COVIP
COMMISSIONE DI VIGILANZA
SUI FONDI PENSIONE

COVIP Protocollo Generale
Uscita Prot. n. 0001247/26 del 12/03/2026
SERVIZIO VIGILANZA FONDI PENSIONE

Ai fondi pensione negoziali

Alle società che hanno istituito fondi pensione aperti

Alle imprese di assicurazione che hanno istituito PIP ex D.lgs. 252/2005

Ai fondi pensione preesistenti

Trasmissione via e-mail

Oggetto: Furti di identità digitale. Indicazioni al settore.

Con la presente Circolare si richiama l'attenzione delle forme pensionistiche in indirizzo sui presidi che le stesse sono tenute ad implementare nel caso di utilizzo di tecnologie informatiche, secondo quanto previsto dalle Istruzioni di vigilanza in materia di trasparenza, di cui alla Deliberazione del 22 dicembre 2020 (di seguito, Istruzioni).

Le richiamate Istruzioni, con particolare riferimento alla gestione telematica dei rapporti tra le forme pensionistiche complementari e gli aderenti/beneficiari, prevedono che le stesse siano dotate di sistemi informatici che consentano, attraverso l'accesso ad aree riservate dei siti *web*, di effettuare, tra l'altro, la trasmissione di richieste di operazioni connesse al rapporto di partecipazione nonché di accedere ai dati relativi alla posizione individuale. Nella predisposizione delle modalità di accesso alle aree riservate dei siti *web*, la forma pensionistica complementare adotta i presidi di sicurezza che ritiene idonei al fine di garantire la tutela della riservatezza e la protezione dei dati e delle informazioni. Il livello di sicurezza deve essere proporzionato alle operazioni e funzioni messe a disposizione dell'aderente.

Sotto il profilo generale, si ricorda inoltre che l'utilizzo di tecnologie informatiche comporta un necessario e continuo processo di adeguamento da parte delle forme pensionistiche complementari, le quali riportano le relative valutazioni in merito alle iniziative da assumere nel piano strategico sulle tecnologie dell'informazione e della comunicazione da inserire nel 'Documento politiche di *governance*'.

Avuto riguardo alle implicazioni derivanti dalla fruizione delle aree riservate da parte degli aderenti, si fa presente che la Scrivente è venuta recentemente a conoscenza di episodi di furti di identità digitale che potrebbero avere anche un impatto sugli strumenti adottati dalle forme previdenziali determinando, in primo luogo, accessi non autorizzati alle aree riservate se non anche modifiche dei dati personali degli iscritti e l'attivazione dei processi finalizzati al pagamento di prestazioni indebite.

Laddove tali strumenti siano utilizzati, senza ulteriori forme di controllo, per modificare i dati di contatto e le coordinate bancarie, per l'iscritto risulterebbe difficile avere immediata evidenza delle eventuali operazioni effettuate, e conseguentemente attivarsi a tutela dei propri interessi.

VIA PIEMONTE, 60
00187 ROMA
Tel. +39 06.69506.1
Fax +39 06.69506.304
protocollo@pec.covip.it
www.covip.it

Si richiede, pertanto, alle forme pensionistiche di porre in essere ogni valida forma di controllo finalizzata alla verifica dell'esistenza di eventuali anomalie nell'utilizzo delle tecnologie informatiche di cui si avvalgono, nonché di individuare le conseguenti attività da implementare al fine di una adeguata gestione dei rischi informatici, assicurando *standard* di sicurezza maggiormente elevati e in linea con la normativa di riferimento.

In tale contesto andrebbe valutata anche l'opportunità di diffondere contenuti informativi tra gli aderenti, volti a richiamarne l'attenzione sui fenomeni in parola, anche avvalendosi del sito *web* della forma pensionistica, rafforzando così la consapevolezza delle condotte rischiose e sensibilizzando azioni di prevenzione da parte dei medesimi.

Avuto riguardo, inoltre, alle modalità di gestione dei rischi ICT, si ricorda che la normativa europea sulla resilienza operativa digitale per il settore finanziario, Regolamento europeo (UE) 2022/2554 e relativa normativa tecnica di attuazione, agli artt. 17 e ss. del citato Regolamento individua i criteri per l'identificazione, classificazione e gestione degli incidenti ICT e delle minacce informatiche, nonché introduce per le forme pensionistiche l'obbligo di segnalare alla COVIP i gravi incidenti ICT e, su base volontaria, di procedere alla segnalazione delle minacce informatiche significative (art. 19 del Regolamento citato).

Si chiarisce, nel merito, che le fattispecie sopra descritte, originate dal furto dell'identità digitale degli aderenti, comportando l'attivazione dei processi informatizzati della forma pensionistica, sono idonee a integrare un grave incidente informatico ai sensi dell'art. 19 del Regolamento DORA e, come tale, soggetto alla segnalazione alla COVIP, secondo le modalità definite nella Circolare prot. n. 1154/25 del 27/2/2025, che ha chiarito i profili applicativi derivanti dalla citata normativa europea sulla resilienza operativa digitale.

Il Presidente

Mario Pepe

MARIO
PEPE
12.03.2026
12:27:49
GMT+01:00