Mefop

Tavolo di lavoro sui temi comunitari

2 febbraio 2022

La revisione della direttiva Iorp2

Attuazione della direttiva Iorp2

- Dicembre 2018: recepimento della direttiva
- Luglio 2020: direttive generali Covip
- Settembre 2020: DM 108/2020
- Dicembre 2020:
  - deliberazione sulla trasparenza;
  - istituzione delle funzioni fondamentali
- Gennaio 2021
  - Istruzioni FPA
- Aprile 2021:
  - prima valutazione interna dei rischi (triennale)
- Maggio/giugno 2021:
  - nuove note informative (SFDR)
  - ORA FPA (giugno)
- Luglio 2021:
  - Documento sul sistema di governo
  - Documento politiche di governance
- Marzo 2022: adeguamento statuti/regolamenti

La revisione della direttiva IORP 2

- Art. 62: entro il 13 gennaio 2023 riesame Comm UE e relazione a Parlamento e Consiglio UE
- Atteso Call for advice Comm UE a EIOPA
- Incertezza sui tempi, Call for advice non prima di giugno 2022

Le tendenze in atto

- DC modello di riferimento, ma quale DC?
- PEPP
- Adeguatezza redditi da pensione: come aumentare adesioni?
  - Best practices su adesione automatica
  - Pension dashboard
  - Best practices su Pension Tracking System

Adeguatezza dal punto di vista prudenziale e di governance

- Nuovo sistema di governo uno degli elementi più complessi
- Miglioramento governance nell'interesse degli aderenti
- Proporzionalità
- Approccio orizzontale, anche con riferimento ai profili della sostenibilità

Revisione IORP2 e sostenibilità

- Commissione UE: *Strategia per finanziare la transizione a una economia sostenibile* del 6 luglio 2021

- Principio doppia materialità

  - Migliorare la resilienza economica e finanziaria rispetto ai rischi di sostenibilità (Integrazione sistematica dei rischi di sostenibilità nel risk management - prospettiva outside-in)

  - Accelerare il contributo degli investitori alla transizione climatica, integrando gli obiettivi della Commissione UE negli investimenti (prospettiva inside-out)

Revisione IORP2 e sostenibilità

- Ricomprendere nell'ambito dei doveri fiduciari del Fp nei confronti degli aderenti/beneficiari i rischi ESG derivanti dagli investimenti

- Prima della revisione di IORP2, Comm UE incarica EIOPA di valutare se

  - ampliare concetto «migliore interesse a lungo termine degli aderenti/beneficiari» (art. 19 IORP2) includendo l'obbligo di considerare gli impatti sulla sostenibilità degli investimenti

  - Investimenti riflettano meglio le preferenze per la sostenibilità degli aderenti e beneficiari

- Incertezza su tempistica del call for advice a EIOPA

L'esempio delle compagnie di assicurazione – Modifiche al Reg. UE 2015/35

- Introduzione del concetto di Preferenze di sostenibilità: «scelta, da parte di un cliente o potenziale cliente, di integrare o meno, e se sì in che misura, nel suo investimento uno o più dei seguenti strumenti finanziari: ecosostenibili (Cfr. Reg. 2020/852-Tassonomia) e art. 8 e 9 SFDR»

- …tengono conto dell'impatto potenziale a lungo termine delle decisioni di investimento sui fattori di sostenibilità e, ove pertinente, tali decisioni riflettono le preferenze di sostenibilità dei loro clienti, prese in considerazione nel processo di approvazione del prodotto di cui all'articolo 4 del regolamento delegato (UE) 2017/2358

L'esempio delle compagnie di assicurazione – Modifiche al Reg. UE 2017/2358

- Reg. delegato UE 2017/2358 integra la direttiva sulla distribuzione dei prodotti assicurativi (2016/97) sui requisiti di governo e controllo del prodotto

- Il processo di approvazione del prodotto tiene conto di interessi, caratteristiche e obiettivi dei clienti, compresi gli eventuali obiettivi legati alla sostenibilità

- Mercato di riferimento: i soggetti che realizzano prodotti assicurativi progettano e commercializzano soltanto prodotti assicurativi compatibili con le esigenze, le caratteristiche e gli obiettivi, compresi eventuali obiettivi legati alla sostenibilità, dei clienti che appartengono al mercato di riferimento

- Canali di distribuzione: le informazioni rese disponibili dal fornitore del prodotto consentono al distributore di individuare qualunque cliente le cui esigenze, caratteristiche e obiettivi, compresi eventuali obiettivi legati alla sostenibilità, non siano compatibili con il prodotto assicurativo

L'esempio delle compagnie di assicurazione – Modifiche al Reg. UE 2017/2359

- Reg. delegato UE 2017/2359 integra la direttiva sulla distribuzione dei prodotti assicurativi (2016/97) sugli obblighi di informazione e le norme di comportamento per i distributori di prodotti assicurativi

- Preferenze di sostenibilità considerate ai fini della valutazione dei conflitti di interesse e nella consulenza al collocamento

Prospetto delle prestazioni pensionistiche

- Digitalizzazione
- Best practices su Pension Tracking System

Attività transfrontaliera

- Finora marginale
- PEPP
- Possibile anche un PEPP a livello negoziale?

