a hozzáférések megfelelő ellenőrzése mellett behatolást jelző rendszerek alkalmazása is fontos biztonsági intézkedés lehet.
l. **Mentések készítése:** Mentések készítése esetén nem szabad megfeledkezni arról, hogy a mentésben lévő adatokat ugyanolyan magas szinten kell védeni, mint az éles rendszerben lévő adatokat.
m. **Incidenskezelés:** A legjobb biztonsági intézkedések mellett is előfordulhatnak incidensek. Az adatkezelőknek előzetesen rendelkezniük kell az incidensek kezelésére vonatkozó szabályozással és mechanizmusokkal, hogy időben és hatékonyan tudjanak reagálni az esetlegesen bekövetkező incidensre.
n. **Használt eszközök lecserélése:** A lecserélésre szánt eszközök esetében gondoskodni kell az adatok törléséről. Ez a kötelezettség mindenféle eszközre vonatkozik, azaz mindig érdemes vizsgálni, hogy az adott eszköz tartalmazhat-e személyes adatot. Egy egyszerű törlés vagy formázás azonban nem elég, hiszen abból visszaállíthatók lehetnek az adatok. Olyan szoftveres megoldást kell alkalmazni, amely ennek a lehetőségét kizárja. (Korábban a NAIH ugyanezt az elvárást támasztotta egy állásfoglalásában: "*A fenti jogszabályhely alapján az adatkezelőnek olyan módon kell törölnie az érintett személyes adatát, hogy annak helyreállítása a továbbiakban ne legyen lehetséges. A fentiekre tekintettel nem elegendő a merevlemezek, illetve más informatikai adathordozók „egyszerű formázása". A beadványban említett ingyenes szoftver (DBAN) vagy bármely más „HDD wipe" jellegű szoftver is megfelelhet ennek a célnak.*") Egyes esetekben törlés helyett a fizikai megsemmisítés is szóba jöhet.
o. **Fizikai biztonság:** A technológiai biztonsági intézkedések mellett a megfelelő fizikai biztonsági intézkedések meglétét is garantálni kell (pl. riasztó berendezés, beléptető rendszer, szervertermek védelme monitorok megfelelő elhelyezése, stb.).
p. **Emberi tényező:** A védelmi intézkedések kapcsán gyakran az emberi tényező hordozza a legnagyobb kockázatot. Erre tekintettel a tudatosítás, az oktatás, a szabályok megtartásának rendszeres ellenőrzése kulcsfontosságú az adatok biztonságának megóvása érdekben.

q. **Tanúsítványok**
Minden esetben mérlegelni kell, hogy mely intézkedések lehetnek alkalmasak a kezelt adatok biztonságának garantálásához. A fentiek ebben nyújthatnak segítséget, de természetesen számos más intézkedés is szükséges lehet az adatkezelés jellegétől függően.

Miért kiemelten fontos a megfelelő adatbiztonság garantálása?

Az adatok megfelelő biztonságának garantálása elengedhetetlen **az adatkezeléssel kapcsolatos bizalom megteremtése és megőrzése érdekében**. Emellett hozzájárulhat az incidensek megelőzéséhez, illetve incidens bekövetkezése esetén annak hatásait is jelentősen csökkentheti vagy a további kockázatok megelőzéséhez is hozzájárulhat (pl. elveszett telefon, illetve laptop távoli törlésének lehetősége).