Firenze, 10 novembre 2026

Gentile Cliente,

Oggetto: comunicazione di violazione dei dati personali ai sensi dell'art. 34 del Regolamento (UE) 2016/679

Le scriviamo per informarLa, in modo diretto e completo, di un fatto che riguarda anche i Suoi dati personali. Un fornitore informatico al quale affidiamo alcuni servizi amministrativi ha subito un attacco informatico e alcuni documenti che lo riguardano sono stati copiati da persone non autorizzate. I nostri sistemi non sono stati toccati, ma i dati sono i Suoi e vogliamo che Lei sappia da noi che cosa è accaduto, quali dati sono coinvolti, che cosa abbiamo fatto, che cosa può fare per proteggersi e a chi rivolgersi per qualsiasi domanda.

Che cosa è successo

L'incidente non ha interessato i sistemi informatici di *L&B Capital SGR S.p.A.* (di seguito la "SGR"), bensì un server dedicato al trasferimento di file gestito da *Xchanging Italy S.p.A.* (di seguito il "Fornitore"), società specializzata nella prestazione di servizi informatico-amministrativi in outsourcing, di cui si avvalgono numerosi operatori del risparmio gestito italiano e che tratta dati personali per conto della SGR. L'evento ha pertanto una rilevanza settoriale, in quanto coinvolge un fornitore condiviso da più intermediari, e non è riconducibile a una compromissione dei sistemi informatici della SGR.Tra il 30 settembre e il 2 ottobre 2026 un soggetto terzo non autorizzato è riuscito ad accedere a quel server, usato dal Fornitore per scambiare con noi documentazione operativa, forzandone le credenziali di accesso, e ha copiato una parte dei file che vi erano custoditi. Il Fornitore ha rilevato l'accesso e lo ha bloccato il 2 ottobre 2026; ci ha informati dell'accaduto il 9 ottobre 2026 e il 14 ottobre 2026 ci ha confermato che tra i file copiati ve ne sono alcuni contenenti dati personali di clienti della SGR, tra cui i Suoi. I servizi che Le forniamo non hanno subito alcuna interruzione. Anche se il fatto è avvenuto presso il Fornitore, i dati sono i Suoi e il compito di informarLa e di tutelarLa è nostro: per questo Le scriviamo. I Suoi investimenti non sono stati toccati: le Sue posizioni, il loro valore e l'operatività dei fondi sono rimasti invariati al momento, e la gestione del Suo patrimonio prosegue regolarmente, ovviamente ove registassimo una qualche anomalia sarà nostra premura informarla e prendere le dovute precauzioni.

Quali dati La riguardano

Le analisi svolte sui file copiati, che il Fornitore ha completato e che stiamo verificando, confermano che i documenti contengono potenzialmente dati identificativi (nome, cognome, data e luogo di

nascita, codice fiscale copia di documenti di riconoscimento), dati di contatto (indirizzo postale, indirizzo di posta elettronica, numero di telefono), informazioni relative ai Suoi investimenti presso la SGR, quali saldi, movimenti e documenti sulle posizioni, e le coordinate bancarie del conto collegato alle Sue sottoscrizioni. Se Lei non è intestatario di un rapporto con la SGR, i Suoi dati compaiono in documenti relativi al rapporto di un nostro cliente, ad esempio quale cointestatario, delegato, legale rappresentante o titolare effettivo; non per tutte le posizioni sono stati esfiltrate le solite informazioni, per avere cognizione della propria informazione la invitiamo a contattarci.

Non risultano, al momento, coinvolti codici di accesso, password e dati di carte di pagamento.

Che cosa può accadere

Non abbiamo, a oggi, alcuna evidenza che i dati copiati siano stati pubblicati o utilizzati, e il Fornitore sta monitorando costantemente le fonti in cui potrebbero comparire. Vogliamo però essere chiari con Lei: chi li possiede conosce la Sua identità, i Suoi recapiti, l'esistenza e l'entità del Suo rapporto con la SGR e le coordinate del Suo conto. Queste informazioni potrebbero essere usate per contattarLa fingendosi la SGR, la Sua banca o un altro intermediario e ottenere da Lei codici, password o disposizioni di pagamento, per tentare di disporre addebiti non autorizzati sul Suo conto, oppure per tentare di assumere la Sua identità presso terzi. Il rischio principale è quindi quello di comunicazioni fraudolente costruite in modo credibile grazie ai Suoi dati.

