Sviluppo Imprese Centro Italia

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE

EDIZIONE APRILE 2018

Il presente Documento illustra il complesso delle misure adottate e degli adempimenti svolti ai fini dell'osservanza delle disposizioni di cui al Regolamento (UE) 2016/679 del Parlamento europeo ("Regolamento") e del Consiglio del 27 aprile 2016 in materia di Tutela Privacy.
Il Regolamento punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione Europea.

Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione Europea ("Unione" o "UE") e non richiede una legge di recepimento nazionale; introduce, altresì, regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (data breach).

Il Documento si compone delle seguenti parti:

- la prima parte è dedicata ad una sintetica descrizione della struttura aziendale e ad una illustrazione generale dell'impianto organizzativo della privacy nella realtà della SGR: struttura, organizzazione, trattamento effettuato;
- segue poi una valutazione dei rischi, con la definizione di quelli afferenti la tutela dei dati personali nonché, più genericamente, di quelli propri dei sistemi informativi, e la descrizione dell'organizzazione aziendale per la protezione dei dati;
- una specifica sezione descrive le misure di sicurezza adottate dalla SGR, con l'esposizione degli accorgimenti per la protezione fisica dei locali e delle risorse, per le protezioni di tipo logico e per la sicurezza delle trasmissioni dei dati;
- una sezione illustra l'attività di formazione offerta agli incaricati;
- seguono gli aspetti connessi alle modalità di controllo e di verifica delle misure adottate.

SOMMARIO

1 DATI GENERALI DELL'AZIENDA

1.1 DATI ANAGRAFICI

SVILUPPO IMPRESE CENTRO ITALIA SOCIETA' DI GESTIONE DEL RISPARMIO S.P.A.
IN BREVE: SICI SGR S.P.A. ("SICI" o "SGR")

Sede legale FIRENZE – 50132 - Viale Giuseppe Mazzini, 46
Numero REA FI – 498755 - Codice fiscale 04888230481 - Partita IVA 04888230481
Forma giuridica: SOCIETA' PER AZIONI
Data di costituzione: 11/05/1998
Presidente: Avv. Daniele Taccetti
Direttore Generale: Dott. Guido Tommei
Recapito telefonico: 055 / 2007.51 Fax 055 / 2007.597
e-mail: info@fondisici.it
PEC: pecsici@legalmail.it

1.2 ATTIVITA' SVOLTA DA SICI SGR S.p.A.

La Società ha per oggetto la gestione, ottenute le autorizzazioni di legge, di uno o più fondi di investimento alternativi di tipo chiuso riservati a clientela professionale ("FIA").

La Società di gestione provvede, nell'interesse dei partecipanti, agli investimenti, alle alienazioni ed alle negoziazioni, all'esercizio dei diritti inerenti ai titoli e di ogni altro diritto compreso nei fondi comuni da essa gestiti, come pure alla distribuzione dei proventi e ad ogni altra attività di gestione degli stessi, con l'osservanza dei limiti previsti e dettati dalle norme di legge in materia, dal regolamento dei fondi e dalle competenti Autorità.

La Società può compiere inoltre le attività necessarie o strumentali al conseguimento dell'oggetto sociale.

All'interno della SGR è presente la Funzione Compliance a cui viene affidato il compito di svolgere attività di coordinamento e di fungere da punto di riferimento, a livello aziendale e nei confronti dell'esterno, per il pieno rispetto e per l'osservanza della Legge. Tale funzione è incentrata sull'attuazione delle disposizioni previste dalla Legge ed è volta a commentare e chiarire i pronunciamenti ed i comunicati emessi dall'Autorità Garante ("Garante") nonché a valutare gli orientamenti e le posizioni assunte dall'Associazione di categoria ("AIFI") in materia di privacy.

In particolare, la Compliance assolve alle seguenti funzioni:

- costituisce il punto di riferimento alle richieste di informazione della clientela, in relazione a quanto previsto dal Regolamento e dalle disposizioni in materia emanate dal Garante e risponde alle istanze formulate dalla clientela, con le modalità previste dal Regolamento curandone le relative formalità;
- funge da raccordo fra le funzioni interne e quelle esterne, in particolare per i rapporti con il Garante;
- segue l'evoluzione della Legge, sia dal punto di vista normativo che applicativo in base alle eventuali disposizioni del Garante;
- costituisce il punto di riferimento per gli altri eventuali "Responsabili del trattamento dei dati personali" e supporta tutte le funzioni interessate, ai fini di una corretta applicazione del Regolamento.

La SGR utilizza, sulla base di un contratto di service, il sistema informativo fornito dalla TT Tecnosistemi S.p.A. di Prato.

La possibilità di verifica dei dati concernenti i movimenti dei conti correnti e dei dossier titoli della SGR è assicurata dal servizio di Corporate Banking fornito da Banca Monte dei Paschi di Siena S.p.A., denominato "PasKey aziendaonline" (già "Paschi in Azienda").

