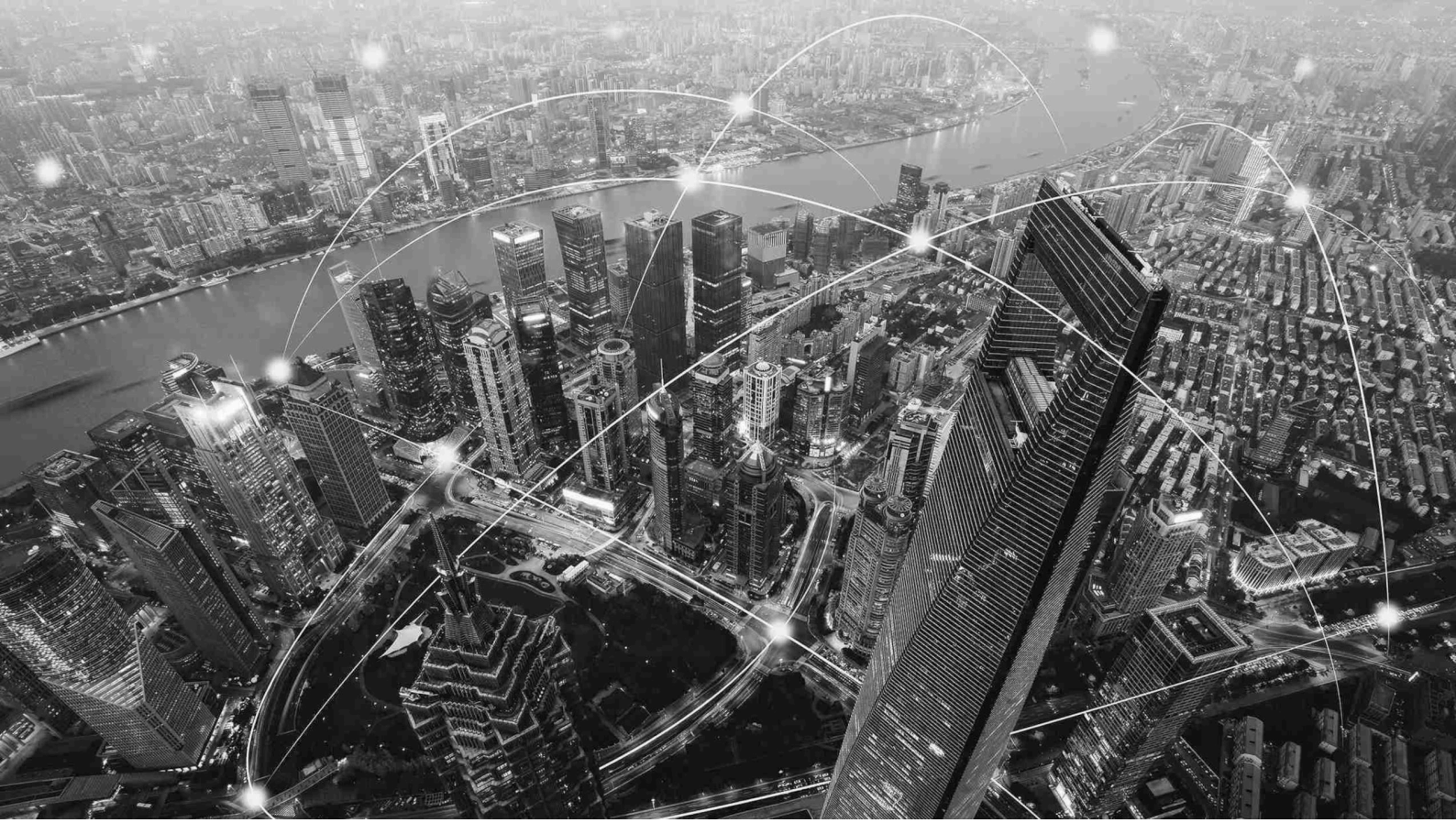


NEWSLETTER

anno 13° - newsletter 2/2026
Aggiornata al 28 febbraio 2026

PRIMO PIANO

- **DORA: comunicazione Banca d'Italia sulle tempistiche di trasmissione del Registro delle informazioni:**

  Con la comunicazione del 13 febbraio 2026, Banca d'Italia ha chiarito le modalità e le tempistiche di trasmissione del Registro delle informazioni sui contratti stipulati con fornitori terzi di servizi ICT, in attuazione del Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA).

- **DORA: chiarimenti del COVIP sulle tempistiche di trasmissione del Registro delle informazioni:**

  Con la circolare n. 847 del 19 febbraio 2026, la COVIP ha fornito indicazioni operative ai fondi pensione in merito alla trasmissione annuale, per l'anno 2026, del Registro delle informazioni relativo agli accordi contrattuali con i fornitori di servizi ICT previsto dal Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA).

- **FIA/OICVM: pubblicazione in GUUE del Regolamento delegato (UE) 2026/466 e del Regolamento delegato (UE) 2026/465:**

  In data 27 febbraio 2026 sono stati pubblicati in Gazzetta Ufficiale dell'Unione Europea il Regolamento delegato (UE) 2026/466 ed il Regolamento delegato (UE) 2026/465 contenenti norme tecniche di regolamentazione (*Regulatory Technical Standards o RTS*) che precisano le

caratteristiche degli strumenti di gestione della liquidità applicabili ai gestori di FIA (GEFIA) e ai gestori di OICVM, in attuazione, rispettivamente, dell'art. 16, par. 2-*decies*, co. 2 della direttiva 2011/61/UE e dell'art. 18-*bis*, par. 5, co. 2 della direttiva 2009/65/CE.

Sommario

PRIMO PIANO 1
1. Legislazione europea 4
1.1. EMIR: pubblicazione in GUUE del Regolamento delegato (UE) 2026/305 4
1.2. Solvency II: pubblicazione in GUUE del Regolamento di esecuzione (UE) 2026/349 4
1.3. Solvency II: pubblicazione in GUUE del Regolamento delegato (UE) 2026/269 5
1.4. FIA/OICVM: pubblicazione in GUUE del Regolamento delegato (UE) 2026/466 e del Regolamento delegato (UE) 2026/465 6
2. Decreti, regolamenti e disposizioni di vigilanza 8
2.1. DORA: comunicazione Banca d'Italia sulle tempistiche di trasmissione del Registro delle informazioni 8
2.2. ACN: pubblicazione in GU della determina in tema di tassonomia degli incidenti informatici 8
2.3. DORA: aggiornamento delle Disposizioni di vigilanza di Banca d'Italia per IP e IMEL 9
2.4. DORA: aggiornamento della Circolare 285 di Banca d'Italia 9
2.5. Garante Privacy: base giuridica e valutazione d'impatto in tema di riconoscimento facciale 10
2.6. DORA: chiarimenti del COVIP sulle tempistiche di trasmissione del Registro delle informazioni 11
3. Orientamenti, linee guida e Q&A 13
3.1. CRR: pubblicazione Linee guida EBA sui metodi di valutazione della diversificazione del portafoglio crediti 13
3.2. DORA: Q&A sulla qualificazione di fornitori ICT delle Autorità pubbliche 13
3.3. ENISA: pubblicazione della metodologia in tema di sicurezza informatica 14
3.4. DORA: Q&A sull'individuazione dei servizi telefonici qualificabili come servizi ICT 15
3.5. DORA: Q&A sulla possibile qualificazione del phishing come incidente ICT 16
3.6. IAIS: pubblicazione della guida pratica sulla gestione del rischio e sulla resilienza operativa 17
3.7. EIOPA: modifica alle Linee guida in tema di revisione e valutazione prudenziale ed esposizione al rischio di mercato e di controparte 18
3.8. EMIR: pubblicazione delle aspettative di vigilanza ESMA 18
3.9. MiFID II/MiFIR: l'ESMA ritira le Linee guida sugli obblighi in materia di dati di mercato 19

