

Ai fondi pensione negoziali

Alle società che hanno istituito fondi pensione aperti

Ai fondi pensione preesistenti con soggettività giuridica

Trasmissione via e-mail

Oggetto: **Regolamento (UE) 2022/2554 sulla resilienza operativa digitale per il settore finanziario. Profili applicativi relativi alle segnalazioni alla COVIP da parte dei fondi pensione.**

Come noto, il 16 gennaio 2023 è entrato in vigore il Regolamento (UE) 2022/2554 sulla resilienza operativa digitale per il settore finanziario (c.d. DORA - *Digital Operational Resilience Act*, di seguito: Regolamento). Il Regolamento definisce norme uniformi a livello europeo per favorire la capacità del settore finanziario di fronteggiare il rischio relativo alle tecnologie dell'informazione e della comunicazione (*Information and Communication Technology*, ICT); le previsioni ivi contenute si applicano a decorrere dal 17 gennaio 2025.

Sono assoggettate al Regolamento le entità finanziarie di cui all'art. 2; in tale ambito rientrano anche i fondi pensione in indirizzo, con esclusione dei fondi con un numero totale di iscritti non superiore a 15 (quanto alla nozione di "iscritto" si fa rinvio all'art. 1, comma 3, del Decreto lgs. 252/2005).

Con la presente Circolare, oltre a un breve riferimento alle norme del Regolamento che più interessano i fondi pensione, si forniscono indicazioni operative riguardo alle segnalazioni alla COVIP relative ai gravi incidenti ICT, alle minacce informatiche significative, nonché al c.d. registro delle informazioni circa i servizi ICT acquisiti da fornitori terzi.

Il Regolamento disciplina, in modo particolare, i seguenti profili:

- a) gestione del rischio ICT: è richiesta l'adozione di un sistema di *governance* e di gestione del rischio ICT tale da assicurare un adeguato livello di resilienza operativa digitale;
- b) gestione, classificazione e segnalazione degli incidenti ICT: sono individuati i criteri per l'identificazione, classificazione e gestione degli incidenti ICT e delle minacce informatiche, nonché sono armonizzate le procedure di segnalazione, secondo criteri e modelli uniformi;
- c) prove di resilienza operativa digitale: è previsto lo svolgimento di programmi di test di resilienza operativa dei sistemi ICT, per valutare l'efficacia delle relative capacità di prevenzione, individuazione, risposta e ripristino;

- d) gestione dei rischi ICT derivanti da soggetti terzi: sono dettati i principi per il monitoraggio e la gestione, da parte delle entità finanziarie, dei rischi informatici derivanti da terzi e viene introdotto un regime europeo di sorveglianza sui fornitori di servizi ICT qualificati come critici. Vi sono, inoltre, obblighi di tenuta e di aggiornamento di appositi registri e di reportistica nei confronti delle autorità competenti;
- e) meccanismi di condivisione delle informazioni tra le autorità competenti nazionali ed europee.

Il Regolamento richiede alle entità finanziarie di predisporre, monitorare e aggiornare un quadro per la gestione dei rischi informatici che consenta di affrontare tali rischi attraverso una strategia di resilienza operativa digitale. Il compito di predisporre il quadro di gestione dei rischi e di verificarne l'attuazione è affidato, ai sensi dell'art. 5, paragrafo 2, del Regolamento, all'organo di amministrazione. Il monitoraggio dell'effettiva esposizione ai rischi informatici è attribuito invece dall'art. 6, paragrafo 4, a una apposita funzione di controllo interno (di seguito: "funzione di controllo ICT"). L'art. 5, paragrafo 3, prevede inoltre, con riferimento agli accordi conclusi con i fornitori terzi di servizi ICT, o l'istituzione di un apposito ruolo deputato a monitorare il rischio derivante da tali contratti o l'affidamento interno a una figura dirigenziale di rango elevato della sorveglianza sulla relativa esposizione al rischio e sulla documentazione pertinente.

