Pill: (segue) Regolamento DORA
"*Comunicazione della Banca d'Italia*", pubblicata in data 30 dicembre 2024

Premessa

La Comunicazione di Banca d'Italia del 30 dicembre 2024 fa seguito:

- allo *statement* del 4 dicembre 2024, in cui le ESAs hanno richiamato l'attenzione del mercato sulla prima applicazione del Regolamento DORA;
- alla "Comunicazione al mercato in materia di sicurezza ICT", pubblicata in data 23 dicembre 2024 (oggetto di precedente Pill).

Anche la presente comunicazione ha quali destinatari gli intermediari sottoposti alla vigilanza prudenziale di Banca d'Italia che rientrano nella definizione di "entità finanziarie" del Regolamento DORA (i.e. banche, imprese di investimento, gestori, istituti di pagamento, istituti di moneta elettronica, emittenti di token collegati ad attività, prestatori di servizi per le cripto attività, fornitori di servizi di *crowdfunding* – di seguito "**intermediari**").

Profili di attenzione per l'applicazione del Regolamento DORA richiamati da Banca d'Italia

1. **Istituzione/collocazione della funzione di controllo dei rischi ICT**
   Il Regolamento DORA prevede l'obbligo di attribuire la responsabilità della gestione dei rischi informatici ad una funzione di controllo ("funzione di controllo ICT"), che abbia un livello appropriato di indipendenza, al fine di evitare conflitti di interesse, senza tuttavia definire specifiche regole sulla sua collocazione organizzativa.

   In assenza di diverse indicazioni nella complessiva disciplina europea, Banca d'Italia, nel rispetto dei principi di proporzionalità e neutralità organizzativa, ed in continuità con quanto già previsto per le banche all'interno della Circolare 285/2013, precisa che gli intermediari potranno valutare se:

   - istituire o confermare un'autonoma funzione ICT, avente i requisiti delle funzioni di controllo di secondo livello, ove istituite,
     oppure
   - affidare lo svolgimento della funzione di controllo ICT alla struttura che svolge la funzione di *risk management* o a quella che svolge la funzione di *compliance*.

   Banca d'Italia specifica, inoltre, che:

   - nei casi in cui le funzioni di *risk management* e di *compliance* siano affidate a un'unica struttura, anche la funzione di controllo ICT può essere affidata a quest'ultima;
   - la scelta sulla collocazione organizzativa della funzione di controllo ICT non deve pregiudicare l'efficace svolgimento di tutti i compiti ad essa attribuiti;
   - la funzione di controllo ICT non può in ogni caso essere affidata alla struttura che svolge la funzione di *internal audit*.

2. **Comunicazione su servizi ICT**

Il Regolamento DORA prevede che i destinatari debbano informare l'autorità competente in merito a eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti (FEI), nonché del momento in cui una funzione diventa essenziale o importante.
Il Regolamento DORA non specifica, tuttavia, le tempistiche di questa informativa preventiva né prevede un potere di autorizzazione/nulla osta da parte dell'autorità competente.

Al riguardo Banca d'Italia chiarisce che, con l'entrata in vigore del Regolamento DORA, quindi a decorrere dal 17 gennaio 2025:

- non troveranno più applicazione le discipline settoriali in riferimento all'utilizzo da parte degli intermediari di servizi ICT prestati da fornitori terzi [1], fermo restando che i procedimenti amministrativi di divieto di esternalizzazione di FEI previsti dalla normativa di vigilanza continuano a trovare applicazione in caso di esternalizzazione di servizi non-ICT;
- prima di dare corso a eventuali accordi contrattuali previsti per l'utilizzo di servizi ICT a supporto di FEI, gli intermediari devono tempestivamente informare Banca d'Italia.

3. **Segnalazione incidenti ICT**

In applicazione del Regolamento DORA, gli intermediari devono segnalare all'Autorità di Vigilanza i gravi incidenti ICT e, su base volontaria, le minacce informatiche significative.

Al riguardo Banca d'Italia precisa che a decorrere dal 17 gennaio 2025 la disciplina vigente in materia sarà abrogata e sostituita dallo schema di notifica disciplinato dal nuovo Regolamento e dagli atti delegati (RTS e ITS).
In particolare, gli intermediari devono:

- classificare gli incidenti ICT e le minacce informatiche secondo quanto previsto dal regolamento delegato (UE) 2024/1772;
- segnalare a Banca d'Italia gli incidenti ICT attraverso la rilevazione denominata "*DORA – Segnalazione gravi incidenti ICT (DORAI)*";
- segnalare a Banca d'Italia le minacce informatiche significative attraverso la rilevazione denominata "*DORA – Segnalazione minacce informatiche significative (DORAM)*", tenendo conto dell'atto adottato dalla Commissione europea del 23 ottobre 2024 che specifica il contenuto e le tempistiche della segnalazione;
- utilizza, ai fini delle predette segnalazioni, i modelli standardizzati disponibili sul sito della Banca d'Italia.

---

[1] A partire dal 17 gennaio 2025, non dovranno ritenersi più applicabili i seguenti procedimenti amministrativi di divieto dell'esternalizzazione previsti dalla normativa secondaria della Banca d'Italia, ove aventi ad oggetto l'esternalizzazione di servizi ICT a supporto di FEI:

- *divieto di esternalizzare funzioni aziendali operative essenziali o importanti (Regolamento della Banca d'Italia di attuazione degli articoli 4-undecies e 6, comma 1, lett. b) e c-bis), del TUF: articolo 50, comma 3);*
- *divieto di esternalizzazione di funzioni aziendali operative essenziali o importanti a fornitori di servizi cloud (Regolamento della Banca d'Italia di attuazione degli articoli 4-undecies e 6, comma 1, lett. b) e c-bis), del TUF: articolo 18, comma 4);*
- *divieto di esternalizzare, in tutto o in parte, funzioni operative importanti e di controllo a un soggetto esterno o nell'ambito del gruppo di appartenenza per IP e IMEL (Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica: Capitolo VI, Sezione II).*

4. **Threat Led Penetration Test (“TLPT”)**

In applicazione del Regolamento DORA, i destinatari identificati secondo i criteri definiti dall’apposito atto delegato in corso di adozione sono tenuti a effettuare test avanzati di penetrazione basati su minacce (“*TLPT”)* almeno ogni tre anni.

Per quanto riguarda gli intermediari vigilati direttamente da Banca d’Italia, l’Autorità di Vigilanza precisa che il processo di identificazione degli intermediari obbligati ad effettuare i TLPT è ancora in corso e una volta concluso procederà ad informare i soggetti interessati nonché a definire, successivamente, una pianificazione per l’esecuzione dei test.

Per consultare la Comunicazione di Banca d’Italia del 30 dicembre, cliccare qui.