1. Legislazione europea

1.1. EMIR: pubblicazione in GUUE del Regolamento delegato (UE) 2026/305

CCP

In data 6 febbraio 2026 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento delegato (UE) 2026/305 del 29 ottobre 2025, che integra il Regolamento (UE) 2012/648 (*European Market Infrastructure* o EMIR), disciplinando le condizioni operative, l'obbligo di rappresentatività e gli obblighi di segnalazione connessi all'obbligo del conto attivo.

L'obiettivo della nuova disciplina, fondata sul progetto di norme tecniche di regolamentazione (*Regulatory Technical Standards* o RTS) predisposto dall'*European Securities and Markets Authority* (ESMA), è quello di assicurare che l'obbligo non rimanga meramente formale. Le controparti devono infatti essere concretamente in grado di utilizzare il conto attivo anche in presenza di improvvisi e significativi aumenti dei volumi di derivati da compensare.

In questa prospettiva, il Regolamento delegato chiarisce anzitutto i presupposti organizzativi richiesti. In base all'articolo 7-*bis*, paragrafo 3, lettere b) e c), del Regolamento EMIR, le controparti devono disporre di sistemi, risorse e strutture interne adeguate per gestire tempestivamente grandi volumi di operazioni e garantire che tutte le nuove transazioni possano essere compensate sul conto attivo in qualsiasi momento. A ciò si aggiunge l'obbligo di monitorare costantemente le esposizioni e di individuare preventivamente eventuali impedimenti di natura giuridica od operativa che possano limitarne l'utilizzo effettivo.

Un ulteriore livello di presidio riguarda la verifica della capacità operativa. Ai sensi dell'articolo 7-*bis*, paragrafo 4, le controparti sono tenute a effettuare *stress test* annuali, a svolgere prove tecniche e funzionali sulla connettività informatica con le CCP o con i partecipanti diretti e a dimostrare all'autorità competente di poter far fronte a eventuali picchi di attività.

Quanto al requisito di rappresentatività previsto dall'articolo 7-*bis*, paragrafo 3, lettera d), il Regolamento delegato demanda all'ESMA – in base al paragrafo 8 – la selezione di un numero limitato di categorie di derivati. Per ciascuna categoria vengono individuate specifiche fasce di scadenza e classi dimensionali delle operazioni. La metodologia adottata è orientata a riflettere la struttura effettiva dei mercati, a mantenere flessibilità rispetto a possibili evoluzioni future e a contribuire alla mitigazione dei rischi sistemici connessi all'eccessiva dipendenza da CCP di Paesi terzi. Al fine di evitare effetti distorsivi, le controparti devono concentrarsi sulle sottocategorie più rilevanti rispetto alla propria operatività, senza essere obbligate a compensare strumenti marginali.

Il Regolamento delegato disciplina inoltre in modo puntuale gli obblighi informativi. Le controparti devono calcolare la propria attività e le esposizioni per ciascuna categoria individuata, trasmettere alle autorità competenti dati aggregati con dettaglio per CCP e fornire informazioni sul numero di operazioni concluse e sulle sottocategorie selezionate. In base all'articolo 7-*ter* dell'EMIR, tali segnalazioni hanno cadenza semestrale e la prima comunicazione deve coprire l'intero periodo iniziale di applicazione della disciplina.

A completamento del quadro, sono stati introdotti modelli standardizzati di *reporting*, volti a garantire uniformità, completezza e maggiore efficacia delle comunicazioni alle autorità di vigilanza.

Per consultare il Regolamento, cliccare qui.

1.2. Solvency II: pubblicazione in GUUE del Regolamento di esecuzione (UE) 2026/349

Assicurazione

In data 18 febbraio 2026 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento di esecuzione (UE) 2026/349, recante le informazioni tecniche necessarie per il calcolo delle riserve tecniche e dei fondi propri di base ai fini delle segnalazioni delle imprese di assicurazione relative al periodo compreso tra il 31 dicembre 2025 e il 30 marzo 2026, in attuazione della Direttiva 2009/138/CE (Solvency II).

Il Regolamento stabilisce che, ai fini del calcolo delle riserve tecniche e dei fondi propri di base oggetto di segnalazione, debbano essere utilizzate le informazioni tecniche stabilite dal Regolamento stesso, precedentemente trasmesse dall'*European Insurance and Occupational Pensions Authority* (EIOPA) alla Commissione europea ed elaborate sulla base dei dati di mercato rilevati alla fine dell'ultimo mese precedente la prima data di riferimento cui si applica il provvedimento.

Nello specifico, le informazioni tecniche di cui sopra sono:

- le strutture per scadenza dei tassi di interesse privi di rischio, indicate nell'Allegato I;
- gli *spread* "fondamentali" rilevanti ai fini del calcolo dell'aggiustamento di congruità (*matching adjustment*), indicati nell'Allegato II;
- gli aggiustamenti per la volatilità per ciascun mercato assicurativo nazionale interessato (*volatility adjustment*), indicati nell'Allegato III.

Per consultare il Regolamento, cliccare qui.

1.3. Solvency II: pubblicazione in GUUE del Regolamento delegato (UE) 2026/269

Assicurazione

In data 18 febbraio 2026 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento delegato (UE) 2026/269 che modifica il Regolamento delegato (UE) 2015/35, per quanto riguarda le riserve tecniche, le misure di garanzia a lungo termine, i fondi propri, il rischio di capitale proprio, il rischio di *spread* sulle posizioni verso la cartolarizzazione, altri requisiti patrimoniali secondo la formula standard, la segnalazione e l'informativa, la proporzionalità e la solvibilità di gruppo.

Inserendosi nel solco della recente revisione dell'impianto normativo di Solvency II da parte della Direttiva (UE) 2025/2, la modifica del precedente Regolamento delegato 2015/35 si è resa necessaria al fine di specificare e aggiornare i principali parametri quantitativi, così da rendere pienamente operativo il nuovo regime dei requisiti prudenziali.