Esperienza acquisita nell'applicazione e impatto sull'attività degli IORPs

- Qual è la vostra esperienza?
- Qual è l'impatto di IORP 2 sull'operatività dei FP?
- Questionario Mefop

Proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario

DORA

Elementi di carattere generale

- Proposta di regolamento presentata il 24 settembre 2020
- Parte del pacchetto della CommUE sulla finanza digitale
  - Sviluppare in sicurezza le attività digitali
- Entità finanziarie
  - Enti pensionistici aziendali e professionali (IORPs)

Ambito di applicazione

- Governance e sistema di controlli interni dei rischi ICT
- Segnalazione alle autorità competenti degli incidenti gravi connessi all'ICT
- Test di resilienza operativa digitale
- Risk management per i servizi ICT forniti da terzi
- Scambio e condivisione informazioni

Proporzionalità

- Talune previsioni alleggerite per microimprese
  - meno di 10 occupati e fatturato o totale di bilancio non superiore a 2 mln EUR.

- Consiglio UE e Parlamento UE
  - IORPs con meno di 15 aderenti in totale non in scopo
  - Piccoli IORPs: esenzioni/semplificazioni per gli schemi con meno di 100 aderenti in totale

Cos'è la resilienza operativa digitale

- Capacità dell'entità finanziaria di creare, assicurare e riesaminare la propria integrità operativa dal punto di vista tecnologico, garantendo, direttamente o indirettamente, tramite il ricordo a servizi offerti da fornitori terzi di ICT, l'intera gamma delle capacità connesse alle ICT necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità.

- Sicurezza della rete e dei sistemi informativi: capacità di resistere a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistema informativo

Rischi relativi alle ICT

- Qualunque circostanza ragionevolmente identificabile in relazione all'uso della rete e dei sistemi informativi, compresi un malfunzionamento, un superamento di capacità, un guasto, una perturbazione, un deterioramento, un uso improprio, una perdita o altri tipi di eventi, dolosi o non dolosi che, qualora si concretizzi, potrebbe compromettere la sicurezza della rete e dei sistemi informativi, di eventuali strumenti o processi dipendenti dalle tecnologie, della continuazione delle operazioni e dei processi, oppure della fornitura di servizi, pregiudicando in tal modo l'integrità o la disponibilità dei dati, del software o di eventuali altre componenti dei servizi e delle infrastrutture di ICT, o ancora causando una violazione della riservatezza, un danno alle infrastrutture fisiche di ICT o altri effetti avversi

Gestione dei rischi ICT

La gestione dei rischi ICT

- Predisposizione di quadri di gestione e di controllo interni…gestione efficace e prudente dei rischi ICT

- Organo di gestione responsabile per la definizione, l'approvazione, l'attuazione, e la vigilanza

  - Organo di gestione: persone equivalenti che gestiscono di fatto l'entità o che assolvono funzioni chiave conformemente alle pertinenti normative nazionali

  - MiFID2: l'organo (o gli organi) cui è conferito il potere di stabilire gli indirizzi strategici, gli obiettivi e la direzione generale dell'entità, che supervisiona e monitora le decisioni della dirigenza e comprende persone che dirigono di fatto l'attività dell'ente.

Le responsabilità e attività dell'organo di gestione

- Responsabilità finale gestione rischi ICT
- Definizione ruoli/responsabilità delle funzioni connesse all'ICT
- Determinazione delle soglie di tolleranza ai rischi ICT
- Approvazione/riesame piano di continuità operativa ICT e piano di ripristino in caso di disastro relativo alle ICT
- Approvazione/riesame piani di audit dei rischi ICT
- Assegnazione e riesame adeguatezza budget per resilienza digitale, inclusa la formazione
- Approvazione e riesame politica di esternalizzazione dei servizi ICT
- Riceve informazione su accordi conclusi con fornitori di servizi ICT
- Riceve informazioni sugli incidenti ICT, loro impatto, misure di risposta, di ripristino, correttivi adottati

Le responsabilità e attività dell'organo di gestione

- Istituzione di un ruolo per il monitoraggio degli accordi in caso di esternalizzazione dei servizi ICT

- Formazione periodica dell'organo di gestione sulla gestione dei rischi ICT

Quadro per la gestione dei rischi ICT

- Strategie, politiche, procedure, strumenti e protocolli…per proteggere le infrastrutture, i locali, i centri dati e le aree designate come sensibili
- Norme internazionali riconosciute e conforme agli orientamenti di vigilanza
- Separazione funzioni di gestione delle ICT, funzioni di controllo, funzioni di audit interno secondo il modello delle tre linee di difesa
- Riesame annuale del quadro di gestione dei rischi ICT, o in occasione di incidenti gravi o a seguito di istruzioni di vigilanza a valle di test di resilienza

