Zurigo, agosto 2023

I gestori di patrimoni e la revisione della legge sulla protezione dei dati - Effetti limitati del trattamento dei dati previsto dalla legge

(Guida pratica per gli operatori del settore dei servizi finanziari redatta da Alexander Rabian, Melanie Käser e Mathias Stauffacher, avvocati dello studio Streichenberg und Partner[1])

Trattamento dei dati per obbligo di legge

Mentre nella precedente legge sulla protezione dei dati il trattamento dei dati personali sulla base di un obbligo legale era una giustificazione generale per il trattamento dei dati personali (art. 27 cpv. 1 vLPD), la nuova legge sulla protezione dei dati (revLPD), entrata in vigore il 1° settembre 2023, richiede un approccio differenziato sotto alcuni aspetti.

I principali requisiti legali per i gestori patrimoniali in materia di trattamento dei dati dei clienti si trovano nelle seguenti leggi sulla vigilanza dei mercati finanziari (ai sensi dell'art. 3 cpv. 1 LFINMA):

- Legge sui servizi finanziari del 15 giugno 2018 (LSerFi).
- Legge sul riciclaggio di denaro del 10 ottobre 1997 (LRD).
- Legge sugli istituti finanziari del 15 giugno 2018 (LIsFi)
- Legge sugli investimenti collettivi di capitale del 23 giugno 2006 (LICol)
- La legge sull'infrastruttura finanziaria del 19 giugno 2015 (LInFi).

Tutte queste leggi federali in senso formale sono accompagnate da ordinanze di attuazione (emanate dal Consiglio federale e, in alcuni casi, anche dall'Autorità federale di vigilanza sui mercati finanziari FINMA), che forniscono anche una base giuridica per il trattamento dei dati personali.

Tra le leggi citate, la LRD e la LSerFi sono quelle che contengono le disposizioni più ampie sul trattamento dei dati personali dei "clienti" in senso lato, ossia delle

[1]Il presente articolo è stato tradotto da ASG dall'originale documento redatto da Alexander Rabian, Melanie Käser e Mathias Stauffacher. In caso di contraddizioni o discrepanze tra le due versioni, la versione originale tedesca fa fede. Link alla versione tedesca

Streichenberg und Partner
Stockerstrasse 38
8002 Zürich
Schweiz
T. +41 44 208 2525
www.streichenberg.ch

parti contraenti e delle persone ad esse collegate (ad esempio, aventi diritto economico / detentori del controllo, procuratori e altre persone legate per motivi familiari, personali o d'affari).

Per il trattamento dei dati personali dei dipendenti della propria azienda esistono inoltre requisiti ai sensi delle leggi sui mercati finanziari (ad es. "Garanzia di attività irreprensibile"), nonché della regolamentazione sul rapporto di lavoro e sulla previdenza sociale.

Normativa basata sul rischio

Una delle caratteristiche della legge svizzera sulla vigilanza dei mercati finanziari è quella di prescrivere un cosiddetto "approccio basato sul rischio" per molte aree normative. Questo principio di base deve essere osservato anche nel determinare quali dati personali devono essere trattati da un consulente /gestore patrimoniale in base ai requisiti di legge.

La legge (ad esempio la LRD e le sue disposizioni attuative, come l'ORD-FINMA) non determina in modo esaustivo quali dati personali debbano/possano essere trattati in caso di regolamentazione basata sul rischio. La legge stabilisce dei principi (come il principio " Know your Customer ") e stabilisce che l'istituto finanziario regolamentato deve adottare tutte le misure necessarie (compreso il trattamento dei dati personali) per garantire che le fattispecie dichiarate illegali o indesiderabili dalla legge non si concretizzino. L'istituto finanziario regolamentato deve identificare, registrare sistematicamente e controllare i rischi di comportamenti non autorizzati o indesiderati generati dalla sua attività (autorizzata), ossia deve condurre un'efficace gestione del rischio.

Sulla base della formulazione astratta delle leggi, non è possibile determinare in modo definitivo quali dati personali di clienti, partner contrattuali, dipendenti e fornitori di servizi un istituto finanziario regolamentato o un intermediario finanziario regolamentato debba trattare per adempiere agli obblighi di legge. A questo proposito, le leggi non stabiliscono alcun "valore massimo" dei dati personali da trattare, ma definiscono piuttosto - se mai - standard minimi normativi.