In primo luogo, è stata migliorata la disciplina delle misure di garanzia a lungo termine, attraverso l'introduzione di un trattamento preferenziale per gli investimenti di lungo periodo in strumenti di capitale. Tale intervento è finalizzato a sostenere la capacità delle imprese di assicurazione di detenere investimenti stabili nel tempo e ad accrescere il capitale disponibile in eccesso rispetto al requisito patrimoniale di solvibilità.

La riforma ha inoltre rafforzato il principio di proporzionalità, prevedendo una nuova categoria

di “imprese piccole e non complesse”. A tali soggetti è riconosciuto l’accesso automatico a misure di semplificazione chiaramente definite, che riguardano diversi ambiti, tra cui gli obblighi di segnalazione e informativa, i requisiti di *governance*, la revisione delle politiche scritte, il calcolo delle riserve tecniche, la valutazione interna del rischio e della solvibilità (ORSA) e la predisposizione dei piani di gestione del rischio di liquidità.

Infine, la Direttiva ha rafforzato la cooperazione tra le autorità di vigilanza, consolidando il ruolo di coordinamento e i poteri di supervisione dell'*European Insurance and Occupational Pensions Authority* (EIOPA) e ampliando gli strumenti macroprudenziali a disposizione delle autorità nazionali, al fine di garantire una maggiore stabilità del sistema assicurativo nel suo complesso.

Per consultare il Regolamento, cliccare qui.

1.4. FIA/OICVM: pubblicazione in GUUE del Regolamento delegato (UE) 2026/466 e del Regolamento delegato (UE) 2026/465

SGR, SICAF, SICAV

In data 27 febbraio 2026 sono stati pubblicati in Gazzetta Ufficiale dell'Unione Europea il Regolamento delegato (UE) 2026/466 ed il Regolamento delegato (UE) 2026/465 contenenti norme tecniche di regolamentazione (*Regulatory Technical Standards* o RTS) che precisano le caratteristiche degli strumenti di gestione della liquidità applicabili ai gestori di FIA (GEFIA) e ai gestori di OICVM, in attuazione, rispettivamente, dell’art. 16, par. 2-*decies*, co. 2 della direttiva 2011/61/UE e dell’art. 18-*bis*, par. 5, co. 2 della direttiva 2009/65/CE.

Con riferimento ai FIA, per ciascun fondo gestito diverso da un fondo chiuso che non ricorra alla leva finanziaria, il GEFIA è tenuto a dotarsi di un sistema adeguato di gestione della liquidità e ad adottare procedure idonee a monitorare il rischio di liquidità, assicurando la coerenza tra il profilo di liquidità degli attivi e le obbligazioni del fondo. In tale ambito, assume rilievo l’obbligo di effettuare prove di stress con cadenza regolare, sia in condizioni di mercato ordinarie sia in scenari di tensione, al fine di valutare l’esposizione al rischio di liquidità e di calibrare conseguentemente le misure di presidio adottate.

Per quanto concerne gli OICVM, l’art. 18-*bis* della direttiva 2009/65/CE impone ai gestori di selezionare almeno due strumenti di gestione della liquidità tra quelli elencati nell’allegato II *bis* (punti da 2 a 8), sulla base di una valutazione di adeguatezza che tenga conto della strategia di investimento, del profilo di liquidità e della politica di rimborso del fondo. I gestori devono inoltre definire politiche e procedure dettagliate che disciplinino l’attivazione e la disattivazione degli strumenti prescelti, nonché le relative modalità operative e amministrative di applicazione, in un’ottica di integrazione tra *governance*, *risk management* e operatività.

Le RTS dettano disposizioni puntuali in relazione all’utilizzo dei principali strumenti di gestione della liquidità, tra cui la sospensione delle sottoscrizioni, dei riacquisti e dei rimborsi, l’introduzione di restrizioni ai rimborsi (c.d. *gates*), la proroga dei termini di preavviso, l’applicazione di commissioni di rimborso, i meccanismi di *swing pricing* e *dual pricing*, il prelievo antidiluizione, i rimborsi in natura e l’istituzione di conti *side pocket*, contribuendo così a uniformare le prassi applicative e a rafforzare la resilienza dei fondi in situazioni di tensione di mercato.

Per consultare il Regolamento delegato (UE) 2026/466, cliccare qui.

Per consultare il Regolamento delegato (UE) 2026/465, cliccare qui.

2. Decreti, regolamenti e disposizioni di vigilanza

2.1. DORA: comunicazione Banca d'Italia sulle tempistiche di trasmissione del Registro delle informazioni

Banca, IMEL, IP, Operatore crowdfunding, SGR, SICAF, SICAV, SIM

Con comunicazione del 13 febbraio 2026, Banca d'Italia ha chiarito le scadenze per il 2026 relative alla trasmissione del Registro delle informazioni sui contratti stipulati con fornitori terzi di servizi ICT, in attuazione del Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA).

Il suddetto Regolamento impone alle entità finanziarie di istituire e mantenere aggiornato, a livello individuale nonché su base consolidata e sub-consolidata, un registro contenente tutte le informazioni sugli accordi contrattuali aventi ad oggetto servizi ICT forniti da terzi. In aggiunta, ai sensi dell'art. 28, paragrafo 3, del Regolamento stesso, il registro in oggetto deve essere reso disponibile all'autorità competente.

In Italia, l'autorità competente, Banca d'Italia, ha specificato come a decorrere dal 2026 l'invio del registro delle informazioni, per il tramite del portale INFOSTAT, dovrà avere cadenza annuale, fissata per il 15 marzo, con dati aggiornati al 31 dicembre dell'anno precedente.

L'Autorità ha inoltre precisato che i registri saranno oggetto di verifiche sulla qualità dei dati e che, qualora emergano errori o incongruenze, le entità finanziarie saranno chiamate a rettificare le informazioni nonché a procedere a un nuovo invio del registro stesso.

Per consultare la Comunicazione, cliccare qui.

2.2. ACN: pubblicazione in GU della determina in tema di tassonomia degli incidenti informatici

Tutti gli operatori

In data 17 febbraio 2026 è stata pubblicata in Gazzetta Ufficiale la determina del 9 febbraio 2026 adottata dall'Agenzia per la Cybersicurezza Nazionale (ACN), recante la definizione della tassonomia degli incidenti informatici ai sensi dell'art. 1, comma 1, della Legge 90/2024.

La disposizione richiamata ha introdotto, a carico dei soggetti individuati dalla legge, uno specifico obbligo di segnalazione relativo a determinate categorie di incidenti aventi impatto su reti, sistemi informativi e servizi informatici, da individuarsi mediante apposita tassonomia, rimandando la definizione di quest'ultima ad un'apposita determinazione tecnica del Direttore generale dell'ACN.

