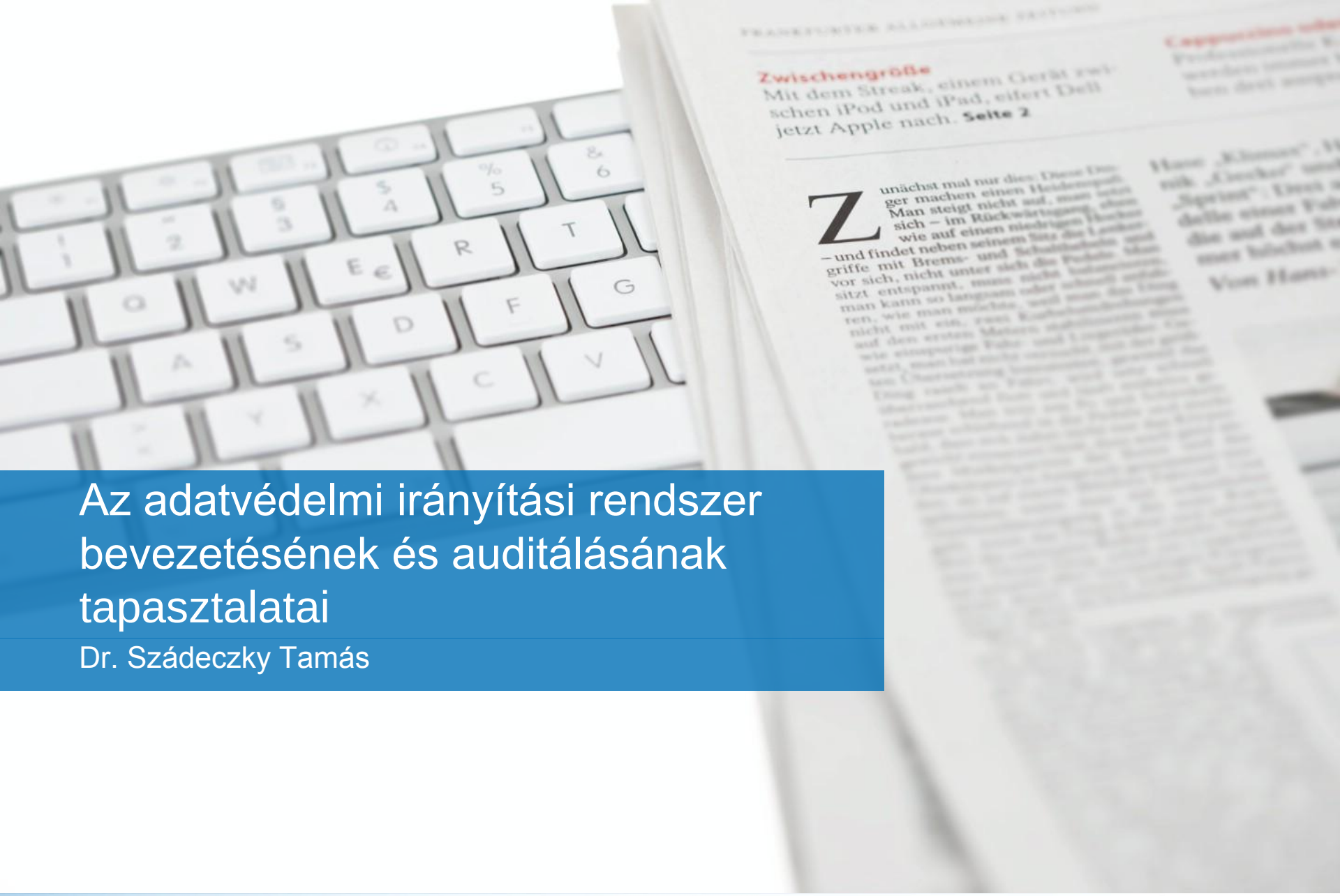

Az adatvédelmi irányítási rendszer bevezetésének és auditálásának tapasztalatai

Dr. Szádeczky Tamás

Irányítási rendszerek

„ISO” megközelítés

- Irányítási rendszer
  - Rendszer politika és célok megfogalmazásához, valamint célok eléréséhez
- Minőségirányítási rendszer [ISO 9000]
  - Irányítási rendszer egy szervezet vezetésére és szabályozására, a minőség szempontjából [ISO 9000]
- Adatvédelmi irányítási rendszer
  - Irányítási rendszer egy szervezet vezetésére és szabályozására, a személyesadat-védelem szempontjából
  - Fogalmilag nem tér el jelentősen a többi irányítási rendszertől, de
    - Jogi követelmények vonatkoznak a területre
    - Nincs olyan absztrakt követelményrendszere, mint egy szabványos rendszernek
    - Nem menedzsmentközpontú a követelményrendszer és nem is gyakorlatias
  - Piaci igény a követelmények pontosabb meghatározása
    - Erre alapvetően alkalmas az ISO megközelítés