A causa della normativa basata sul rischio, ogni fornitore di servizi finanziari deve determinare autonomamente, tra le altre cose, quali dati personali intende trattare per soddisfare i requisiti di legge. Nel fare ciò, essi hanno un notevole potere discrezionale.

I gestori patrimoniali autorizzati dalla FINMA devono disporre di un sistema di direttive ben sviluppato, che deve essere approvato dalle autorità di vigilanza (FINMA e organismi di vigilanza) e sottoposto a un audit periodico da parte delle società di revisione incaricate, al fine di garantire che sia concepito in modo da soddisfare adeguatamente i requisiti legali. La verifica non riguarda il superamento dei requisiti legali per l'identificazione, la misurazione e la gestione dei rischi, ma piuttosto il loro mancato rispetto. Oggetto delle istruzioni deve essere anche un sistema di controllo interno ("SCI") adeguato alla portata e alla complessità delle

operazioni aziendali, nonché ai rischi generati dalle operazioni aziendali per gli investitori e in particolare per l'integrità e la reputazione della piazza finanziaria. La gestione di un tale sistema di controllo interno richiede anche il trattamento di dati personali relativi a clienti, organi direttivi, dipendenti, ma anche dei dipendenti con funzioni chiave presso partner di outsourcing e persino presso fornitori.

Il gestore patrimoniale autorizzato, i suoi organi coinvolti nella gestione, i dipendenti e le persone ausiliarie esterne devono sempre rispettare il principio della garanzia di attività irreprensibile e di una buona reputazione. Le persone coinvolte nell'azienda devono assicurarsi di non esercitare alcuna influenza dannosa sul requisito di garanzia di attività irreprensibile. Il requisito di garanzia di attività irreprensibile richiede il trattamento dei dati personali dei dipendenti in misura che va oltre l'ambito delle aziende senza un corrispondente obbligo di garanzia legale. L'ambito esatto deve essere determinato dal gestore autorizzato in applicazione dell'approccio basato sul rischio. Inoltre, i dati personali dei dipendenti, che si occupano dei clienti, devono essere trattati sulla base della loro sufficiente conoscenza della legge e delle loro conoscenze specialistiche.

Anche nel caso di utilizzo dei dati personali raccolti e quindi trattati in adempimento di obblighi legali per finalità di marketing, il corrispondente trattamento dei dati da parte dei consulenti alla clientela e dei gestori patrimoniali deve basarsi su requisiti legali. Per quanto riguarda l'offerta di strumenti finanziari, la LSerFi stabilisce che i dati personali degli investitori potenziali ed effettivi sono trattati nell'ambito della segmentazione della clientela da effettuare (compresi eventuali opting-in o opting-out), dell'adempimento degli obblighi informativi e dell'adempimento dei requisiti per l'offerta di strumenti finanziari.

In sintesi, si può affermare che la regolamentazione dei servizi finanziari basata sul rischio concede agli istituti finanziari e agli intermediari finanziari un'ampia autonomia nel determinare quali dati personali devono o dovrebbero essere trattati. L'approccio normativo basato sul rischio prescrive anche il trattamento dei dati personali che richiedono una protezione speciale (forse con l'eccezione di dati sanitari molto specifici) e prevede anche il trattamento dei profili della personalità (in particolare di clienti, dipendenti, persone chiave presso i partner di outsourcing) con i dati personali che richiedono una protezione speciale (ad esempio, informazioni sulle attività politiche nel quadro delle norme sul trattamento delle persone politicamente esposte).

Applicabilità dei principi fondamentali della nLPD

I seguenti principi giuridici di base sulla protezione dei dati si applicano anche se il responsabile del trattamento dei dati ha la giustificazione del trattamento dei dati prevista dalla legge:

- Principio di liceità (art. 6 cpv. 1 nLPD): nel caso di un gestore patrimoniale autorizzato, soddisfatto da ampie basi giuridiche e da interessi pubblici o privati prevalenti in un ampio quadro di riferimento;
- Principio della limitazione dello scopo (utilizzo conforme allo scopo, art. 6 cpv. 1 nLPD): i dati possono essere utilizzati solo per gli scopi previsti