Sotto il profilo generale, il Regolamento preserva il principio di proporzionalità consentendo alle entità finanziarie, ai fini del recepimento delle nuove previsioni europee, di integrare il modello di *governance* e il sistema dei controlli interni già adottati, ai sensi della propria disciplina di settore, tenendo conto della natura, della dimensione, della portata e della complessità delle loro attività.

In applicazione del suddetto principio di proporzionalità, il Regolamento prevede altresì per alcune categorie di enti di minori dimensioni, un regime semplificato quanto agli adempimenti e alle figure coinvolte. Tra i soggetti destinatari di tale regime semplificato, alla luce della natura e della finalità dei fondi pensione, è previsto uno specifico riferimento all'art. 3, paragrafo 1, n. 53 del Regolamento ai fondi pensione piccoli e, cioè, quelli con meno di cento aderenti in totale.

In linea generale, ai sensi dell'art. 16, la disciplina semplificata si traduce nella disapplicazione delle disposizioni di cui agli articoli da 5 a 15; la ricaduta principale in termini di *governance* per i fondi di minori dimensioni consiste nella loro sottrazione all'obbligo di istituire la funzione di controllo ICT, mentre resta impregiudicato quello di elaborare, monitorare e aggiornare il quadro per la gestione dei rischi ICT.

In relazione poi ai fondi pensione aperti – destinatari, come entità finanziarie, delle disposizioni del Regolamento – si fa presente che, ferma restando la competenza delle rispettive Autorità di vigilanza sui soggetti gestori, l'adeguamento alle disposizioni del Regolamento stesso in ordine all'attività di gestione del fondo pensione aperto potrà avvenire tenendo conto degli assetti societari di *governance* adottati sulla base della normativa di settore.

Con specifico riguardo alla funzione di controllo ICT, il Regolamento, nel prevederne l'istituzione, non specifica l'esatta collocazione della stessa a livello organizzativo assicurandone tuttavia un livello appropriato d'indipendenza per evitare conflitti d'interessi.

Si ritiene, dunque, che i fondi pensione possano scegliere se istituire un'apposita funzione, distinta da quelle fondamentali di cui alla Direttiva IORP II oppure se affidarla alla struttura che svolge già la funzione di gestione del rischio. Il Regolamento non individua specifici requisiti di professionalità per l'assunzione di detto incarico; in considerazione, tuttavia, dell'elevato tecnicismo dell'attività richiesta, appare opportuno che i fondi al momento della nomina del titolare della funzione di controllo ICT valutino con attenzione il grado di professionalità e le competenze nel settore del candidato.

La collocazione organizzativa scelta con riguardo alla funzione di controllo ICT non potrà in alcun modo pregiudicare l'efficace svolgimento di tutti i compiti ad essa attribuiti dal Regolamento per prevenire e contrastare l'esposizione delle entità finanziarie ai rischi ICT.

La predetta funzione non potrà, in alcun caso, essere affidata alla struttura che svolge la funzione di revisione interna.

Segnalazione dei gravi incidenti ICT e notifica volontaria delle minacce informatiche significative

Ai sensi dell'art. 19 del Regolamento, i fondi pensione segnalano alla COVIP i gravi incidenti ICT, classificati secondo il Regolamento delegato (UE) 2024/1772. Su base volontaria, inoltre, gli stessi fondi possono notificare alla COVIP le minacce informatiche significative. Tali adempimenti sono effettuati nel rispetto di quanto previsto dagli atti delegati e dalle norme tecniche di regolamentazione e attuazione del Regolamento (Regolamento delegato (UE) 2025/301; Regolamento di esecuzione (UE) 2025/302).