Adatbiztonság formalizálása

A kulcs az ISO 27001

- CoC 8. Security aspects
  - 8.1 Employers shall ensure the security of the processing of data relating to the monitoring of employees.
  - 8.2 Information security management system of the employer shall cover all aspects of data processing that relates to the monitoring of employees.
- Általános előírások
  - Szükséges a mögöttes műszaki tartalmat meghatározni
  - Célszerűen valamely nemzetközi szabvány követendő: COBIT, ISO 27001
  - ISO 27001 IBIR szabvány tanúsítható, a tanúsítvány felhasználható a megfelelés bizonyítására

Tanúsítás, audit követelmények

Szabványok segítségül hívása

- Irányítási rendszerek tanúsítása
  - ISO/IEC 17021:2011 kiválasztott követelményei
  - Pártatlanság, függetlenség követelménye, összeférhetetlenség
  - Auditorokra vonatkozó követelmények
  - Audit és tanúsítás folyamatára vonatkozó követelmények
- Adatbiztonsági követelmények
  - ISO/IEC 27001:2005 kiválasztott követelményei
  - ISO/IEC 27006:2011 módszertani előírásai, auditkövetelmények
- A TÜV Rheinland akkreditált tanúsító, felkészült auditorokkal
  - Jelentős know-how az irányítási rendszerek területén
  - Létező adatvédelmi tanúsítási rendszer (minden adatkezelésre)
- Az adatvédelem nem irányítási rendszer, de a létező követelmények alkalmazhatók rá, növelik az egységességet
- Ez a tanúsítási rendszer nem akkreditálható

Az akkreditációs logók nem a jelen szolgáltatás akkreditált voltát jelzik, hanem a TÜV Rheinland irányítási rendszer szabványokra akkreditált voltát illusztrálják.

Tanácsadási tapasztalatok

Új típusú problémakör

- Az adatvédelmi jogi és az információbiztonsági kompetenciák jól kiegészítik egymást
  - A két problémakör más megközelítést igényel
- Nagyon fontos a hatókör pontos meghatározása
  - Konkrét adatkezelések szintjéig
    - Pl. elektronikus levelezés és központi nyomtatás
  - Ezeket az adatkezeléseket részletesen elemezni szükséges
  - Információbiztonság mindig túlmutat az adott rendszeren
    - Elektronikus levelezés szerverének karbantartása, hozzáférések kiosztása, stb.
- Az ISO 27001 beszámítható, de nem kötelező
  - Ha a meglévő tanúsítvány hatókörében benne van a vizsgált adatvédelmi hatókör, akkor nem kell vizsgálni a megfelelőséget
  - Viszont nem kell kiépíteni a rendszert, ezért külön dokumentációt nem igényel a megfelelés

Tanácsadási tapasztalatok

Fájdalommentes megfelelés

- Hosszabb idő alatt, mélységében
  - Igény esetén a rendszer teljes átvizsgálásával
  - Részletes javaslatokkal, szabályzatokkal, mindig rendelkezésre álló tanácsadókkal

- Rövid idő alatt, hatékonyan
  - Felgyorsult világunkban szükséges lehet a gyors megfelelés kialakítása
  - Pareto-elv alkalmazása a tanácsadásban
    - A következmények 80%-a az okok mindössze 20%-ára vezethető vissza
  - Ez jelentősen csökkenti a költségeket is, bár nagyobb valószínűséggel marad nem-megfelelőség
  - Elavult szabályozáson, becsontosodott hibás gyakorlaton sokat tud segíteni

- Elérhető előnyök
  - Kisebb a kockázata a hatósági bírságnak (akár 10 MFt)
  - Kisebb az akár nem szándékos visszaélés valószínűsége

Köszönöm a figyelmüket!

tamas.szadeczky@hu.tuv.com