Che cosa Le chiediamo di fare

Le chiediamo alcune semplici attenzioni. Diffidi di telefonate, messaggi e posta elettronica che facciano riferimento ai Suoi investimenti e Le chiedano di fornire codici, password, dati di carte o di effettuare pagamenti, anche se chi La contatta conosce il Suo nome, il Suo codice fiscale, le Sue coordinate bancarie o l'importo delle Sue posizioni. La SGR non Le chiederà mai, per telefono, per messaggio o per posta elettronica, credenziali di accesso, codici di sicurezza o disposizioni di trasferimento di denaro, e non Le chiederà mai di modificare le coordinate bancarie per i rimborsi con questi mezzi. Non apra collegamenti né allegati contenuti in messaggi che non ha richiesto. Se riceve un contatto sospetto, interrompa la conversazione e ci chiami ai recapiti ufficiali indicati in questa lettera o sul nostro sito, mai ai numeri forniti da chi La contatta. Controlli con regolarità i movimenti del Suo conto corrente, i Suoi rendiconti e le comunicazioni dell'area riservata, e segnali subito alla Sua banca e a noi addebiti, operazioni o variazioni che non riconosce. Se utilizza la stessa password del Suo indirizzo di posta elettronica anche per altri servizi, Le consigliamo per prudenza di cambiarla. Se dovesse subire un tentativo di frode, lo segnali alle autorità e ce ne dia notizia: potremo aiutarLa.

Che cosa abbiamo fatto

Appena informati, abbiamo sostituito tutte le credenziali di accesso al server coinvolto e abbiamo ottenuto dal Fornitore l'elenco dei documenti copiati, che stiamo verificando. Il Fornitore ha messo in sicurezza il sistema, ha rafforzato le misure di sicurezza dell'ambiente interessato, ha svolto un'indagine tecnica con specialisti di analisi forense e mantiene un monitoraggio costante delle fonti in cui i dati sottratti potrebbero essere diffusi, senza che a oggi siano emersi segnali di diffusione.

Abbiamo notificato la violazione al Garante per la protezione dei dati personali e a Banca d'Italia. Abbiamo contestato formalmente al Fornitore quanto accaduto. Stiamo informando tutte le persone coinvolte con questa stessa comunicazione.

A chi rivolgersi

Per qualsiasi domanda su questa comunicazione, e per sapere quali dei Suoi dati risultano coinvolti, può scrivere all'indirizzo privacy@lbcapitalsgr.it o telefonare al numero 055 263331. Il personale che Le risponderà è stato istruito su quanto accaduto e potrà darLe le informazioni disponibili sulla Sua posizione. Se ha sottoscritto tramite la Sua banca o il Suo consulente, può rivolgersi anche a loro: sono stati informati e potranno indirizzarLa.

Come riconoscere questa comunicazione

Questa lettera Le viene inviata per posta elettronica, all'indirizzo in nostro possesso o a quello che il Suo collocatore ci ha fornito ai soli fini di questa comunicazione, oppure per posta ordinaria all'indirizzo che ci ha comunicato. Non contiene collegamenti da aprire né richieste di dati. Può verificarne l'autenticità consultando la sezione Avvisi del sito www.lbcapitalsgr.it o chiamando i recapiti ufficiali della SGR.

Aggiornamenti

Le verifiche sui documenti coinvolti sono ancora in corso. Se emergeranno elementi che modificano quanto Le abbiamo scritto, in particolare sulle categorie di dati o sulla loro eventuale diffusione, La informeremo. Pubblicheremo inoltre gli aggiornamenti nella sezione "*Avvisi*" del sito www.lbcapitalsgr.it.

I Suoi diritti

Lei ha il diritto di proporre reclamo al Garante per la protezione dei dati personali, Piazza Venezia 11, 00187 Roma, protocollo@pec.gpdp.it. Resta ferma la possibilità di esercitare in ogni momento i diritti previsti dagli articoli 15 e seguenti del Regolamento (UE) 2016/679 scrivendo ai recapiti sopra indicati.

Ci dispiace sinceramente per il disagio che questo episodio, avvenuto presso un nostro fornitore, può comportarLe. La fiducia che ci accorda è ciò a cui teniamo di più: per questo abbiamo scelto di dirLe subito tutto ciò che sappiamo, anche se le verifiche non sono concluse, e di esigere dal Fornitore il pieno rispetto degli impegni di sicurezza assunti con noi.

Continueremo a tenerLa informata e a gestire il Suo patrimonio con la cura di sempre.

Restiamo a Sua disposizione.

L&B Capital SGR S.p.A.
Tommaso Federici
Amministratore Delegato