La strategia di resilienza digitale

- Propedeutica alla definizione del quadro di gestione dei rischi ICT
  - Come la gestione dei rischi ICT sostiene gli obiettivi e la strategia commerciale dell'Entità
  - Soglie di tolleranza ai rischi ICT e obiettivi di sicurezza
  - Architettura delle ICT
- Mappatura dei rischi ICT e misure di prevenzione e di protezione
- Incidenti gravi ICT e misura delle misure di prevenzione
- Dipendenza da outsourcing per servizi ICT
- Test di resilienza operativa digitale
- Strategia di comunicazione nel caso di incidenti
- Documento politiche di governance:
  - Politica di gestione dei rischi e di revisione interna, Piano strategico ICT, Sistema informativo e presidi di sicurezza adottati, Politica delle esternalizzazioni, Piani di emergenza

La gestione dei rischi ICT

- Identificazione, classificazione e documentazione del patrimonio informativo, dei rischi, hardware, account potenzialmente a rischio, almeno annuale e ogni qualvolta cambia in modo rilevante il sistema informativo

- Misure di protezione: elaborazione di un Documento sulla politica di sicurezza ICT, accesso limitato e controllato alle reti (elaborazione di politiche, procedure e controlli sul diritto all'accesso, assicurare isolamento istantaneo in caso di incidente), politiche e protocolli di autenticazione degli accessi, elaborazione di politiche per le modifiche ai profili di ICT

- Individuazione delle attività anomale (adeguatezza delle risorse)

- Risposta e ripristino (contingency plan, parte integrante del piano di ripristino dell'entità)

Contingency plan

- Registrazione degli incidenti ICT e continuità delle funzioni critiche
- Favorire una risposta rapida ed efficace agli incidenti e favorire le azioni di ripristino
- Stima di impatti, danni e perdite
- Comunicazione ai soggetti interessati e all'autorità di vigilanza
- Piani di continuità le funzioni ICT esternalizzate
- Test dei contingency plan almeno annualmente (Covip triennale), inserimento di scenari di attacchi informatici
- Funzione di gestione delle crisi ICT in caso di attivazione dei piani di continuità
- Segnalazione all'autorità competente di costi e perdite derivanti dagli incidenti ITC

Politica di back up

- Parte del piano per la gestione dei rischi ICT
- Ampiezza dei dati oggetto di backup, frequenza minima, metodi di ripristino
- Delega ESAs e ENISA sui vari profili, conseguente regolamento delegato CommUE

Incidenti connessi all'ICT

Il processo di gestione degli incidenti

- Definizione e applicazione di un processo per la gestione degli incidenti
- Procedure di identificazione e classificazione degli incidenti
- Ruoli e responsabilità da attivare per i diversi incidenti
- Piani di comunicazione al personale, agli stakeholder esterni e mass media
- Segnalazione degli incidenti gravi all’organo di gestione
- Procedure di risposta agli incidenti
- Classificazione incidenti rimessa a Entità, criteri fissati nel regolamento da precisare ulteriormente in atto delegato

Obbligo di segnalazione degli incidenti gravi

- Segnalazione all'autorità di vigilanza degli incidenti
  - Notifica iniziale, notifica intermedia, relazione finale
- Contenuto delle segnalazioni rimesso a atto delegato
- Tempestiva comunicazione ai clienti nel caso di impatto sui lori interessi finanziari
- Possibile delega a terzi dell'obbligo di segnalazione, previa autorizzazione autorità competente

Test di resilienza

Test di resilienza

- Parte del sistema di risk management ICT, programma di test
- Svolti da soggetti indipendenti, interni o esterni
- Trattamento dei risultati
- Frequenza annuale per test su applicazioni e sistemi critici
- Test avanzati di penetrazione basati su minacce con cadenza triennale tramite tester
- Entità individuale dalle autorità nazionali, quadro test definito da regolamento delegato

Gestione dei rischi ICT derivanti da terzi

Un paio di definizioni utili

- Servizi ICT: servizi digitali e di dati forniti attraverso sistemi ICT a uno o più utenti interni o esterni, compresa la fornitura di dati, l'inserimento di dati, la conservazione di dati, i servizi di trattamento e comunicazione di dati, il monitoraggio di dati nonché i servizi commerciali e di sostegno alle decisioni basati sui dati

- Fornitore terzo di servizi ICT: impresa che fornisce servizi digitali e di dati, compresi i fornitori di servizi di cloud computing, software, servizi di analisi dei dati e centri di dati

Rischi ICT derivanti da terzi

- Entità sempre responsabile
- Registro di informazioni su tutti gli accordi contrattuali per l'uso di servizi ICT prestati da terzi
- Comunicazione autorità competente almeno annuale sul numero di nuovi accordi per l'uso di servizi ICT
- Informazione tempestiva a autorità competente su contratti relativi a funzioni critiche
  - ESAs designano i fornitori di servizi ICT critici
- Previsioni clausola audit e «Covip» e strategie di uscita per evitare perturbazioni al servizio
- Valutazione rischio di concentrazione

Grazie per l'attenzione

Mefop

Via Aniene, 14

00198 Roma

P.iva 05725581002

www.mefop.it

CONTATTI

Tel. 0648073537

Email. motroni@mefop.it

SEGUICI SU

mefop-spa

@MEFOP

Mefop

MefopFondiPensione