La SGR si serve, altresì, sulla base di un contratto di service, di Nexi S.p.A. (già Istituto Centrale delle Banche Popolari Italiane S.p.A. o ICBPI S.p.A.) con sede in Milano per la gestione della contabilità dei fondi, oltre che per lo svolgimento dell'attività di Depositario. La possibilità di verifica dei dati concernenti i movimenti dei conti correnti e dei dossier titoli relativi ai fondi gestiti è assicurata dal servizio di Corporate Banking fornito da Nexi.

La SGR si avvale, inoltre:

- dello Studio Chimenti, con sede in Firenze, per lo svolgimento della consulenza fiscale e contabile;
- dello Studio Lunardo, con sede in Firenze, per lo svolgimento della consulenza in tema di amministrazione del personale.

Ai fini della presente normativa in tema di privacy, anche tali soggetti sono Titolari del trattamento dei dati personali.

Nella SGR tutti i dipendenti che procedono alla elaborazione dei dati personali a cui hanno accesso in relazione alle mansioni svolte per la sussistenza di un rapporto di lavoro subordinato operano sulla scorta delle direttive impartite dal Titolare, che ne controlla necessariamente l'applicazione ed il rispetto.

2 LA NORMATIVA DI LEGGE IN MATERIA DI PRIVACY – ASPETTI GENERALI

2.1 RIFERIMENTI NORMATIVI ESSENZIALI

I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali devono rispettare i diritti e le libertà fondamentali, in particolare, il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza.

Il Regolamento ha l'obiettivo di contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano, di conseguenza, nuove sfide per la protezione dei dati personali.

La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo.

La tecnologia attuale consente tanto alle imprese private, quanto alle autorità pubbliche, di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.

Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

E' stato quindi ritenuto necessario che tale evoluzione richiedesse un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consenta lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano quindi il controllo dei dati personali che li riguardano e che la

certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le Autorità pubbliche.

Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati è stato reso equivalente in tutti gli Stati membri. È stato ritenuto opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione.

Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possano ostacolare la libera circolazione dei dati personali nel mercato interno, è stato emanato il citato Regolamento per garantire la certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offrire alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento.

Inoltre, il Regolamento assicura un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le Autorità di controllo dei diversi Stati membri.

Per il buon funzionamento del mercato interno è stato ritenuto necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Per tener conto della specifica situazione delle micro, piccole e medie imprese (come definite dall'art. 2 dell'allegato della raccomandazione 2003/361/CE) il Regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni.

Il Regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli già previsti dal D. Lgs. 196/2003 - Codice in materia di protezione dei dati personali - (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

A questo scopo, i dati personali devono essere:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati e legittimi e, se utilizzati in altre operazioni del trattamento, in termini non incompatibili con tali scopi;
- esatti, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2.2 GLOSSARIO

La normativa intende per (cfr. art. 4 del Regolamento):

1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online

o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
14))«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
16) «**stabilimento principale**»:
    - per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    - con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente Regolamento;
17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente Regolamento;
18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
    a. il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b. gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c. un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»:
   a. trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
   b. trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente Regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente Regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

2.3 PRINCIPI

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**») e al titolare del trattamento è richiesto di essere in grado di comprovarlo («**responsabilizzazione**»); inoltre, possono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali («**limitazione della finalità**»).

I dati raccolti devono essere altresì adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**») esatti e, se necessario, aggiornati; inoltre, devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Il trattamento è lecito solo se l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, come ad esempio, per l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, per adempiere un obbligo legale al quale è soggetto il titolare del trattamento o per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica e in esecuzione di un compito di interesse pubblico.

In generale, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ad eccezione, ad esempio, quando il trattamento è

necessario per assolvere gli obblighi in materia di diritto del lavoro o della sicurezza e protezione sociale in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica.

2.4 DIRITTI DELL'INTERESSATO

Il titolare del trattamento adotta misure appropriate per fornire all'interessato, entro un mese dal ricevimento della richiesta stessa, tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi;
- il diritto di proporre reclamo a un'autorità di controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle relative informazioni.

L'interessato ha inoltre il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa oltre a poter richiedere la loro cancellazione qualora i dati personali non siano più necessari rispetto alle finalità per le quali erano stati raccolti e trattati.2.5 TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato.

Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento tratti i dati personali soltanto su istruzione documentata del titolare del trattamento.

E' altresì richiesto al responsabile del trattamento che metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi assunti e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Nelle imprese o organizzazioni con più di 250 dipendenti, il titolare del trattamento e, ove applicabile il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio al fine di garantire la sicurezza del trattamento e la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

Qualora la violazione dei dati personali possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La designazione di un responsabile della protezione dei dati è prevista nei casi in cui il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico o che riguardi trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala o, infine che si tratti di dati relativi a condanne penali e a reati.

2.6 AUTORITA' DI CONTROLLO

Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«**autorità di controllo**»).

Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al Regolamento.