Si inserisce in tale quadro anche il Decreto Legislativo 128/2024 (c.d. decreto NIS), il cui art. 31, commi 1 e 2, stabilisce che l'Autorità nazionale competente NIS, ai fini dell'applicazione degli artt. 23, 24, 25, 27, 28 e 29, debba determinare obblighi proporzionati, tenendo conto, tra l'altro, del livello di esposizione al rischio dei soggetti interessati, delle loro dimensioni, nonché della probabilità e della gravità degli incidenti, inclusi gli impatti di natura sociale ed economica.

In attuazione di tale previsione, l'ACN aveva già adottato la determina n. 379907/2025, con la quale sono state definite le modalità operative e le specifiche di base per l'adempimento degli obblighi previsti dal decreto NIS; in particolare, l'Allegato 3 individua la tassonomia degli "incidenti significativi di base" riferita ai soggetti qualificati come importanti.

L'ACN ha inoltre precisato come la prenotifica e la notifica effettuate conformemente all'art. 25 del decreto NIS valgano anche ai fini dell'assolvimento dell'obbligo di segnalazione

previsto dall'art. 1, comma 1, della Legge 90/2024.

Per consultare la Determina, cliccare qui.

2.3. DORA: aggiornamento delle Disposizioni di vigilanza di Banca d'Italia per IP e IMEL

IMEL, IP

Banca d'Italia, con provvedimento del 3 febbraio 2026, pubblicato in Gazzetta Ufficiale il 18 febbraio 2026 ed efficace a partire dal giorno successivo, ha aggiornato le Disposizioni di vigilanza per gli istituti di pagamento (IP) e per gli istituti di moneta elettronica (IMEL) al fine di riordinare la disciplina relativa ai sistemi informativi e alla gestione dei rischi operativi e di sicurezza, in linea con il quadro normativo introdotto dal Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA) e dai relativi atti delegati, dalla Direttiva (UE) 2022/2556 nonché dagli Orientamenti EBA dell'11 febbraio 2025 (EBA/GL/2025/02).

Il suddetto provvedimento, oltre ad aver abrogato il procedimento amministrativo relativo al divieto di esternalizzazione di funzioni operative connesse a servizi di pagamento o emissione di moneta elettronica ed al sistema dei controlli interni, sistema informativo o componenti critiche dello stesso, ha modificato le seguenti parti delle Disposizioni di vigilanza per IP e IMEL:

- il Capitolo I, Sezione I e II;
- il Capitolo VI, Sezioni I, II e IV;
- gli Allegati A, B, C, D ed E.

Per consultare il Provvedimento, cliccare qui.

2.4. DORA: aggiornamento della Circolare 285 di Banca d'Italia

Banca

Banca d'Italia, con atto di emanazione del 3 febbraio 2026 pubblicato in Gazzetta Ufficiale il 18 febbraio 2026, ha aggiornato la Circolare 285 del 17 dicembre 2013, recante le Disposizioni di vigilanza per le banche, in attuazione del Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA), dei relativi atti delegati nonché della Direttiva (UE) 2022/2556.

Le modifiche introdotte dal suddetto provvedimento riguardano:

- le Disposizioni introduttive;
- Parte Prima, Titolo I, Capitolo I;
- nella Parte Prima, Titolo IV, Capitolo 3, Capitolo 4 e Capitolo 5.

In sintesi, le principali novità introdotte consistono in:

- abrogazione delle Sezioni del Capitolo 4 relative a: governo del sistema informativo, gestione del rischio ICT e di sicurezza, sicurezza dell'informazione e delle operazioni ICT, gestione dei progetti e dei cambiamenti ICT, esternalizzazione del sistema informativo e ricorso a fornitori terzi di servizi ICT; tali Sezioni vengono sostituite da rinvii diretti alle disposizioni del Regolamento DORA e dei relativi atti delegati, concernenti strumenti, metodi, processi e politiche per la gestione dei rischi informatici, la regolamentazione dei contratti con fornitori terzi, e la gestione degli incidenti e delle minacce ICT significative;

- il sistema di gestione dei dati, non ricompreso nel *framework* DORA, è stato spostato nel Capitolo 3 "Il sistema dei controlli interni";

- la sezione sulle disposizioni specifiche per la prestazione di servizi di pagamento è stata aggiornata per recepire gli Orientamenti EBA dell'11 febbraio 2025 (EBA/GL/2025/02), abrogando i precedenti Orientamenti EBA/GL/2019/04, mantenendo solo i paragrafi relativi alla gestione del rapporto con gli utenti dei servizi di pagamento;

- il Capitolo 5, relativo ai requisiti di continuità operativa applicabili a tutti gli operatori, è stato modificato per allinearsi alle disposizioni della Direttiva 2022/2556 e rimuovere le norme sulla continuità operativa ICT, sostituite da quelle direttamente applicabili del Regolamento DORA e dei relativi atti delegati.

Banca d'Italia ha precisato che l'aggiornamento non modifica, per il momento, l'Allegato A, Sezione III, del Capitolo 5 sui requisiti particolari per i processi a rilevanza sistemica, in quanto tale tematica coinvolge anche altri operatori finanziari oltre alle banche ed è oggetto di approfondimenti più ampi.

Le modifiche sono entrate in vigore il giorno successivo alla pubblicazione in Gazzetta Ufficiale e le banche dovranno adeguarsi alle nuove disposizioni del Capitolo 5 della Parte Prima, Titolo IV, entro sei mesi dall'entrata in vigore dell'aggiornamento.

Gli aggiornamenti si applicano anche alle succursali in Italia di banche extracomunitarie, a decorrere dall'entrata in vigore della normativa di attuazione dell'art. 58-*quinquies* del TUB, introdotto dal D. Lgs. 208/2025; fino a tale data, per le succursali extracomunitarie continueranno a trovare applicazione i Capitoli 3, 4 e 5 della Parte Prima, Titolo IV, della Circolare 285/2013 nella versione precedente al presente aggiornamento.

Per consultare il Provvedimento, cliccare qui.

2.5. Garante Privacy: base giuridica e valutazione d'impatto in tema di riconoscimento facciale

Tutti gli operatori

Il Garante per la protezione dei dati personali, con provvedimento n. 35 del 29 gennaio 2026, si è pronunciato in merito alla corretta individuazione della base giuridica e all'obbligo di effettuare una valutazione d'impatto nell'ambito dell'utilizzo di sistemi di riconoscimento facciale.

Nel caso esaminato dall'Autorità, un'università telematica si era avvalsa di strumenti di riconoscimento biometrico al fine di identificare i partecipanti ai corsi e di poterne così accertare o meno l'effettiva frequenza dei corsi. L'Ateneo aveva individuato quale base giuridica del trattamento il consenso degli interessati, qualificandolo tuttavia come necessario

per poter accedere alle attività formative.

