KÖZPONTI STATISZTIKAI HIVATAL

A Központi Statisztikai Hivatal információbiztonsági politikája

A Központi Statisztikai Hivatal (továbbiakban: KSH) Magyarország egyik legjelentősebb hivatalosstatisztikaiadat-vagyonával rendelkezik, tevékenységéből eredően kiemelt fontosságúnak tekinti az adatok és az informatikai rendszerek védelmét, amelyet információbiztonsági alapelvek szerint működő, a biztonsági besorolásoknak megfelelő, védett működési környezetben és elektronikus információs rendszerekben lát el.

A KSH az az alább közzétett információbiztonsági politikájában az európai statisztikákról szóló európai parlamenti és tanácsi rendelettel,[1] az Európai és Nemzeti Statisztika Gyakorlati Kódexének elveivel, az Európai Unió Általános Adatvédelmi Rendeletével,[2] az információs önrendelkezési jogról és az információszabadságról szóló törvénnyel,[3] a hivatalos statisztikáról szóló törvénnyel[4] és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvénnyel[5] összhangban fogalmazza meg információbiztonsági alapelveit

A KSH az informatikai biztonság területén az alábbi alapelveket érvényesíti:

1. **Bizalmasság**: az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
2. **Sértetlenség**: a tárolt adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), a származás ellenőrizhető, megállapítható (letagadhatatlanság), illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
3. **Rendelkezésre állás**: az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók.
4. **A védelem teljeskörűsége:** az erre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:
    a) az összes rendszerelemre;
    b) a rendszerek architektúrájának összes rétegére mind az informatikai infrastruktúra, mind az alkalmazások szintjén;
    c) a központi,illetve a végponti informatikai eszközökre és környezetükre.
5. **A védelem zártsága:** az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedés végrehajtása megtörténik, és azok összességükben szabályozott és szerves egészet alkotnak.

[1] 223/2009/EK európai parlamenti és tanácsi rendelet az európai statisztikákról
[2] 2016/679 (EU) európai parlament és tanács rendelete
[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
[4] 2016. évi CLV. törvény a hivatalos statisztikáról
[5] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

6. **A védelem kockázatarányossága:** a védelem mértéke és költségei a felmért kockázatokkal arányosak. Cél a szükséges és elégséges védelmi költséggel elért maximális védelmi képesség.
7. **A védelem folyamatossága:** a kialakított védelmi intézkedések az időben állandóan változó biztonsági környezet és viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

A hivatal az alapelvek figyelembe vételével tervezte meg, alakította ki, működteti és fejleszti információbiztonsági irányítási rendszerét, annak érdekében, hogy a kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszerek elemeinek sértetlenségét és rendelkezésre állását veszélyeztető mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek teljes életciklusára kiterjedő védelmét biztosítsa logikai, fizikai és adminisztratív védelmi intézkedések bevezetésével.

A KSH vezetése elkötelezett, kiemelten fontos feladatnak tartja a KSH elektronikus információs rendszerei és a bennük tárolt adatok védelmét, és elkötelezi magát arra, hogy folyamatosan biztosítsa a kor technológiai szintjének megfelelő informatikai biztonsági védelmi intézkedések megtételéhez szükséges erőforrásokat. A hivatal ellenőrző folyamatok kialakításával, rendszeres kontrolltevékenységekkel és az információbiztonság folyamatokba integrálásával fejleszti a biztonsági szintet.

A KSH vezetése elkötelezett aziránt, hogy az adatkezelésre vonatkozó elvárások meghatározása az információbiztonsági alapelveknek megfelelően történjen, illetve az elvárásoknak megfelelően korszerű és biztonságos adatkezelés valósuljon meg. A hivatal messzemenően figyelembe veszi az adatok minőségére, bizalmasságára, az adatátadások rendszerességére és az adatbiztonságra vonatkozó elvárásokat, az elvárások teljesítéséhez védelmi intézkedéseket vezet be, a szükséges erőforrásokat biztosítja.

A KSH vezetése, minden munkatársa és szerződéses partnere felelős a kezelésükre bízott adatokra vonatkozó információbiztonsági alapelvek, elvárások betartásáért, az alapelvekről, elvárásokról rendszeresen oktatott és az elvárásoknak, alapelveknek megfelelően védi a kezelt adatokat.

Budapest, 2019. március 1.

Dr. Vukovich Gabriella
a KSH elnöke