dalla legge senza dover rispettare ulteriori disposizioni della nLPD. Tuttavia, questi sono molto estesi;
- Principio di proporzionalità (art. 6 cpv. 2 nLPD): i dati possono essere trattati solo nella misura necessaria allo scopo. Il regolamento basato sul rischio stabilisce un quadro di riferimento ampio e lascia al gestore patrimoniale la propria discrezionalità;
- Buona fede (Art. 6 cpv. 2 nLPD): l'adempimento dei requisiti di legge è sempre un trattamento dei dati in buona fede. Questo principio limita il trattamento dei dati all'applicazione appropriata di un approccio basato sul rischio, ma lascia al responsabile del trattamento dei dati un'ampia discrezionalità;
- Obbligo di trasparenza/dovere di informazione (art. 6 cpv.3 nLPD / art. 19 e segg. nLPD): i dati trattati sono ottenuti per uno scopo riconoscibile. Questo requisito è soddisfatto semplicemente informando clienti, investitori, ecc.;
- Impostazioni predefinite favorevoli alla protezione dei dati (art. 7 nLPD; "Privacy by Design/Default"): Questo principio viene relativizzato dalle leggi di controllo applicabili all'interno di un quadro molto ampio. Spesso le impostazioni predefinite favorevoli alla protezione dei dati sono in conflitto con gli obiettivi e le finalità della normativa;
- Accuratezza dei dati (Art. 6 cpv. 5 nLPD): le leggi di vigilanza applicabili prevedono che il gestore patrimoniale autorizzato debba essere convinto dell'esattezza dei dati personali trattati. Il trattamento intenzionale o negligente dei dati personali influisce sul requisito di garanzia di attività irreprensibile. Alcune leggi sulla vigilanza dei mercati finanziari prevedono una verifica basata sul rischio della tempestività e dell'esattezza dei dati personali trattati;
- Sicurezza dei dati (art. 8 nLPD): le direttive devono prevedere requisiti adeguati di sicurezza dei dati.

Registro delle attività di trattamento (Art. 12 nLPD)

Le attività di trattamento dei dati personali svolte da un gestore patrimoniali derivano dalle sue direttive. Il registro delle attività di trattamento dei dati deve essere redatto eccezion fatta per i casi in cui l'azienda abbia meno di 250 dipendenti e non vengano trattati dati personali particolarmente sensibili o venga effettuata una profilazione ad alto rischio.

Nondimeno, poiché i gestori patrimoniali trattano regolarmente dati personali particolarmente sensibili nell'ambito dei loro obblighi legali, in particolare ai sensi della LRD, e possono anche effettuare una profilazione ad alto rischio, allo stato attuale delle conoscenze è consigliabile tenere un registro delle attività di trattamento dei dati.

Non è necessario, quando si trattano dati personali elettronicamente, tenere registri dettagliati e minuziosi di ogni singolo dato trattato ("elenchi con campi di dati"). Soprattutto quando si attua un approccio basato sul rischio al trattamento

dei dati personali ai fini normativi, non vengono trattate in modo schematico caratteristiche identiche per tutti i clienti, gli aventi diritto economico o i procuratori. L'elenco delle attività di trattamento non deve essere un documento separato dal corpus delle direttive, ma deve essere integrato nel corpus delle direttive.

Comunicazione di dati personali all'estero (art. 16 e segg. nLPD)

Comunicazione di dati personali all'estero non è di per sé vietata. L'elaborazione dei dati su server e strutture di archiviazione dati situati all'estero è quindi ancora possibile per i gestori patrimoniali.

L'allegato I dell'ordinanza sulla protezione dei dati riveduta (nLPD) elenca gli Stati e i territori che, secondo la valutazione del legislatore, presentano un livello adeguato di protezione dei dati. Oltre agli Stati del SEE, anche numerosi altri Stati sono certificati come aventi un livello adeguato di protezione dei dati. Tuttavia, ciò non vale per gli Stati Uniti. L'elaborazione dei dati su server situati negli Stati Uniti è quindi consentita solo in misura limitata.

Obbligo di informare sulla raccolta di dati personali (art. 19 e segg. nLPD)

La trasparenza del trattamento dei dati comprende anche l'obbligo di informare adeguatamente l'interessato sul trattamento dei dati personali. L'art. 19 della legge rivista sulla protezione dei dati si applica all'obbligo di fornire informazioni nell'acquisizione dei dati. Nell'ambito dei loro obblighi legali (in particolare ai sensi della LRD), i gestori patrimoniali non solo ottengono informazioni sui clienti, ecc. dal cliente, ma utilizzano anche altre fonti di dati (ad esempio per verificare la plausibilità dei dati raccolti dal cliente). Va da sé che i dati che il gestore patrimoniale riceve direttamente dal cliente vengono elaborati.

