



Az
“adatvédelmi felelős”
és az
“információbiztonsági vezető”
(megbízott, felelős...)
funkciók közötti különbségek



Bevezetés

A társadalmi létben

- az együttélés megkönnyítésére -

szabályokat alkotunk.

A szabályok között találjuk meg a

törvényeket és a szabványokat is.

Mindkettőre igaz, hogy jó lenne, ha pontosan és szabatosan fogalmazna.



A belső adatvédelmi felelős és az ő problémái

A baj akkor kezdődik, amikor a törvények csak általános elvárásokat fogalmaznak meg.

Az 1992. évi LXIII. törvény (a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról) a jobb törvények közül van.

Világos a törvényalkotó szándéka, az átadni szándékozott gondolat. A továbbiakban részletezi azokat a követelményeket, elvárásokat amelyek teljesülése szükséges a célhoz való eljutáshoz, meghatározza, hogy milyen "szervezetben" és milyen feladatokkal gondolja velünk végrehajtani ezeket a követelményeket, de ez is igényli a magyarázatot, értelmezést,

hogy értelmet lehessen csempészni a végrehajtásba.



A rendszer felépítése

Adatvédelmi biztos

Az Országgyűlés adatvédelmi biztost választ, aki hivatalból ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok megtartását.

Adatvédelmi nyilvántartás

A személyes adatokat kezelő adatkezelő köteles e tevékenysége megkezdése előtt az adatvédelmi biztosnak nyilvántartásba vétel végett bejelenteni

- az adatkezelés célját;
- az adatok fajtáját és kezelésük jogalapját;
- az érintettek körét;
- az adatok forrását;
- a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját;
- az egyes adatfajták törlési határidejét;
- az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;
- a belső adatvédelmi felelős nevét és elérhetőségi adatait.



A rendszer felépítése

Belső adatvédelmi felelős

Az adatkezelő, illetőleg az adatfeldolgozó szervezetén belül, közvetlenül a szerv vezetőjének felügyelete alá tartozó - jogi, közigazgatási, számítástechnikai vagy ezeknek megfelelő, felsőfokú végzettséggel rendelkező - belső adatvédelmi felelőst kell kinevezni vagy megbízni:

- közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
- kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;
- vezeti a belső adatvédelmi nyilvántartást;
- gondoskodik az adatvédelmi ismeretek oktatásáról.



A rendszer felépítése

Adatbiztonság

10. § (1) Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
- (2) Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.



Összegezve. A belső adatvédelmi felelős feladata:

- Fő feladata a törvényesség feletti őrködés.
- Az adatvédelmi nyilvántartása alapján alakítsa ki a saját rendszerét, ahol a törvény csak annyira engedi meg az eltérést, hogy a saját szervezete speciális vonásai érvényesüljenek.

(Tulajdonképpen a törvény által "megfoghatóan előírt" feladatok végrehajtása.)

- Adatbiztonság címszó alatt kap olyan feladatokat, amelyeket a törvény is csak homályosan fogalmaz meg (10. § (1)), és (a 2. bekezdésben is csak) legfeljebb orientál, hogy ezeket a feladatokat mely területeken és hogyan lehetne végrehajtani.

(Ráadásul, egyik szakmai területen sincs otthon, és intézkedési jogosultságot sem biztosít számára a törvény.)

- Adatvédelmi és adatbiztonsági szabályzatot kell készítenie, amelynek sem a tartalmáról, sem a formájáról nem rendelkezik a törvény.

(Nézőpont kérdése, hogy miért ez a legnehezebb feladata. Azért, mert a törvény nem nyújt az elkészítéshez semmi támpontot, vagy azért, mert ez a feladat teljesen önálló gondolkodást igényel.)



Az információbiztonsági vezető (megbízott, felelős...)

Azon szervezeteknél, ahol szükséges a belső adatvédelmi felelős poszt, ott "erősen ajánlott" az MSZ ISO/IEC 27001:2006 (információbiztonsági) rendszer kiépítése.

Az adatvédelmi törvény és az információbiztonsági szabvány meglehetősen hasonló tématerületet fed le, de a feladatuk, megvalósításuk, lehetőségeik nagyon eltérőek.

Az információbiztonsági szabvány konkrétan meghatározza a kereteket (az információbiztonsági rendszer kereteit), de a keret megtöltését értelmes tartalommal a szervezetre bízta.

A személyek tekintetében irányelveket mutat, de nem határozza meg, hogy pl. kell lennie a szervezetnél információbiztonsági vezetőnek (megbízottnak, felelősnek, stb.).

Az elnevezés és a feladat-, jogkör "áthagyományozódott" a minőségirányításból.

(ISO 9001 - A felső vezetőségnek ki kell jelölnie a szervezet vezetőségének egy tagját, akinek egyéb felelősségi körétől függetlenül olyan felelősségi körrel és hatáskörrel kell rendelkeznie...)



Az információbiztonsági vezető (megbízott, felelős...)

Továbbá csak meghatározza a követelményeket, elvárásokat, de nem mondja meg az oda vezető utat.

És ez jó! Vagy rossz! (Ez mindig csak nézőpont kérdése.)

Jó, mert lehetőséget hagy arra, hogy az információbiztonsági rendszer mindig a legoptimálisabban személyre szabott lehessen.

