„Papír helyett működés”

Élő adatvédelmi és kiberbiztonsági rendszer építése, a megfelelés új korszaka

Dr. Amigya Andrea Ll.M.

ARB PRIVACY CONSULTING

Papír helyett működés avagy

Élő adatvédelmi és kiberbiztonsági rendszer építése a megfelelés új korszaka

Dokumentáció helyett ellenállóképesség

Miért nem a papír mennyisége a döntő, miért csúszik szét a dokumentáció és a gyakorlat, és hogyan lehet ezt mérésekkel, szimulációkkal és kontrollalapú működéssel helyrehozni?

A kérdés

Van papír - de működik-e?

A fordulat

Policy helyett kontroll + bizonyíték

A cél

Mérhető, tesztelt, ellenálló szervezet

ARB PRIVACY CONSULTING

1. Az alapállítás

A dokumentum a kontroll leírása.
A megfelelés viszont a kontroll működése.

- Lehet 120 szabályzat, és mégis lehet működésképtelen incidenskezelés.
- Lehet kiváló tájékoztató, de gyenge érintetti jogkezelés.
- Lehet audit-ready mappa, de nincs működő döntési lánc stresszhelyzetben.

Mit nézzünk valójában?

- Működik-e a kontroll a valós folyamatban?
- Van-e felelőse és bizonyítéka?
- Mérhető-e a teljesítménye?
- Stresszhelyzetben is működik-e?
- Tanul-e a rendszer az eltérésekből?

ARB PRIVACY CONSULTING

2. Miért kap túl nagy figyelmet a papír?

A dokumentáció látványos és gyorsan elkészültnek tűnik.

A működés nehezebben bizonyítható: mérni, tesztelni, gyakorolni kell.

A szabályzat projektesíthető, a működtetés folyamatos vezetői feladat.

A szervezet a kézzelfogható outputot szereti: van policy, van lista, van auditcsomag.

A valódi okok

- pszichológiai kényelem
- auditlogika és beszállítói elvárások
- széttöredezett felelősség
- kevés kontroll-KPI
- alacsony hibabiztonságú kultúra

ARB PRIVACY CONSULTING

3. A legnagyobb vakfolt: a papír és a valóság közötti rés

Tipikus tünetek

- Az adatkezelési nyilvántartás nem fedi le a tényleges rendszereket.
- Van incidenskezelési eljárás, de nincs gyakorolt döntési rend.
- Van hozzáférés-kezelési policy, de nincs rendszeres felülvizsgálat.
- A tájékoztató és a valós adatáramlás eltér egymástól.
- A beszállítói szabály megvan, de a felülvizsgálat elmarad.

Következmény

A szervezet azt hiszi, hogy megfelel, mert a dokumentáció rendezett.

Valójában viszont a kontrollok működése, a döntési lánc, az evidenciák és a reagálási képesség nincsenek egyben.

A legdrágább hiba: amikor a papír megnyugtat, de a működés nem véd.

ARB PRIVACY CONSULTING

4. Mi lehet ennek az oka?

Szervezeti okok
- széttöredezett felelősség
- külön működő jog, IT, biztonság, HR, üzlet

Kulturális okok
- a megfelelés külső teher
- kevés tanulás hibákból és incidensekből

Vezetői okok
- státusz van, kontroll-KPI nincs
- nincs egységes kontrollgazda

Technológiai okok
- sok manuális lépés
- hiányzó naplózás és evidence-gyűjtés

ARB PRIVACY CONSULTING

A dokumentáció és a működés szétcsúszása nem egyetlen hiba, hanem szervezeti tervezési probléma.