Ai sensi dell'art. 20 nLPD, l'obbligo di fornire informazioni sulla raccolta dei dati non si applica se il trattamento dei dati corrispondenti è previsto dalla legge. Ciò vale in particolare per il trattamento dei dati dei clienti e dei dati personali dei dipendenti. Per quanto riguarda i clienti, l'obbligo di informazione non si applica in larga misura a causa del segreto professionale. Anche se i dati personali vengono divulgati all'estero in un modo consentito dall'art. 16 nLPD (ad es. memorizzati su un server), gli interessati non devono essere informati in modo specifico.

Una dichiarazione completa e dettagliata sulla protezione dei dati nei confronti dei clienti e dei dipendenti non è quindi necessaria per i gestori patrimoniali che operano in modo tradizionale. Tuttavia, nell'ambito dei requisiti generali di trasparenza, è opportuno informare i clienti sull'ampio trattamento dei dati previsto dalla legge. È importante che il gestore patrimoniale dichiari in questa informativa che la sua società è il responsabile del trattamento dei dati.

Tuttavia, i gestori patrimoniali che trattano dati personali in misura maggiore, come ad esempio i dati personali dei candidati a un posto di lavoro, sono obbligati per legge a informare queste persone sul tipo, la portata e la durata del trattamento dei dati.

Tuttavia, i gestori patrimoniali che operano con un modello di business fortemente o solo parzialmente basato sulla comunicazione e sulla fornitura di servizi via web hanno ulteriori obblighi di informazione. L'integrazione delle applicazioni web nella gestione degli asset richiede il trattamento di dati personali (ad esempio, registrazioni elettroniche dell'utilizzo dell'applicazione web), che non è coperto dai requisiti di legge ma deriva dallo specifico modello di business e dai corrispondenti accordi contrattuali. Questi gestori patrimoniali trattano i dati personali in misura superiore ai requisiti di legge e hanno di conseguenza obblighi di informazione più ampi che rendono necessaria una dichiarazione completa sulla protezione dei dati.

Le disposizioni relative all'uso dei "cookie" sui siti web rimangono invariate. L'obbligo di fornire informazioni rimane in vigore. La nuova legge sulla protezione dei dati non richiede il consenso.

Trattamento dei dati per conto delle banche

Nell'ambito della delega di compiti formali ai sensi della LRD, i gestori patrimoniali autorizzati trattano regolarmente dati personali per conto delle banche "deleganti" ("delega" secondo la CDB). Ciò comporta un trattamento di dati personali per conto del gestore patrimoniale, che costituisce al contempo un trattamento di dati proprio prescritto dalla legge.

Poiché si tratta di un trattamento coincidente di dati personali che il gestore patrimoniale deve trattare anche lui stesso in conformità ai requisiti di legge, non sono necessarie particolari precauzioni da parte del gestore patrimoniale per il trattamento dei dati commissionato.

Se il gestore patrimoniale elabora dati personali e li trasmette alle banche mandanti, il che avviene normalmente con la "delega" degli obblighi formali di due diligence secondo la CDB, ma anche con un ulteriore trattamento dei dati secondo le modalità previste (ad es. preparazione del KYC), il cliente interessato deve essere informato di conseguenza. Ciò può essere fatto in modo generale nell'ambito delle informazioni generali sul cliente.

Divulgazione di dati a terzi, in particolare a responsabili del trattamento commissionati

Se il gestore patrimoniale fa elaborare i dati personali a terzi in Svizzera o all'estero, deve garantire nei relativi contratti che l'elaborazione dei dati da parte del responsabile incaricato avvenga solo in modo conforme alle norme applicabili al gestore patrimoniale. A tal fine, i contratti devono contenere clausole di protezione dei dati adeguate.

In particolare, il gestore patrimoniale deve anche assicurarsi, tramite apposite clausole, che l'incaricato del trattamento degli ordini abbia preso le necessarie precauzioni per tutelare il segreto professionale. In questo caso si applicano i requisiti di vigilanza della FINMA in materia di outsourcing.

Obbligo di informazione in caso di processo decisionale individuale automatizzato (art. 21 nLPD)

Le classificazioni del rischio ai sensi della LRD o delle attività di investimento ai sensi della LSerFi (classificazione basata su questionari) non costituiscono "decisioni individuali automatizzate" ai sensi della nLPD, anche se i sistemi informatici forniscono risultati a tale scopo. A causa dei requisiti normativi, le persone responsabili hanno la responsabilità personale di determinare le decisioni corrispondenti. I "sistemi automatizzati" utilizzati sono solo degli ausili.

