

Gentile Cliente,

Desideriamo informarla che la nostra Società di Gestione del Risparmio, in data odierna, ha ricevuto una comunicazione in merito ad un attacco informatico che ha interessato i sistemi informativi di un proprio fornitore di servizi amministrativi. A seguito delle verifiche tecniche avviate dal fornitore con il supporto di esperti di cybersecurity, il fornitore ha comunicato di avere individuato evidenze di esfiltrazione, da parte di un soggetto terzo, di file utilizzati nell'ambito dei servizi prestati alla nostra organizzazione.

1. Quali dati sono stati coinvolti?

Le categorie, il volume e il contenuto dei file coinvolti sono ancora in corso di accertamento da parte del fornitore, tuttavia il fornitore ritiene che i documenti esfiltrati dal terzo contenessero dati personali. Al momento non si è a conoscenza di alcuna pubblicazione o divulgazione al pubblico dei dati coinvolti. Il fornitore ci ha comunicato che le indagini sono ancora in corso.

Si precisa che l'incidente:

- non ha riguardato la struttura informatica interna di 8a+ Investimenti SGR;
- non ha riguardato in alcun modo i prodotti finanziari gestiti dalla nostra Società: gli strumenti finanziari e la liquidità sono depositati presso la banca depositaria (non coinvolta nell'incidente informatico) e di conseguenza i Suoi investimenti presso 8a+ non sono incorsi in alcun rischio.

2. Cosa abbiamo fatto e cosa stiamo facendo

Il fornitore ci ha comunicato di aver attivato i propri protocolli per mettere in sicurezza l'accesso all'ambiente interessato e di aver adottato misure di contenimento.

La nostra Società ha provveduto, appena ricevuta la comunicazione dell'accaduto da parte del fornitore, conformemente a quanto previsto dalle nostre procedure interne e dalla normativa di riferimento, a:

- Segnalare l'incidente a Banca d'Italia (Autorità di Vigilanza competente ai sensi della normativa applicabile).
- Notificare l'accaduto al Garante per la Protezione dei Dati Personali.

3. Quali sono i potenziali rischi e cosa Le consigliamo di fare

L'esfiltrazione di questi dati potrebbe esporLa a tentativi di frode mirati: [attenzione al Phishing e Smishing.](#)

Per mitigare qualsiasi rischio, Le raccomandiamo caldamente di prestare la massima attenzione a e-mail, SMS o telefonate sospette che richiedono l'inserimento di password, PIN o codici di sicurezza. Ricordi che la nostra SGR non le chiederà mai queste credenziali via e-mail o telefono.

Per qualsiasi dubbio, chiarimento o per ricevere assistenza dedicata, può contattare il nostro team di supporto al seguente indirizzo e-mail: dpo@ottoapiu.it.

9 ottobre 2026

8a+ Investimento SGR S.p.A.