5. Mit jelent az élő megfelelési rendszer?

Naprakész
nem évente egyszer néznek rá

Működésbe épített
nem külön compliance-sziget

Mérhető
vannak kontroll-KPI-ok és KRI-ok

Tesztelt
nemcsak leírt, hanem gyakorolt

Bizonyítható
van napló, döntési lánc és audit trail

Tanuló rendszer
incidensekből és eltérésekből fejlődik

ARB PRIVACY CONSULTING

Élő megfelelés = operatív kontrollrendszer + visszamérés + folyamatos korrekció

6. A megoldás: papírközpontúból kontrollközpontú működés

1	**Kontrolltérkép**	kötelezettség - kontroll - felelős - evidencia - gyakoriság
2	**Policy to process**	minden szabályozás mögött legyen konkrét folyamat és szerepkör
3	**Process to evidence**	ne az legyen a kérdés, van-e szabályzat, hanem az, mi bizonyítja a működést
4	**Vezetői dashboard**	a board kockázati képet lásson, ne csak státuszt
5	**Rendszeres tesztelés**	tabletop, breach drill, helyreállítási és DSR-próba

ARB PRIVACY CONSULTING

7. Mit kell mérni?

Adatvédelmi mérőszámok

- érintetti kérelmek válaszideje
- határidőn túli ügyek aránya
- ROPÁ / nyilvántartás frissítettsége
- DPIA-felülvizsgálatok aránya
- incidens felismerési és eszkalációs idő

Kiberbiztonsági mérőszámok

- MTTD / MTTR
- patch compliance
- MFA-lefedettség
- kritikus sebezhetőségek javítási ideje
- backup visszaállítási sikerarány

Integrált megfelelési mutatók

- policy-process-evidence lefedettség
- tesztelt kontrollok aránya
- kontrollhibák javítási ideje
- ismétlődő audit findingok száma

A jó mérőszám nem a papír meglétét, hanem a kontroll viselkedését mutatja.

8. Miért fontosak a szimulációk?

A szimuláció a megfelelés valóságtartalom-vizsgálata.

Adatvédelmi incidens	ki veszi észre, ki minősít, mennyi idő alatt jutunk döntésig
Érintetti joggyakorlás próba	ki tudjuk-e gyűjteni az adatokat a valós rendszerekből
Ransomware tabletop	döntési lánc, backup, kommunikáció, hatósági értesítés
Beszállítói incidens	vendor- és processzorlánc, szerződéses eszkaláció, működő kontroll
Belső jogosultsági visszaélés	észlelhetőség, naplózás, HR-jog-IT koordináció

A szimuláció nem kellemetlen gyakorlat; ez a megfelelés valósági tesztje.

9. A megfelelés 4 szintje

1. Papíralapú

szabályzatok vannak, működési bizonyíték kevés

2. Folyamatalapú

folyamatok leírva, szerepkörök részben tiszták

3. Kontrollalapú

kontrollgazdák, rendszeres mérés, evidenciák

4. Ellenálló szervezet

tesztelt működés, gyors reagálás, folyamatos tanulás

ARB PRIVACY CONSULTING

A cél nem a több szabályzat, hanem a magasabb érettségi szint.

10. Egy 90 napos átállási logika

0-30 nap

- kulcskontrollok feltérképezése
- kontrollgazdák kijelölése
- legnagyobb papír-valóság rések azonosítása

31-60 nap

- mérőszámok és evidence-logika kialakítása
- első tabletop és DSR-próba
- vezetői dashboard prototípus

61-90 nap

- szimulációk futtatása
- korrekciós ciklusok lezárása
- éves kontrollteszt-program indítása

ARB PRIVACY CONSULTING

A megfelelés új korszaka

A papír nem véd meg.
A működő rendszer igen.

- A jövő megfelelése nem az, ki mit írt le, hanem az, mi működik bizonyíthatóan.
- Az adatvédelem és a kiberbiztonság közös tere ma már az ellenállóképesség.
- A jó szervezet ismeri a folyamatait, méri a kontrolljait, gyakorolja a reakcióit és tanul a hibáiból.

ARB PRIVACY CONSULTING

A kontroll csak akkor kontroll, ha működik, mérhető és bizonyítható.

KÖSZÖNÖM A FIGYELMET!

+36-30-9332-972

arb@arbconsulting.hu

ARB PRIVACY CONSULTING