Il membro o i membri e il personale di ogni autorità di controllo sono tenuti, in virtù del diritto dell'Unione o degli Stati membri, al segreto professionale in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei loro compiti o nell'esercizio dei loro poteri, sia durante che dopo il

mandato. Per tutta la durata del loro mandato, tale obbligo del segreto professionale si applica in particolare alle segnalazioni da parte di persone fisiche di violazioni del Regolamento.

Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del Regolamento nel territorio del rispettivo Stato membro.

Le autorità di controllo non sono competenti per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali.

Ad ogni autorità di controllo è richiesto di:

a) sorvegliare e assicurare l'applicazione del Regolamento;

b) promuovere la consapevolezza e favorire la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;

c) fornire consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;

d) promuovere la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente Regolamento;

e) fornire, su richiesta, informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente Regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;

f) trattare i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione e svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare, ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

g) collaborare, anche tramite scambi di informazioni, con le altre autorità di controllo e prestare assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento;

h) svolgere indagini sull'applicazione del Regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

i) sorvegliare gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare, l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;

j) adottare clausole contrattuali o impartire disposizioni operative al fine di garantire il rispetto del Regolamento;

k) redigere e tenere un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati;

l) offrire consulenza sui trattamenti;

m) incoraggiare l'elaborazione di codici di condotta, e fornire un parere su tali codici di condotta e approvare quelli che forniscono garanzie sufficienti;

n) incoraggiare l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati e approvare i criteri di certificazione;

o) effettuare, ove applicabile, un riesame periodico delle certificazioni rilasciate;

p) definire e pubblicare i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta e di un organismo di certificazione;

q) effettuare l'accreditamento di un organismo per il controllo dei codici di condotta e di un organismo di certificazione;

r) autorizzare le clausole contrattuali e le altre disposizioni;

s) approvare le norme vincolanti d'impresa;

t) contribuire alle attività del comitato;

u) tenere registri interni delle violazioni del Regolamento e delle misure adottate;

v) svolgere qualsiasi altro compito legato alla protezione dei dati personali.

Ogni autorità di controllo agevola la proposizione di reclami tramite misure quali un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione e svolge i propri compiti senza spese né per l'interessato né, ove applicabile, per il responsabile della protezione dei dati.

Inoltre, è demandato all'autorità di controllo il compito di vigilare sul rispetto del Regolamento richiedendo, se del caso, al titolare del trattamento informazioni e, in caso di violazioni accertate, anche mediante visite ispettive, comminare sanzioni.

Al fine di contribuire all'applicazione coerente del presente Regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante lo scambio delle informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il Regolamento in maniera uniforme mettendo in atto le opportune misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare anche ispezioni e indagini.

Il Comitato europeo per la protezione dei dati («**Comitato**») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.

La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del Comitato.

Il Garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del Regolamento.

3 IL TRATTAMENTO DEI DATI

3.1 CATEGORIE DEI DATI TRATTATI

Nello svolgimento della sua attività, la SGR effettua il trattamento dei dati secondo le specifiche di seguito indicate.

Fonte dei dati personali

I dati personali in possesso della SGR sono raccolti direttamente presso le società target ovvero presso terzi come, ad esempio, nell'ipotesi in cui la SGR acquisisca dati da società esterne a fini di informazioni economiche e finanziarie a scopi di due diligence, commerciali, ricerche di mercato, offerte dirette di prodotti o servizi.

Finalità del trattamento cui sono destinati i dati

I dati personali sono trattati nell'ambito della normale attività della SGR e secondo le seguenti finalità:

- finalità strettamente connesse e strumentali alla gestione dei rapporti con le imprese target;
- finalità strettamente connesse e strumentali all'instaurazione e gestione del rapporto di lavoro con i dipendenti e consulenti;

- finalità connesse agli obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria nonché da disposizioni impartite da autorità a ciò legittimate dalla legge e da organi di vigilanza e controllo. Le operazioni di trattamento effettuate dalla SGR si riferiscono principalmente a dati riguardanti le categorie di interessati di seguito elencate:
  - personale dipendente;
  - candidati per l'instaurazione di un posto di lavoro;
  - consulenti e liberi professionisti;
  - soci della SGR;
  - sottoscrittori del fondi gestiti dalla SGR;
  - società target e proponenti dei progetti;
  - fornitori;
  - soggetti o organismi pubblici;
  - amministratori e sindaci.

Le informazioni raccolte vengono quindi registrate in banche dati, la cui classificazione, oltre che delle categorie di interessati a cui i dati si riferiscono, tiene conto delle finalità per le quali i dati stessi sono stati raccolti.

Riportiamo di seguito uno schema delle banche dati costituite in azienda, la cui gestione tiene conto dei criteri sopra esposti.