Valutazione dell'impatto sulla protezione dei dati (art. 22 nLPD).

Questo obbligo non si applica se il trattamento dei dati viene effettuato sulla base di un obbligo legale (cpv. 4).

Notifica di violazioni della sicurezza dei dati (art. 24 nLPD) - procedura conforme alla comunicazione della FINMA.

I gestori patrimoniali svolgono un'attività sottoposta a vigilanza. I requisiti legali per la gestione delle violazioni della sicurezza dei dati previsti dalla nLPD sono quindi in parte ampiamente superati dai requisiti di vigilanza dell'autorità di autorizzazione FINMA. In particolare, in caso di cyber-attacchi alle cosiddette funzioni critiche (che comprendono anche i sistemi IT), devono essere rispettati i requisiti della comunicazione FINMA sulla vigilanza 05/2020. L'organo principale da informare in questo caso è l'OV. La FINMA deve essere informata anche nelle procedure di autorizzazione in corso.

Le "semplici" violazioni interne della sicurezza dei dati (ad esempio l'accesso ai dati dei clienti da parte di collaboratori non autorizzati) devono essere segnalate all'IFPDT se possono comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata. In pratica, tuttavia, questo rischio elevato esiste solo se esiste una minaccia di "fuga di dati verso l'esterno". In questi casi, tuttavia, è necessario informare prima all'organismo di vigilanza competente. L'informazione dell'IFPDT deve essere coordinata con l'autorità di vigilanza.

I principi della procedura devono essere disciplinate nelle direttive.

Diritto all'informazione (art. 25 e segg. nLPD):

Si tratta in particolare del rapporto tra il diritto all'informazione ai sensi della legge sulla protezione dei dati e gli obblighi di informazione e di rendicontazione ai sensi della LSerFi. A causa del segreto professionale sancito dalla LIsFi, i dati personali non possono essere divulgati a persone diverse dal rispettivo titolare del segreto, a meno che non vi siano particolari obblighi di divulgazione previsti dalla legge. Le leggi sulla vigilanza prevedono anche ulteriori motivi per rifiutare, limitare o ritardare (art. 26 cpv. 2 nLPD) la divulgazione di informazioni. Si tratta di informazioni

relative all'adempimento dell'obbligo di segnalazione ai sensi della LRD e di altri obblighi di segnalazione del diritto prudenziale, divieti di informazione basati su disposizioni di autorità e del divieto di comunicare ad altri /divieto di tipping-off) un'informazione previsto dagli ordinamenti giuridici nazionali ed esteri (ad esempio anche in materia fiscale).

A fronte di queste numerose possibili limitazioni del diritto all'informazione, si può sostenere a ragione che la LSerFi definisce il quadro informativo per la consulenza agli investimenti e la gestione patrimoniale. Nel caso delle attività di intermediazione finanziaria ai sensi della LRD, il rifiuto, la restrizione o il semplice ritardo delle informazioni è una conseguenza della natura preventiva-punitiva della LRD. Il diritto all'informazione non deve essere utilizzato per compromettere gli obiettivi della LRD (prevenzione e lotta al riciclaggio di denaro e al finanziamento del terrorismo). In caso di dubbio, il gestore patrimoniale autorizzato deve limitare o addirittura rifiutare di fornire informazioni ai sensi della nLPD.

Limitazioni

Le dichiarazioni di cui sopra si applicano in misura limitata se

A. i dati relativi a persone fisiche vengono raccolti per finalità diverse dalla fornitura di servizi di gestione patrimoniale, consulenza sugli investimenti, ricezione e inoltro di ordini di strumenti finanziari e offerta di strumenti finanziari (ad es. nell'ambito della registrazione online a una newsletter per non clienti);

B. il trattamento dei dati rientra non solo nell'ambito di applicazione della nLPD, ma anche in quello del diritto sulla protezione dei dati dell'UE, in particolare del GDPR. A questo proposito, tuttavia, va notato che, secondo il parere qui espresso, l'accettazione e l'assistenza di clienti domiciliati nel SEE nell'ambito della reverse sollicitation (considerando 111 seconda frase MiFID II e 43 seconda frase MiFIR) non comporta l'applicabilità del GDPR.

***