A questo riguardo, sono state predisposte due segnalazioni DORA: una dedicata ai gravi incidenti ICT; l'altra alle minacce informatiche significative. Per entrambe le segnalazioni, i fondi pensione utilizzano i moduli in formato ".xlsx" allegati alla presente Circolare e resi disponibili anche nell'apposita sezione del sito internet della COVIP dedicata alle segnalazioni. Una volta compilati, i moduli sono trasmessi alla COVIP alla casella di posta elettronica certificata protocollo@pec.covip.it, specificando nell'oggetto, a seconda dei casi, "DORA: segnalazione gravi incidenti ICT" ovvero "DORA: segnalazione di minacce informatiche significative".

Per la trasmissione di entrambe le segnalazioni sono fornite istruzioni operative, allegate alla presente Circolare e rese disponibili anche nella suddetta sezione del sito internet della COVIP. Per eventuali chiarimenti di ordine tecnico è possibile contattare il servizio di helpdesk al numero 06-69506307 o alla casella di posta elettronica servizio.segnalazioni.mv@covip.it.

Segnalazione del registro delle informazioni sugli accordi contrattuali sull'uso dei servizi ICT prestati da fornitori terzi

L'art. 28, paragrafo 3, del Regolamento richiede a tutte le entità finanziarie di mantenere e aggiornare un registro completo delle informazioni riguardanti gli accordi contrattuali per l'utilizzo di servizi ICT prestati da fornitori terzi. Con il Regolamento di esecuzione (UE) 2024/2956 sono state, inoltre, stabilite le norme tecniche di attuazione per quanto riguarda i modelli standard in relazione al registro delle informazioni.

Il medesimo art. 28, paragrafo 3, del Regolamento prevede, altresì, che, su richiesta, le entità finanziarie mettono a disposizione dell'autorità competente il registro delle informazioni completo o, a seconda della richiesta, determinate sezioni del registro insieme alle informazioni giudicate necessarie per consentire l'efficace vigilanza sull'entità finanziaria.

L'art. 31 del Regolamento prevede, poi, che le Autorità di supervisione europea (ESA) designino i fornitori terzi di servizi ICT che ritengono critici per le entità finanziarie, ai fini della successiva vigilanza degli stessi da parte dell'autorità di sorveglianza capofila. È inoltre previsto che la dipendenza delle entità finanziarie da terzi nel settore delle ITC è valutata sulla base delle informazioni ricevute dalle autorità nazionali competenti.

Al riguardo, le ESA hanno ritenuto necessario, onde poter effettuare tale designazione, acquisire la disponibilità dei suddetti registri. Le ESA hanno quindi emanato la Decisione dell'8 novembre 2024 nella quale hanno previsto che le autorità nazionali competenti richiedano alle entità finanziarie vigilate l'invio sistematico del registro completo e hanno indicato le scadenze e le procedure necessarie per la trasmissione del medesimo. In particolare, le autorità competenti, tra le quali la COVIP, dovranno trasmettere il registro completo all'Autorità bancaria europea (EBA), incaricata per conto di tutte le ESA, su base annuale; la prima trasmissione del registro da parte di COVIP è prevista entro il 30 aprile 2025, con data di riferimento 31 marzo 2025 per le informazioni ivi contenute.

Tenuto conto di quanto sopra, i fondi pensione in indirizzo dovranno segnalare alla COVIP il sopra indicato registro delle informazioni. A tale riguardo, la COVIP fornirà per tempo indicazioni riguardo agli schemi da utilizzare e istruzioni tecnico-operative per la segnalazione del registro mediante la piattaforma INFOSTAT-COVIP, in modo da consentire il successivo inoltro all'EBA entro la scadenza sopra riportata.

Il Presidente f.f.
Balzani Francesca Balzani
Francesca
27.02.2025
16:53:41
UTC



Allegati:

All. 1 - Modulo di segnalazione gravi incidenti ICT

All. 2 - Modulo di segnalazione minacce informatiche significative

All. 3 - Istruzioni operative per la trasmissione delle segnalazioni dei gravi incidenti ICT e delle minacce informatiche significative