- finalità amministrativo-contabili;
- trattamento giuridico ed economico del personale;
- gestione del personale:
  - reclutamento, selezione, valutazione e monitoraggio del personale
  - formazione professionale;
  - sistema premiante;
- adempimento di obblighi fiscali e contabili;
- gestione dei fondi di previdenza aziendale;
- gestione dei rapporti di lavoro e delle relazioni sindacali;
- adempimenti connessi all'igiene e alla sicurezza sul lavoro;
- pianificazione e monitoraggio dei compiti, del volume di lavoro e delle prestazioni lavorative;
- gestione e monitoraggio delle imprese target
- adempimenti connessi all'amministrazione ed alla gestione degli azionisti;
- adempimenti connessi all'amministrazione ed alla gestione degli amministratori e dei sindaci revisori;
- gestione dei fornitori;
  - selezione dei fornitori;
  - amministrazione dei fornitori;
  - amministrazione dei contratti, ordini, fatture;
  - servizi di controllo interno;
  - controlli sulla sicurezza;
  - controlli sulla qualità dei servizi erogati;
  - controlli sull'integrità del patrimonio.

Finalità connesse allo svolgimento di attività di ricerca e promozione

- analisi e indagini di mercato;
- promozione di SICI e dei fondi da questa gestiti.

I luoghi in cui vengono custoditi i dati devono essere così intesi:

- in caso di trattamenti non automatizzati, i vari luoghi in cui sono conservati fisicamente i dati personali (uffici, dipendenze, archivi);
- in caso di trattamenti automatizzati, l'ubicazione delle memorie dell'elaboratore (o degli elaboratori) sul quale (o sui quali) sono registrati i dati personali.

Nella SGR i dati trattati con strumenti non automatizzati sono ubicati e conservati prevalentemente presso:

- la Direzione Generale della SGR sita in Firenze;
- gli archivi informatici sono invece detenuti presso:
  - la Direzione Generale della SGR a Firenze;
  - il Depositario (anche Outsourcer dei Fondi gestiti) a Milano;
  - gli intermediari destinatari della gestione della liquidità e del patrimonio eccedenti e dei conti correnti;
- banche dati sono ubicate e conservate anche presso:
  - Studio Chimenti (Firenze) per la gestione della contabilità aziendale;
  - Studio Lunardo (Firenze) per la tenuta del libro paga e amministrazione dei dipendenti;
  - KPMG S.p.A. (Firenze) quale società di revisione.

3.2 MODALITA' DI TRATTAMENTO

In relazione alle indicate finalità, il trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità per cui sono raccolti. Per il trattamento dei dati effettuato in forma automatizzata, viene utilizzato, sulla base di un contratto di service con la TT Tecnosistemi S.p.A. Le elaborazioni avvengono mediante l'utilizzo di specifici applicativi, che comunque non comportano tipologie di trattamento di dati diversi da quelli già presenti nel sistema centrale. Essi costituiscono delle applicazioni nell'ordinaria gestione previste dalla vigente normativa.

Per il trattamento automatizzato dei dati relativi alla gestione della contabilità dei fondi gestiti, la SGR si serve, sulla base di un contratto di service, di Nexi. Possono inoltre essere effettuati, con sistemi automatizzati o meno, tutti quei trattamenti per i quali il Regolamento non prevede particolari adempimenti o richiesta di autorizzazioni.

Le circostanze che più interessano le attività della SGR sono:

- trattamento di dati contenuti o provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- trattamenti effettuati esclusivamente per la gestione del protocollo, relativamente ai dati necessari per la classificazione della corrispondenza inviata per fini diversi da quelli di informazione commerciale, invio di materiale pubblicitario, vendita diretta, ricerche di mercato e comunicazione commerciale interattiva;
- tenuta di rubriche (telefoniche o analoghe) non destinate alla diffusione, utilizzate unicamente per ragioni di ufficio e di lavoro e per fini comunque diversi da quelli di

informazione commerciale, invio di materiale pubblicitario, ricerche di mercato e comunicazione commerciale interattiva;

- trattamenti effettuati unicamente per l'adempimento di specifici obblighi contabili, retributivi, previdenziali, assistenziali e fiscali; tali trattamenti fanno riferimento alle sole categorie di dati, di interessati e di destinatari della comunicazione e diffusione strettamente collegate a tale adempimento;
- trattamenti effettuati per adempiere e dare esecuzione agli obblighi di legge e a quelli previsti dai contratti stipulati con gli outsourcers e, comunque, sempre per la corretta amministrazione e gestione della Società nel rispetto della vigente normativa primaria e secondaria.

La SGR non tratta "**dati sensibili**" (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le condanne, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale) relativi alla clientela e, per il personale dipendente, solo ciò che è strettamente necessario per l'amministrazione del rapporto di lavoro previsto dalla vigente normativa in materia.