Nel concreto, in fase di registrazione al corso, il sistema adottato prevedeva la creazione di un modello biometrico mediante l'acquisizione dell'immagine del volto dell'interessato nonché di una fotografia del documento di identità. I docenti inoltre, durante lo svolgimento delle lezioni, potevano richiedere l'acquisizione di un'ulteriore immagine tramite *webcam*, al fine di verificarne la corrispondenza con il modello precedentemente generato. I dati così raccolti venivano conservati per dodici mesi, a fronte di una durata media dei corsi pari a cinque o sei mesi, con la finalità dichiarata di gestire eventuali contestazioni o richieste successive da parte degli studenti.

Con riferimento alla valutazione d'impatto, l'Ateneo, dopo una prima valutazione in senso negativo circa la sua necessità, aveva successivamente predisposto una DPIA, priva tuttavia di data certa e di sottoscrizione da parte del titolare del trattamento.

L'Autorità ha ritenuto che, nel caso di specie, la base giuridica corretta dovesse essere individuata nell'esecuzione di un compito di interesse pubblico connesso all'attività formativa, escludendo la validità del consenso quale fondamento del trattamento. Ai fini della validità, infatti, il consenso deve essere liberamente prestato; nel contesto esaminato, tale requisito non risultava soddisfatto, poiché l'accesso alle lezioni era subordinato alla prestazione del consenso e sussisteva un evidente squilibrio tra interessato e titolare, non essendo riconosciuta agli studenti una reale alternativa.

Il Garante ha inoltre evidenziato il mancato rispetto dei principi di minimizzazione, limitazione della conservazione e adeguata protezione dei dati. In caso di esito positivo della verifica biometrica, non sussisteva alcuna giustificazione per la conservazione dei dati oltre il periodo strettamente necessario allo svolgimento del corso; in caso di esito negativo, sarebbe stato possibile procedere a un accertamento dell'identità "de visu" da parte del docente, rendendo superflua la memorizzazione delle informazioni biometriche.

L'Autorità ha infine ribadito che, ai sensi dell'art. 35 del Regolamento (UE) 2016/679 (*General Data Protection Regulation* o GDPR), la valutazione d'impatto è obbligatoria in presenza di trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche. Tale obbligo assume particolare rilievo in caso di trattamento di categorie particolari di dati personali, quali quelli biometrici, imponendo anche la verifica della possibilità di adottare soluzioni meno invasive idonee a conseguire le medesime finalità. Laddove, inoltre, il trattamento di dati sensibili avvenga su larga scala, l'obbligo di redazione della DPIA risulta ancor più stringente.

Per consultare il Provvedimento, cliccare qui.

2.6. DORA: chiarimenti del COVIP sulle tempistiche di trasmissione del Registro delle informazioni

Fondi pensione

In data 19 febbraio 2026, la COVIP, con la circolare n. 847, ha fornito indicazioni operative ai fondi pensione in merito alla trasmissione annuale, per l'anno 2026, del Registro delle informazioni relativo agli accordi contrattuali con i fornitori di servizi ICT previsto dal Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA).

Nella suddetta circolare, l'Autorità ha chiarito come a partire dal 2026 l'invio del registro delle informazioni dovrà avere cadenza annuale, fissata al 17 marzo, con dati aggiornati al 31 dicembre dell'anno precedente. Tale termine è stato individuato in considerazione della

scadenza fissata dall'EBA per la ricezione, entro il 31 marzo 2026, dei registri delle informazioni sui fornitori ICT trasmessi dalle autorità nazionali competenti ai sensi del Regolamento DORA.

La COVIP ha infine richiamato l'attenzione dei fondi pensione sull'obbligo di dotarsi di un codice LEI in corso di validità, necessario al rispetto delle convenzioni di nomenclatura definite a livello europeo per la corretta gestione e trasmissione dei dati.

Per consultare la Circolare, cliccare qui.

3. Orientamenti, linee guida e Q&A

3.1. CRR: pubblicazione Linee guida EBA sui metodi di valutazione della diversificazione del portafoglio crediti

AISP, Banca, Fiduciarie, IMEL, Intermediario 106 Tub, IP, SICAF, SICAV, SIM

In data 13 febbraio 2026 l'*European Banking Authority* (EBA) ha pubblicato le Linee guida definitive volte a chiarire come applicare, in modo proporzionato, i criteri di diversificazione ai portafogli di crediti al dettaglio nell'ambito del Regolamento (UE) 575/2013 (*Capital Requirements Regulation* o CRR).

In forza dell'art. 123, paragrafo 1, del Regolamento CRR, infatti, è attribuito all'EBA il compito di specificare metodologie idonee a verificare quando le esposizioni al dettaglio possano considerarsi parte di un numero significativo di posizioni analoghe al fine di assicurare che i rischi connessi a tali esposizioni risultino sostanzialmente attenuati grazie a un adeguato livello di diversificazione, come richiesto dalla lettera c) della medesima disposizione.

Viene infatti previsto dalla disciplina prudenziale che le esposizioni *retail* possano beneficiare della ponderazione di rischio preferenziale del 75% solo se rappresentano una quota rilevante di un insieme ampio di esposizioni con caratteristiche omogenee, così da garantire una riduzione effettiva del rischio tramite la frammentazione del portafoglio.

In concreto, per accedere alla ponderazione del 75%, gli enti devono dimostrare che il portafoglio ammissibile sia adeguatamente diversificato. Come criterio di riferimento iniziale, nessuna esposizione verso una singola controparte, o verso un gruppo di clienti connessi, dovrebbe eccedere lo 0,2% del totale del portafoglio *retail* rilevante. In alternativa, la ponderazione preferenziale resta applicabile anche in caso di superamento della soglia dello 0,2%, purché le esposizioni eccedenti non rappresentino più del 10% del portafoglio *retail* complessivo ammissibile.

Le Linee guida affrontano inoltre il tema delle esposizioni *retail* oggetto di cartolarizzazione, distinguendo tra il caso in cui l'ente operi come *originator* e quello in cui agisca come investitore, prevedendo criteri differenziati per la verifica della diversificazione. Per gli enti investitori, è stata prevista una deroga circoscritta e temporanea nell'ipotesi in cui i modelli di trasparenza applicabili non rendano disponibili informazioni a livello di singolo debitore: in tali casi, la condizione di diversificazione può considerarsi soddisfatta, entro i limiti stabiliti, al fine di evitare effetti penalizzanti non giustificati.

Per consultare le Linee guida, cliccare qui.

3.2. DORA: Q&A sulla qualificazione di fornitori ICT delle Autorità pubbliche

AISP, Banca, IMEL, IP, Operatore crowdfunding, SGR, SICAF, SICAV, SIM

L'*European Banking Authority* (EBA), mediante la Q&A n. 7466/2025 del 6 febbraio 2026, ha fornito chiarimenti in ordine alla qualificazione delle Autorità pubbliche quali fornitori di servizi ICT ai sensi del Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA).