Rossz, mert nem "erősíti" sablon megoldások átvételét más szervezetektől. (Gondolkodásra kényszerít.)

Jelenleg a nálunk tanúsított információbiztonsági rendszerek kb. 90 %-a (szigorúbban nézve 99 %-a) mechanikusan, sablonok alapján kiépített rendszer, legfeljebb a sablont próbáljuk meg többé-kevésbé a szervezetre szabni.

Nem lehet mondani, hogy teljesen alkalmatlanok a feladatukra - hiszen tanúsítottak -, de a hatékonyságuk erősen megkérdőjelezhető.

Más kérdés, hogy még cégvezetőt nem hallottunk panaszkodni, hogy drága pénzen fenntartanak egy kétséges hatékonyságú rendszert. Nincs is viszonyítási lehetősége (azaz, azt hiszi, hogy olyannak kell lenni) és ha tudja, hogy nem jó, akkor sem dicsekszik vele.



Az információbiztonsági vezető (megbízott, felelős...)

A sablonok alkalmazásából adódó **hibák** (a nem lelkiismeretes, vagy nem hozzáértő felkészítői, illetve tanúsítói tevékenység eredménye jobbra) **gyorsan kijavíthatók** lennének, ha nem a már említett ISO 9001-ből vennénk át bizonyos sémákat. Ilyen pl. az információbiztonsági vezető helye, szerepe a rendszerben.

A minőségirányítási rendszer menedzsment rendszer. A menedzsment elemeket mindenki ismeri – mert vagy vezető, vagy vezetett. A helyes sorrendű egymáshoz illesztésüktől függ a rendszer hatékonysága és ezt egy ember – a minőségirányítási vezető – át tudja látni.

Az információbiztonság kereteiben felvetődő problémák (akár a kockázatértékelés, akár a védelmi szabályok kérdéseit nézzük) megoldásához **több "szakterület" tudása és azok összehangoltsága** szükséges.



Az információbiztonság gyakorlati területei:

- ★ **objektum, terület védelem,**
- ★ **személy védelem** (rendszerben a személy védelme, vagy a rendszer védelme személyektől),
- ★ **"hagyományos" adatok, módszerek, eszközök védelme** (elsősorban a papíralapúak),
- ★ **informatikai védelem,**
- ★ **katasztrófák** (elemi károk, természeti csapások, társadalmi konfliktusok) **elleni védelem.**

Látszik, hogy a területek megnevezései "csak" **gyűjtőfogalmak**, azaz további önálló területekre oszthatók.

Továbbá látszik, hogy az egyik szakmaterületen bevezetett védelmi intézkedésnek áthúzódó hatása lesz más szakmaterületekre, azaz **a rendszer hatékonyabbá válik**, illetve olcsóbbá.



Az információbiztonsági vezető (megbízott, felelős...)

És az is látszik, hogy még nem született meg az az információbiztonsági vezető, aki egy személyben birtokolná az összes szakmaterület szükséges tudását.

Mentalitást kell váltani az ISO 9001-hez képest, ahol a minőségirányítási vezető mindent tud, ő a "legokosabb".

Az információbiztonsági rendszerben a vezető "csak" a kérdést, követelményt tudja megfogalmazni, illetve a szakterületek megoldási javaslatait (egymással is összehangolva) koordinálni.

(Egyébként az MSZ ISO/IEC 27001:2006 is így rendelkezik, csak "bújtatva":

"Az információbiztonsági tevékenységeket a szervezet különböző részeitől delegált és megfelelő feladat- és munkaköri funkciókkal felruházott képviselők révén kell koordinálni."

(A6.1.2.)



Összegezve. Az információbiztonsági vezető feladata:

- A szabvány szigorúan meghatározott keretei között, de nagyfokú önállóságot, kreativitást feltételezve szervezze a rendszert.
- Koordinálja a védelembe bevont szakmaterületek munkáját.
- Ellenőrizze, elemezze, stb. a megvalósított védelem gyakorlati hatékonyságát.



A két funkció együttműködésének lehetőségei

A gyakorlatban sokszor előfordul, hogy a belső adatvédelmi felelős és az információbiztonsági vezető **egymás riválisai**. Adódik abból, hogy hasonlóak a működési területeik, de nem tisztázták, vagy inkább **nem megértették a feladataik**, lehetőségeik.

Valójában pedig az lenne az **elvárás** (és az érdekük is), **hogy szorosan együttműködjenek**, mivel nagyon jól kiegészítik egymást még a "hiányosságaikban" is.

- A **belső adatvédelmi felelős** egy meghatározott törvényesség őre, de a törvény által is csak homályosan megfogalmazott gyakorlati adatbiztonsági feladatok megvalósításához sem szakmai hozzáértéssel nem rendelkezik, sem jogosultsággal (legalábbis a törvény alapján).
- Az **információbiztonsági vezető** a kérdéskörbe tartozó védelmi problémák megoldásához rendelkezik jogosultsággal, (a koordináción keresztül) szakmai háttérrel és lehetőséggel. Az ő "hiányossága" rendszerint a biztonsági kérdések felvetésében a legnagyobb.

Világ adatvédelmi felelősei és információbiztonsági vezetői, működjetek együtt!



Köszönöm megtisztelő figyelmüket!

Oláh Tamás
(30) 9797937
olaht@infobiz.hu