3.3 SICUREZZA DEI DATI PERSONALI

Uno degli aspetti principali del Regolamento riguarda le misure di sicurezza che devono essere adottate per il controllo e la custodia dei dati che formano oggetto di trattamento. Le misure di sicurezza richiamate sono intese in senso ampio e riguardano il complesso delle misure fisiche, logiche, informatiche, organizzative e procedurali atte ad evitare che:

- i dati personali risultino accessibili a persone non autorizzate;
- formino oggetto di trattamenti non consentiti o non conformi alle finalità della raccolta;
- vengano distrutti o perduti, anche accidentalmente.

Nella SGR tutto il personale è incaricato del trattamento dei dati personali e, in virtù di questa qualifica, ciascun dipendente, entro i limiti definiti dei compiti che gli sono stati assegnati, è autorizzato a compiere tutte le operazioni di trattamento previste dalla mansione svolta e a rispettare le misure di sicurezza.

Al fine di meglio definire la sicurezza dei dati personali, si procede ad una ricognizione delle possibili tipologie di rischio connesse all'attività svolta dalla SGR. Una prima ripartizione dei rischi è effettuata sulla base del seguente criterio:

<u>Origine</u>

- interni connessi all'attività dei dipendenti della SGR;
- esterni connessi all'attività di terzi;
- ambientali relativi ad eventi devastanti (quali incendi, terremoti, alluvioni).

<u>Cause</u>

- carenze organizzative derivanti da responsabilità non correttamente assegnate, da sottovalutazione dei rischi, ecc.;
- colpa o dolo.

Modalità

- intercettazioni per intrusioni lungo la rete di trasmissione dei dati (ivi inclusa intercettazione di corrispondenza);
- "backdoor" punti di ingresso non noti, volutamente previsti in fase di programmazione del software;
- "Troian Horses " software predisposto per operare in modo non conosciuto;
- "virus" informatici, capaci di autopropagarsi e danneggiare programmi, procedure e dati.

Rischi di distruzione o perdita dei dati

Rischi fisici

- incendio (per cause naturali, per comportamento colposo o doloso). Nella valutazione del rischio incendio occorre comunque tenere presente anche la nostra ubicazione rispetto ad una sede di intervento dei Vigili del Fuoco che consente la copertura, dal momento della richiesta di soccorso, in un tempo abbondantemente al di sotto della soglia di intervento "rapido" che prevede la copertura entro 20 minuti;
- allagamenti (per cause naturali, per comportamento colposo o doloso);
- furto e rapina;
- scasso;
- perdita accidentale, sottrazione, furto di tabulati ed elenchi;
- perdita, sottrazione, furto di p.c. portatili.

Rischi informatici

- caduta di energia elettrica;
- cancellazione fortuita di dati;
- smagnetizzazione dei supporti;
- virus informatici.

Rischi connessi all'integrità dei dati

Rischi fisici

- Manomissione dolosa dei dati (da parte di terzi)

Rischi informatici

- Manomissione dolosa dei dati (da parte di terzi)

Rischi di accesso non autorizzato

Rischi fisici

- intrusione di persone non autorizzate in locali riservati della SGR;
- negligenza da parte del personale dipendente nel lasciare i dati incustoditi (tabulati ed elenchi abbandonati sopra la scrivania, durante e dopo l'orario di lavoro) e non protetti (elenchi e tabulati riposti in armadi od altri contenitori senza aver provveduto a chiuderli o a riporre la chiave in un luogo sicuro);

- impossibilità da parte del personale dipendente di riporre i dati in luoghi adeguatamente protetti e sicuri in quanto i contenitori non sono muniti di chiavi o hanno la chiusura difettosa;
- uso di stampanti centralizzate, in cui vengono indirizzate le stampe di varie unità;
- mancata conferma che i tabulati o gli elenchi relativi a dati particolari e la cui stampa è stata effettuata con procedure accentrate, siano pervenuti correttamente alla persona che li ha richiesti;
- disguido, per errore manuale o guasto tecnico, di messaggi trasmessi per telefax.

Rischi informatici

- non osservanza (per motivi operativi) della necessaria segretezza nell'uso della parola chiave;
- mancata chiusura del posto di lavoro in caso di allontanamento, anche momentaneo, dell'operatore;
- mancata disabilitazione dell'operatore del livello e dei profili di cui era in possesso prima dell'ultimo trasferimento;
- controlli non adeguati sul personale esterno adibito all'assistenza tecnica;
- intrusione durante la trasmissione di messaggi e di dati tramite il servizio di posta elettronica via Internet.

Rischi di trattamento non consentito o non conforme alle finalità della raccolta

Rischi fisici

- mancato recepimento delle disposizioni impartite dalla clientela, in seguito allo smarrimento del modello in cui è stato prestato o negato il consenso al trattamento dei dati;
- disguido, per errore manuale o guasto tecnico, di messaggi trasmessi per telefax;
- diffusione di dati a persone non interessate al trattamento ("procuratori" non facoltizzati).

Rischi connessi alla trasmissione dei dati

Rischi fisici

- danneggiamento - per guasto tecnico, manomissione dolosa, mancanza di energia elettrica di alimentazione - di dispositivi di interconnessione (modem, router, firewall) fra rete aziendale e società di fornitura Servizio SIA e Connessione Internet.