Il quesito sottoposto all'Autorità era diretto a stabilire se l'esenzione prevista dal considerando 63, terza frase (seconda parte), del Regolamento DORA – riferita alle Autorità pubbliche che erogano servizi ICT nell'esercizio di funzioni statali – debba essere interpretata quale esclusione generalizzata applicabile a tutte le Autorità pubbliche, come definite dall'art. 3, punto 65, del medesimo Regolamento, ovvero se tale deroga debba ritenersi circoscritta al solo ambito dei servizi e delle soluzioni di pagamento.

Il considerando 63, prima frase, stabilisce in via generale che il perimetro della vigilanza sui fornitori terzi di servizi ICT debba comprendere un'ampia platea di soggetti. La terza frase del medesimo considerando precisa, inoltre, che anche i partecipanti all'ecosistema dei pagamenti che svolgano attività di elaborazione dei pagamenti o gestiscano infrastrutture di pagamento sono da qualificarsi, ai fini del Regolamento DORA, come fornitori terzi di servizi ICT. Nella stessa disposizione sono tuttavia previste due specifiche esclusioni: da un lato, le banche centrali, ove operino sistemi di pagamento o di regolamento titoli; dall'altro, le Autorità pubbliche, quando forniscano servizi connessi alle ICT nell'ambito dell'adempimento di funzioni statali.

L'incertezza interpretativa concerneva, pertanto, l'estensione dell'esenzione riconosciuta alle Autorità pubbliche, ossia se essa operi in termini generali per qualsiasi servizio ICT reso nell'esercizio di pubbliche funzioni oppure se sia limitata a servizi ICT qualificati, quali, ad esempio, quelli afferenti al settore dei pagamenti. Ulteriore profilo di dubbio riguardava l'ampiezza della nozione di "servizi connessi alle ICT", non definita dal Regolamento DORA, e la sua eventuale maggiore estensione rispetto al concetto di "servizi ICT".

A titolo esemplificativo, si è prospettato il caso di una pubblica amministrazione che metta a disposizione di istituti finanziari strumenti software per la gestione di sovvenzioni, anche rifinanziate da istituzioni dell'Unione europea: in tale ipotesi, pur trattandosi di attività evidentemente correlate alle ICT, l'ente pubblico opererebbe nell'ambito dell'adempimento di una funzione statale e, pertanto, non dovrebbe essere qualificato quale fornitore terzo di servizi ICT, con conseguente esclusione dall'ambito della gestione del rischio ICT di terze parti da parte dell'intermediario finanziario.

L'EBA ha chiarito che il considerando 63 del Regolamento DORA deve essere interpretato in senso estensivo, nel senso di escludere, in linea generale, le Autorità pubbliche dall'ambito applicativo della disciplina relativa alla designazione dei fornitori di servizi ICT ai fini del Regolamento. Ne deriva che un'Autorità pubblica che metta a disposizione dati a favore di soggetti finanziari non rientra, per ciò solo, nel perimetro del Regolamento DORA quale fornitore di servizi ICT.

Coerentemente, gli obblighi relativi al contenuto degli accordi contrattuali con fornitori terzi di servizi ICT, previsti dall'art. 30, paragrafo 2, trovano applicazione esclusivamente nei casi in cui l'entità finanziaria si avvalga di un fornitore terzo qualificabile come tale ai sensi del Regolamento Dora; qualora l'Autorità pubblica non assuma tale qualifica, non risultano applicabili i correlati requisiti contrattuali, ivi inclusi quelli di cui alle lettere b) e d) del citato paragrafo.

Per consultare il quesito e la relativa risposta, cliccare qui.

3.3. ENISA: pubblicazione della metodologia in tema di sicurezza informatica

Tutti gli operatori

In data 16 febbraio 2026, l'*European Union Agency for Cybersecurity* (ENISA) ha pubblicato una metodologia dedicata alle esercitazioni in materia di sicurezza informatica, finalizzata a fornire un impianto teorico di riferimento per la programmazione, lo svolgimento e la successiva valutazione di tali attività (*Cybersecurity Excercise Methodology*).

Il documento pubblicato propone un quadro teorico organico per la pianificazione, l'esecuzione e la valutazione delle esercitazioni, con particolare attenzione al corretto coinvolgimento dei soggetti e degli *stakeholder* rilevanti nelle diverse fasi del processo. Esso integra, inoltre, contenuti di natura teorica elaborati sulla base delle lezioni apprese, delle

migliori prassi di settore e delle esperienze maturate in ambito *cybersecurity*. La metodologia è concepita per essere impiegata congiuntamente a un apposito *toolkit* di supporto, comprensivo di modelli operativi e materiali di indirizzo destinati a facilitare l'organizzazione di esercitazioni efficaci e coerenti con gli obiettivi prefissati.

L'impianto metodologico si rivolge a professionisti della sicurezza informatica, organizzazioni pubbliche e private nonché autorità governative che intendano acquisire competenze nella progettazione e gestione di esercitazioni, valutare il livello attuale di preparazione rispetto a potenziali attacchi informatici, sensibilizzare il management sull'importanza strategica di tali iniziative ovvero testare, in un'ottica integrata, competenze, capacità di risposta, resilienza alle minacce e conformità ai requisiti normativi applicabili.

Per consultare la Metodologia, cliccare qui.

3.4. DORA: Q&A sull'individuazione dei servizi telefonici qualificabili come servizi ICT

AISP, Banca, IMEL, IP, Operatore crowdfunding, SGR, SICAF, SICAV, SIM

L'*European Banking Authority* (EBA), con Q&A n. 7539/2025 del 6 febbraio 2026, è intervenuta per precisare quali servizi telefonici possano essere ricompresi nella nozione di "servizi ICT" ai sensi del Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA).

Ai sensi dell'art. 3, paragrafo 21, del Regolamento DORA, per servizi ICT devono intendersi i servizi digitali e di gestione dei dati erogati tramite sistemi ICT, su base continuativa, a favore di uno o più utenti interni o esterni, ivi inclusi i modelli "*hardware as a service*" e i servizi *hardware* accompagnati da supporto tecnico mediante aggiornamenti *software* o *firmware*; sono invece espressamente esclusi i servizi telefonici analogici tradizionali. Il considerando 35 del Regolamento DORA precisa che tale esclusione riguarda unicamente la categoria circoscritta dei servizi di telefonia analogica qualificabili come servizi di rete telefonica pubblica commutata (PSTN), servizi di rete fissa o *Plain Old Telephone Service* (POTS).

Permanevano tuttavia dubbi interpretativi in ordine alla qualificazione delle infrastrutture di telecomunicazione di più recente generazione, quali le linee in fibra ottica, comprese quelle "spente" o non ancora attivate. In particolare, ci si interrogava se tali infrastrutture, pur non avendo natura analogica, potessero essere assimilate ai servizi di rete fissa e, per tale via, beneficiare dell'esclusione.

