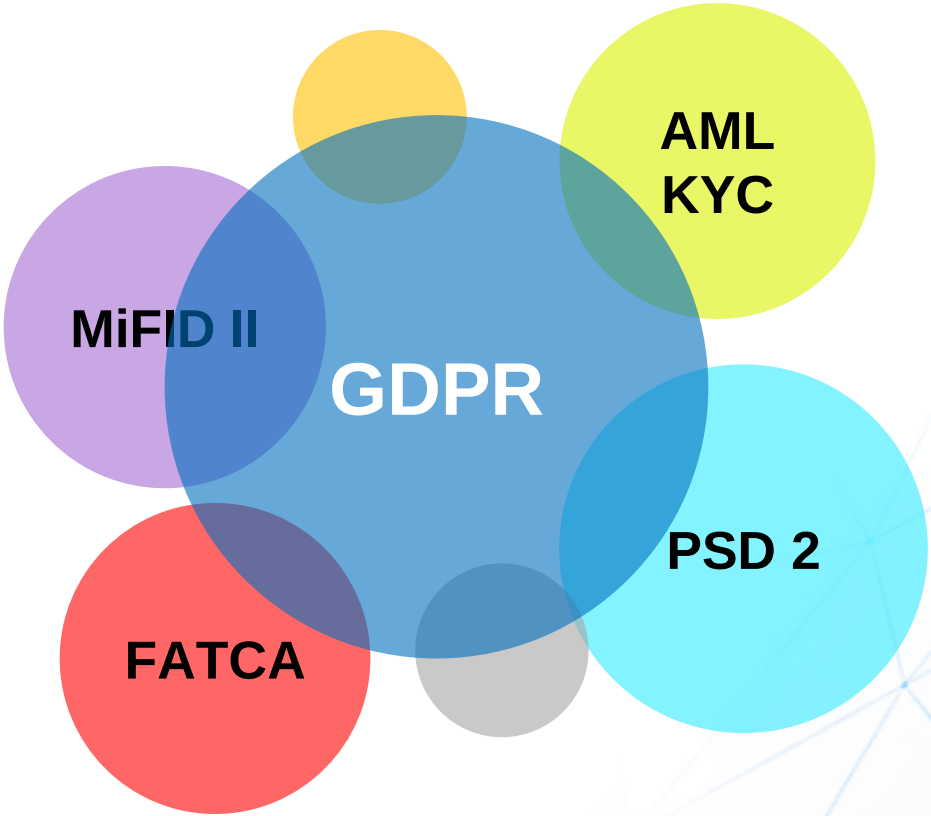
SYPHER

GDPR în contextul conformității financiar-bancare

Multiple reglementări influențate de GDPR



SYPHER

Obligațiile operatorului

- Ținerea evidenței activităților de prelucrare
- Evaluarea impactului asupra protecției datelor
- Măsuri tehnice și organizatorice adecvate
- Rezolvarea solicitărilor de la persoanele vizate
- Evaluări periodice ale conformității

SYPHER

Responsabilitatea pentru conformarea cu GDPR

WP243

- *RPD* (DPO-ul) *nu este responsabil personal* de neconformarea organizației la cerințele privind protecția datelor.
- *Operatorul sau persoana împuternicită* de către operator este cel sau cea care trebuie *să se asigure și să fie în măsură să demonstreze* că prelucrarea se efectuează în conformitate cu acest regulament.
- Conformitatea privind protecția datelor este *responsabilitatea operatorului sau a persoanei împuternicite de către operator*.

SYPHER

Responsabilitate distribuită/ delegată

***RPD* (DPO-ul)**

- acordă asistență operatorului pentru monitorizarea conformității
- consiliază operatorul privind EIPD
- este punct de contact pentru autoritatea de supraveghere
- alte activități, *conform fișei postului*

CEO/Board

- alocă sprijin/resurse adecvate pentru volumul de muncă (personal, spațiu, echipamente, software, formare etc)
- urmărește progresul

***Data stewards/ champions/* alte persoane**

- *conform fișei postului*

AML/KYC

- Analiza **temeiului legal** (interes legitim, consimțământ), în contextul în care nu toate prelucrările se fac **exclusiv** pentru îndeplinirea unei obligații legale
- Asigurarea **proporționalității/gradualității** prelucrării – diferențiere a volumului de date colectate/tipului de prelucrări pentru clienții cu risc redus față de cei cu risc ridicat.
- Dreptul la **informare și rectificare** – persoanele vizate nu au mereu relații directe cu instituția financiar-bancară

PSD 2

- Prelucrarea datelor unor persoane vizate în baza interesului legitim când există consimțământ dat doar de o parte a tranzacției (“**Silent party data**”)
- Diferențe privind **consimțământul** între PSD2 (consimțământ contractual) și GDPR (consimțământ explicit)
- Suficiența **standardelor tehnice** stabilite de European Banking Authority în contextul GDPR

SYPHER

FATCA

- Rezoluția Parlamentului European (5 iulie 2018) privind efectele negative ale Legii SUA referitoare la conformitatea fiscală aplicabilă conturilor din străinătate (FATCA) asupra cetățenilor UE și îndeosebi asupra „americanilor accidentali”
- Declarația Comitetului European pentru Protecția Datelor (ian 2019) privind intenția de a elabora până la **sfârșitul anului 2019** ghiduri privind dezvoltarea de garanții adecvate pentru transferul de date către IRS

Recomandări

- Identificați-vă **responsabilitățile formal asumate și** necesarul de pregătire/resurse pentru a le îndeplini
- Identificați activitățile efectuate in baza unei *obligații legale*, și analizați/inventariați separat eventualele **prelucrări suplimentare** ce necesită un alt temei legal
- Asigurați-vă că aveți implementat un sistem de lucru care vă permite să **revizuiți periodic** activitățile pentru care aveți responsabilități (în special cele de conformitate, inclusive eventuale schimbari legislative relevante)
- Consultați DPO-ul atunci când aveți **neclarități/îndoieli** privind o activitate

SYPHER

SYPHER

Mulțumesc!
Întrebări?