Rischi informatici

- intrusione di virus informatici atti a distruggere e/o manomettere i dati personali;
- intrusione da parte di soggetti esterni nella rete informatica durante l'utilizzo della posta elettronica tramite Internet o durante l'interconnessione a siti Internet.

Rischi connessi al reimpiego di supporti di memorizzazione

Rischi fisici

- accesso ai dati da parte di persone non autorizzate per mancata o incompleta cancellazione;

- trattamento non consentito o non conforme alle finalità della raccolta per mancata o incompleta cancellazione.

Rischi connessi alla conservazione dei dati e della documentazione relativa al trattamento

Rischi fisici

- distruzione o perdita accidentale per incendio, alluvione, furto;

Rischi informatici

- trattamento non consentito o non conforme alle finalità della raccolta;
- trattamento per un periodo di tempo superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e successivamente trattati;
- accesso e trattamento dei dati da parte di persone non autorizzate.

Rischi connessi all'utilizzo di archivi e contenitori

Rischi fisici

- trattamento non consentito o non conforme alle finalità della raccolta;
- trattamento per un periodo di tempo superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e successivamente trattati;
- accesso e trattamento dei dati da parte di persone non autorizzate.

3.4 TRATTAMENTI CON STRUMENTI ELETTRONICI

Il trattamento di dati personali viene effettuato con strumenti elettronici e con l'osservanza delle seguenti misure di sicurezza:

a. autenticazione informatica;
b. adozione di procedure di gestione delle credenziali di autenticazione;
c. utilizzazione di un sistema di autorizzazione;
d. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g. Periodica revisione ed aggiornamento delle procedure inerenti la sicurezza della gestione dei dati.

3.5 TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici viene svolto con le seguenti modalità:

a. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b. previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c. previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

3.6 MISURE ORGANIZZATIVE DI SICUREZZA

Le misure adottate dalla SGR per la sicurezza dei dati possono essere schematicamente rappresentate come di seguito.

Analisi dei rischi

I rischi hanno già formato oggetto di analisi ed è stata definita in maniera formale mediante il self assessment dei processi operativi già in precedenza alla stesura del presente documento; essa, è stata da sempre presente nel vissuto quotidiano della SGR sì da farla essere adeguatamente preparata nell'approntare le misure di sicurezza richieste dalla vigente normativa in tema di privacy.

Misure fisiche di sicurezza

Gli accessi ai locali della Direzione Generale, utilizzati a fini strumentali e nei quali si svolgono attività di trattamento dati personali, avvengono tutti direttamente dall'esterno tramite porte a comando elettrico. Tali ingressi sono presidiati dal personale che eroga il servizio di portierato fino alle 13.30 e si ha una videocamera che li monitora. Tale presidio avviene, inoltre, anche da parte del personale dipendente della SGR.

Sono installati sistemi di sorveglianza anti-intrusione tipo allarme; inoltre, l'immobile, fuori dall'orario di lavoro e nei giorni festivi, è oggetto di visite ispettive da parte di una compagnia di guardie giurate.

Quando presente, il personale addetto al servizio di portierato indirizza i visitatori verso i destinatari ed effettua l'identificazione dei visitatori che avviene attraverso il riconoscimento degli stessi da parte della portineria mediante preventiva comunicazione, da parte del dipendente della SGR, degli appuntamenti programmati o richiesta al dipendente dell'effettivo appuntamento con il visitatore.

In assenza del servizio di portierato, gli eventuali accessi sono gestiti attraverso il videocitofono.

Custodia in classificatori o armadi non accessibili

I documenti cartacei sono conservati all'interno di armadi posti nei singoli uffici o nell'archivio. Detti armadi sono chiudibili con chiavi e vengono serrati al termine dell'attività lavorativa. Nel caso in cui sia previsto o comunque verificato l'accesso nella sede di personale estraneo, i documenti, comprese eventuali comunicazioni fax sopraggiunte, vengono accuratamente riposti negli uffici in modo tale che non siano visionabili se non con l'autorizzazione del dipendente che presidia l'ufficio stesso.

Il controllo del personale esterno che accede ai locali della SGR per interventi di manutenzione viene espletato sia sotto forma di monitoraggio, sia dal punto di vista qualitativo al fine di mantenere quelle condizioni ambientali ottimali al funzionamento delle apparecchiature tecniche utilizzate per il trattamento dei dati.

Misure logiche di sicurezza

L'accesso al Sistema Informativo Aziendale (SIA) è consentito solo tramite il processo di identificazione dell'operatore, al quale è assegnato un codice identificativo (numero di matricola) ed è protetto da una parola chiave.

Attraverso l'abbinamento del codice identificativo personale alla parola chiave viene garantita l'autenticazione e la legittimità dell'incaricato.

Gli accessi al SIA sono memorizzati in un flusso di LOG, riepilogativo delle sessioni di collegamento.