L'EBA ha richiamato la formulazione ampia adottata dal Regolamento DORA, che ricomprende nella definizione di servizi ICT qualsiasi servizio digitale — ossia elettronico e non meramente elettrico — idoneo a incidere direttamente sul funzionamento dei sistemi informativi e di comunicazione delle entità finanziarie. In tale ambito rientrano anche i servizi di connettività e di trasmissione dati, incluse le reti di telecomunicazione e, conseguentemente, le infrastrutture in fibra ottica.

L'Autorità ha inoltre chiarito che l'espressione "servizi telefonici analogici tradizionali" deve essere intesa con riferimento alla telefonia a commutazione di circuito di tipo analogico, quale quella veicolata tramite rete PSTN per il servizio POTS, caratterizzata dalla trasmissione della voce mediante segnali elettrici analogici continui. Il riferimento ai servizi di rete fissa contenuto nel considerando 35 va dunque interpretato in coerenza con tale nozione e concerne esclusivamente le linee fisse utilizzate per il tradizionale servizio vocale analogico, non già l'infrastruttura fisica in quanto tale.

La ratio dell'esclusione non risiede nel mezzo trasmissivo impiegato (rame, fibra o altro), bensì nella tecnologia sottostante. La rete telefonica pubblica analogica opera mediante modulazione elettrica continua, mentre la fibra ottica è destinata al trasporto di segnali ottici digitali, basati su trasmissione a commutazione di pacchetto e su sistemi elettronici necessari per l'attivazione, l'instradamento e la protezione dei flussi informativi; tale infrastruttura è tipicamente utilizzata per servizi di comunicazione digitale, inclusi servizi di telefonia IP e piattaforme *cloud*. La circostanza che la fibra sia temporaneamente inattiva non ne modifica la natura di mezzo destinato al traffico digitale, trattandosi comunque di capacità trasmissiva che, una volta attivata, concorre direttamente al funzionamento dei sistemi ICT.

Alla luce della finalità del Regolamento DORA, volta a garantire la resilienza operativa digitale e la continuità dei servizi ICT a supporto del settore finanziario, la distinzione tra fibra "attiva" e "inattiva" risulta priva di rilievo: ciò che assume importanza è il ruolo dell'infrastruttura quale componente critica da implementare, monitorare e proteggere, anche ai fini del ripristino in caso di interruzioni.

Ne consegue che, diversamente dai servizi vocali analogici tradizionali — progressivamente dismessi e non più centrali sotto il profilo della resilienza digitale — i servizi fondati su infrastrutture in fibra ottica costituiscono elementi essenziali delle comunicazioni digitali contemporanee e devono pertanto essere ricompresi nell'ambito dei servizi ICT ai sensi del Regolamento DORA.

Per consultare il quesito e la relativa risposta, cliccare qui.

3.5. DORA: Q&A sulla possibile qualificazione del phishing come incidente ICT

AISP, Banca, IMEL, IP, Operatore crowdfunding, SGR, SICAF, SICAV, SIM

L'*European Banking Authority* (EBA), con Q&A n. 7613/2025 del 6 febbraio 2026, ha fornito chiarimenti in merito alla qualificazione di singoli episodi di phishing rivolti ai clienti di un'entità finanziaria nella loro "sfera privata" ai fini della definizione di incidente ICT di cui all'art. 3, n. 8, del Regolamento (UE) 2022/2554 (c.d. *Digital Operational Resilience Act* o DORA) e della conseguente obbligatorietà di segnalazione prevista dall'art. 19, par. 1, dello stesso Regolamento.

Il quesito riguarda la possibilità di considerare tali episodi di *phishing* come incidenti ICT quando essi colpiscono i clienti al di fuori dei canali ufficiali dell'ente finanziario, ad esempio tramite clic su link di *phishing* nella posta elettronica privata o inserimento delle credenziali su pagine di *phishing* che imitano la *homepage* dell'ente.

Affinché un episodio di *phishing* possa essere qualificato come incidente ICT grave, devono essere soddisfatti i criteri definiti dagli artt. 3, par. 8 e 10, del Regolamento DORA, ossia deve verificarsi una compromissione della sicurezza delle reti e dei sistemi informativi. Tuttavia, l'art. 3, par. 8, non specifica se tale compromissione debba riguardare direttamente l'ente finanziario o se possa estendersi anche ai clienti.

L'istante ha evidenziato che i criteri per la valutazione di incidenti gravi indicati nel Regolamento Delegato (UE) 2024/1772 non chiariscono il rapporto tra art. 6 del Regolamento Delegato e la definizione di incidente ICT ai sensi del Regolamento DORA, generando approcci divergenti tra le autorità di vigilanza nazionali e potenziali incertezze nell'interpretazione della norma e nella comparabilità delle segnalazioni. Inoltre, la segnalazione obbligatoria di tutti gli episodi di *phishing* dei clienti comporterebbe un rilevante carico operativo per le entità finanziarie, dato l'elevato numero di incidenti che supererebbero

le soglie di rilevanza previste dagli artt. 8, par. 1, lett. a) e 9, par. 5, lett. a), del Regolamento Delegato.

L'EBA chiarisce che un episodio di *phishing* che colpisce la sfera privata del cliente e non influisce direttamente sui servizi dell'ente finanziario, né su quelli erogati tramite i fornitori terzi dell'ente, non costituisce un incidente correlato alle ICT né un incidente operativo o di sicurezza dei pagamenti ai sensi del Regolamento DORA. Di conseguenza, in tali circostanze, non si applicano le soglie per la classificazione di incidente ICT grave e non scatta l'obbligo di segnalazione.

Al contrario, se l'ente finanziario è direttamente bersaglio dell'attacco — ad esempio tramite *phishing* rivolto ai propri dipendenti — o se una campagna di *phishing* su larga scala compromette i servizi dell'ente, l'evento può essere qualificato come incidente ICT ai sensi del Regolamento DORA e, una volta raggiunte le soglie previste, essere classificato come incidente ICT grave, attivando gli obblighi di notifica previsti dal Regolamento.

Per consultare il quesito e la relativa risposta, cliccare qui.

3.6. IAIS: pubblicazione della guida pratica sulla gestione del rischio e sulla resilienza operativa

Assicurazione

In data 12 febbraio 2026 l'*International Association of Insurance Supervisors* (IAIS) ha pubblicato la versione definitiva di una guida pratica dedicata alla gestione del rischio e alla resilienza operativa nel settore assicurativo. Il documento individua specifici obiettivi rivolti sia alle imprese di assicurazione sia alle Autorità di vigilanza, corredati da un apposito *toolkit* operativo a supporto dell'implementazione (*Application Paper on operational resilience objectives and toolkit*).

Nel quadro regolamentare di riferimento, gli *Insurance Core Principles* (ICP) ribadiscono la necessità che le compagnie si dotino di assetti di *governance* e processi di *risk management* idonei a presidiare in modo efficace l'insieme dei rischi cui sono esposte.

Il documento si articola in due componenti tra loro complementari:

- obiettivi di resilienza operativa, che definiscono un *framework* di alto livello funzionale al conseguimento degli ICP;
- *toolkit* di supporto, che mette a disposizione delle Autorità di vigilanza strumenti e approcci pratici per l'attuazione delle aspettative regolamentari.

Sotto il profilo contenutistico, la guida affronta, tra l'altro:

- il rapporto tra resilienza operativa, assetti di *governance* e gestione del rischio operativo;
- gli elementi essenziali di un sistema efficace di resilienza operativa, illustrando un'ampia gamma di prassi adottate a livello di vigilanza;
- obiettivi specificamente indirizzati ai supervisori assicurativi, accompagnati da indicazioni operative in merito al coordinamento con altre Autorità competenti, alla trasparenza delle comunicazioni verso gli ed alla promozione di una cultura orientata al miglioramento continuo e all'apprendimento in materia di resilienza operativa.

Per consultare la Guida, cliccare qui.

3.7. EIOPA: modifica alle Linee guida in tema di revisione e valutazione prudenziale ed esposizione al rischio di mercato e di controparte

Assicurazione

In data 13 febbraio 2026, l'*European Insurance and Occupational Pensions Authority* (EIOPA) ha pubblicato gli aggiornamenti alle proprie Linee guida in materia di processo di revisione e valutazione prudenziale (*Supervisory Review Process* – SRP) ed alle Linee guida in materia di trattamento delle esposizioni al rischio di mercato e di controparte nell'ambito della formula standard per le imprese di assicurazione.

Per entrambi i documenti, originariamente adottati nel 2015, le modifiche ora introdotte si collocano nel contesto della revisione della Direttiva (UE) 2009/138 (Solvency II) e mirano ad aggiornare il quadro di riferimento, chiarendo e semplificando le disposizioni esistenti e ampliandone l'ambito applicativo per includere i rischi emergenti.

Per quanto riguarda le Linee guida sul processo di revisione prudenziale, le modifiche hanno riguardato l'allineamento delle disposizioni agli sviluppi normativi più recenti e alle di vigilanza maturate negli ultimi anni e l'integrazione di nuovi processi e presidi volti a intercettare rischi e tendenze emersi successivamente.

Vengono inoltre fornite indicazioni affinché le Autorità nazionali integrino nei propri processi di revisione prudenziale anche i rischi di sostenibilità, i rischi ICT e l'impiego di strumenti di tecnologia di vigilanza (*SupTech*).

Per quanto concerne, invece, le Linee guida sul trattamento delle esposizioni al rischio di mercato e di controparte nelle formula standard, le modifiche sono volte principalmente ad aggiornare i richiami normativi e a rendere il testo più chiaro e lineare. Più nello specifico, alcune Linee guida sono state eliminate, in quanto il relativo contenuto risultava già sufficientemente disciplinato dalle disposizioni di Solvency II o non più coerente con il quadro normativo vigente mentre altre sono state riviste al fine di estenderne o meglio precisarne l'ambito di applicazione. E' stata inoltre introdotta una nuova Linea guida per chiarire il trattamento prudenziale dei fondi con leva finanziaria.

Per consultare le Linee guida sul processo di revisione prudenziale, cliccare qui.

Per consultare le Linee guida sul trattamento delle esposizioni al rischio di mercato e di controparte nella formula standard, cliccare qui.

3.8. EMIR: pubblicazione delle aspettative di vigilanza ESMA

CCP

In data 20 febbraio 2026, l'*European Securities and Markets Authority* (ESMA) ha pubblicato un documento contenente aspettative di vigilanza in relazione all'obbligo di rappresentatività connesso al requisito del conto attivo (*Active Account Requirement* – AAR) previsto per le controparti centrali ai sensi del Regolamento (UE) 2012/648 (*European Market Infrastructure Regulation* o EMIR).

L'Autorità rammenta che l'obbligo di rappresentatività richiede alle controparti interessate di

compensare un determinato numero di operazioni attraverso i conti attivi detenuti presso controparti centrali stabilite nell'Unione Europea. Le operazioni oggetto dell'obbligo devono riguardare le sottocategorie di derivati ritenute maggiormente rilevanti e devono essere coerenti con l'operatività che le medesime controparti attualmente compensano presso controparti centrali di secondo livello.

Il documento fornisce, in particolare, indicazioni sulle modalità attraverso cui le controparti sono tenute a conformarsi all'obbligo di rappresentatività e a darne evidenza mediante le relative comunicazioni alle autorità competenti. Esso intende altresì favorire l'armonizzazione delle prassi di vigilanza e la convergenza applicativa tra le autorità nazionali in relazione alla supervisione delle controparti soggette all'AAR, tema che ha assunto crescente rilievo nel contesto regolamentare europeo.

Nel dettaglio, l'ESMA chiarisce i criteri per l'individuazione delle sottocategorie di derivati più rilevanti ai fini dell'adempimento dell'obbligo, illustra le modalità di segnalazione delle operazioni effettuate e propone un esempio pratico volto a rappresentare un corretto adempimento degli obblighi informativi connessi alla rappresentatività.

Per consultare il documento, cliccare qui.

3.9. MiFID II/MiFIR: l'ESMA ritira le Linee guida sugli obblighi in materia di dati di mercato

Banca, Intermediario 106 Tub, SGR, SICAF, SICAV, SIM, SIS

L'*European Securities and Markets Authority* (ESMA), con decisione del 23 febbraio 2026, ha disposto il ritiro, con effetto immediato, delle proprie Linee guida relative agli obblighi in materia di dati di mercato previsti dalla disciplina MiFID II/MiFIR.

Tale decisione si inserisce nel processo di allineamento del quadro regolamentare alle nuove norme tecniche di regolamentazione concernenti l'obbligo di rendere i dati di mercato disponibili al pubblico a condizioni commerciali ragionevoli, introdotte dal Regolamento delegato (UE) 2025/1156, applicabile dal 23 novembre 2025.

Il Regolamento delegato individua le condizioni che devono essere rispettate dai gestori di mercati regolamentati e dalle imprese di investimento che gestiscono sedi di negoziazione, nonché dai dispositivi di pubblicazione autorizzati (APA), dai sistemi consolidati di pubblicazione (CTP) e dagli internalizzatori sistematici, al fine di garantire che i dati di mercato siano messi a disposizione a condizioni commerciali eque e ragionevoli, sulla base di clausole contrattuali imparziali e secondo criteri uniformi nell'ambito dell'Unione Europea.

È previsto un regime transitorio per i fornitori di dati di mercato già autorizzati anteriormente all'entrata in applicazione del regolamento delegato, i quali dispongono di tempo fino al 22 agosto 2026 per adeguare i contratti in essere ai nuovi requisiti stabiliti dalle norme tecniche di regolamentazione.

Per consultare la Decisione, cliccare qui.

* * *

Per qualsiasi chiarimento o approfondimento, non esitate a contattarci.