La procedura antivirus, che utilizza una base dati contenente l'elenco dei virus conosciuti (aggiornata in modo automatico direttamente su ciascuna postazione P.C.), si attiva automaticamente ad ogni avvio del sistema operativo.

Le password utilizzate per l'accesso al SIA sono memorizzate dopo specifica cifratura.

4 IL SISTEMA INFORMATIVO

Nella realtà della SGR, analogamente a tutto il mondo bancario e finanziario, il patrimonio informativo è considerato da sempre una vera e propria ricchezza aziendale e, come tale, è costantemente presidiato con specifiche misure di protezione e salvaguardia dei dati.

Il Sistema Informativo Aziendale si è sviluppato nel tempo tenendo costantemente presenti le esigenze di assicurare un'adeguata protezione dei dati gestiti.

La SGR utilizza, sulla base di un contratto di service, il sistema informativo fornito da TT Tecnosistemi S.p.A. di Prato. La possibilità di verifica dei dati concernenti i movimenti dei conti correnti e dei dossier titoli della SGR è assicurata dal servizio di Corporate Banking fornito da Banca Monte dei Paschi di Siena S.p.A., denominato "PasKey aziendaonline" (già "Paschi in Azienda").

Il Servizio TT|Tre60 PLUS fornito da TT Tecnosistemi S.p.A. comprende il noleggio di una postazione di lavoro così composta:

Computer Desktop Hp ProDesk 400

- Processore I5
- RAM 8GB
- Hard Disk 1 TB
- Scheda di rete
- Tastiera 102 K
- 4 USB Port
- Mouse
- Garanzia del produttore per tutta la durata del contratto (36mesi).

Monitor Hp ProDisplay P223 21,5"

- LED full HD (1080p)

Sistema Operativo

- Microsoft Windows 10 Professional

Applicazioni di Office incluse

- Microsoft Outlook
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft OneNote
- Microsoft Publisher

Applicazioni di sicurezza incluse

- Antivirus
- Antimalware
- Backup Agent

Servizi Standard inclusi

- Exchange On Line
- Skype for Business
- SharePoint
- Teams
- OneDrive
- Backup della postazione di Lavoro (Max 200 GB/PDL scopo DR) su area storage locale compresa
- Manutenzione della postazione di lavoro
  - Aggiornamento proattivo
  - HelpDesk dedicato
  - Ripristino Pdl in caso di Fault
- Impostazione OneDrive (1 TB per utente)
- Definizione Utenti

Servizi extra Offerti (compreso nel canone)

- Export / Import Posta Elettronica da attuale gestore
- Migrazione dati di tipo File (Max 50 GB Utente)
- Server Virtuale in Cloud come area di condivisione di tipo file sharing e domain controller. Area destinata al file sharing 250 GB
- Backup su Azure del Server Virtuale (Max 500 GB compresa retention)
- Ticket extra NBD on site (fino ad un massimo di 7) per supporto attività su postazioni di lavoro Risorse Azure previste

Tali risorse sono regolate dalle condizioni contrattuali predisposte da Microsoft.

- 1 indirizzo IP statico
- VPN Gateway
- Backup 1 istanza/e x 512, LRS
- Virtual Machine o (2 vCPU, 7 GB di RAM); Windows - dischi del sistema operativo gestiti – S15

Per il trattamento automatizzato dei dati relativi alla gestione della contabilità dei fondi gestiti da SICI si serve inoltre, sulla base di un contratto di service, di Nexi S.p.A. La possibilità di verifica dei dati concernenti i movimenti dei conti correnti e dei dossier titoli relativi ai fondi gestiti è assicurata dal servizio fornito da Nexi che, ai fini della privacy, è titolare del trattamento dei dati.

Dal 28 maggio 2008, la tenuta della contabilità generale della SGR ed i relativi adempimenti fiscali sono affidati al Dott. Vieri Chimenti (Studio Chimenti), mentre la contabilità del personale è affidata al consulente del lavoro Dott. Luca Lunardo (Studio Lunardo). Entrambi, ai fini della normativa privacy, sono titolari del trattamento dei dati.

Dal 1° gennaio 2017 le attività amministrative legate all'operatività dei Fondi, quali il calcolo del NAV e le attività di back-office nonché l'attività di Depositario sono state affidate a Nexi S.p.A. e normate da appositi accordi sia con riferimento ai sistemi informativi che alle risorse dedicate alla gestione dei processi.

L'Outsourcer amministrativo dispone del sistema informativo ARCHIMEDE che è in grado di gestire gli aspetti contabili e normativi previsti per i Fondi, nonché di fornire uno strumento di analisi e di reporting a supporto delle scelte decisionali. Il software permette di avere accesso:

- alla contabilità del Fondo con evidenza della gestione del ciclo attivo e passivo economico e patrimoniale, con i dettagli anagrafici dei clienti e fornitori, e degli scadenzari e partitari clienti e fornitori;
- alla contabilità del Fondo con evidenza delle prime note collegate alla movimentazione dei portafogli;

- alla reportistica (bilanci di verifica secondo riclassificazioni gestionali e normative, bilanci di verifica per centri di costo, partitari su singoli codici contabili o su insiemi di codici contabili, elenco completo registrazioni, libro giornale, registri IVA e dettagli liquidazioni IVA);
- alle evidenze relative alla segnalazioni di vigilanza verso Banca d'Italia.

Il software include l'accesso alle funzionalità di Registro Ordini:

- funzionalità di inserimento ordini;
- funzionalità di inserimento eseguiti;
- funzionalità di ricerca e stampa registro ordini.

Il software include le seguenti funzionalità:

- consultazione dei dati anagrafici ed operatività degli investitori dei Fondi della SGR;
- amministrazione e registrazione delle operazioni dei sottoscrittori collegate alla gestione dei fondi: sottoscrizione, emissione/ritiro certificati, conversioni, trasferimenti quote, rimborsi, gestione richiamo degli impegni;
- produzione reportistica per i sottoscrittori; - produzione dati di controllo per la Banca Depositaria.

Il modulo prevede l'accesso alle seguenti funzionalità di interrogazione:

- Consultazione dei dati anagrafici dei sottoscrittori dei fondi;
- Consultazione dei saldi quote delle posizioni in fondi;
- Consultazione delle operazioni dei sottoscrittori;
- Funzionalità di reporting:
  - report sottoscrittori con elenco sottoscrittori per fondo;
  - report operazioni con elenco delle operazioni per fondo;
  - registro ordini relativi all'operatività dei sottoscrittori.

Il modulo applicativo AUI è specificamente sviluppato per l'ordinata tenuta delle registrazioni richieste dalla normativa in materia di antiriciclaggio. Tale applicativo "Modulo Antiriciclaggio" prevede l'accesso alle seguenti funzionalità di interrogazione:

- visualizzazione dell'archivio transitorio delle registrazioni (anagrafiche, rapporti continuativi, titolari effettivi, movimenti rilevanti, legami) attinenti alla gestione degli obblighi in materia di antiriciclaggio previsti normativamente in capo alla SGR;
- visualizzazione dell'archivio consolidato della SGR, con il medesimo dettaglio di cui al punto precedente;
- estrazione di reporting collegato alle registrazioni effettuate.

Il modulo applicativo Anagrafe Rapporti è specificamente sviluppato per l'ordinario invio delle segnalazioni all'Agenzia delle Entrate. Tale Applicativo Modulo Anagrafe Rapporti prevede l'accesso alle seguenti funzionalità in interrogazione:

- Flussi mensili di anagrafiche clienti;
- Flusso annuale dei saldi.

Le applicazioni sopra presentate sono di proprietà di Unione Fiduciaria e sono sviluppate sull'architettura di seguito descritta:

- livello dati: composta da DB2-400 che gestiscono l'organizzazione dei dati in modo efficiente e sicuro;
- livello logico: risiedono le funzionalità di elaborazione dati;
- livello di presentazione: composto dagli strumenti che permettono all'utente di interagire con il sistema.

Le scelte tecnologiche effettuate dall'outsourcer informatico in termini di hardware e software si possono riassumere come segue:

Soluzioni hardware

- Server : Costituito da due sistemi IBM ISERIES Power 8 in Disaster Recovery ubicati presso due siti posizionati in diverse aree geografiche di Milano ed in comunicazione tramite doppio link intraced ad alta velocità. All' interno di ognuno dei due sistemi ISERIES sono configurate le partizioni AS400 (Application Server 400) sulle quali risiede l' applicativo Archimede. I sistemi ISERIES sono multi processore ed è possibile intervenire sulla configurazione di ogni singola partizione per adeguare la quantità di processore e di memoria RAM. I dati risiedono su Storage IBM, modello V900 con memorie flash allo stato solido. L'infrastruttura hardware è completamente ridondata tra i due CED ed è attiva la replica dati a livello hardware in modalità sincrona METROMIRROR;
- Antiriciclaggio: DB SQL SERVER INTEL – Server DL380 in Alta Affidabilità su piattaforma MS Windows 2008 R2;
- Application Server – Server Intel in alta affidabilità su piattaforma VMWARE
- File server: SFTP pubblico costituito da un cluster Power HA su sistema operativo AIX;
- LAN: Gli apparati di rete per la gestione del Front-end sono ridondati nei punti vitali.

Soluzioni software

- Sistemi operativi: OS400 V7R1;
- Database: DB2-400;
- Strumenti di sviluppo applicazioni: RPG ILE 400 RDI;
- Application server: AS400;
- Web server: APACHE

Da un punto di vista dei sistemi informativi Nexi, per le attività di Depositario, adotta un sistema di "Esternalizzazione del Sistema Informativo".

Per l'attività inerente la tenuta dei conti Domestici e Estero, il Depositario utilizza Bancakdati per l'erogazione del servizio e della proceduta Titoli.

Per la custodia degli strumenti finanziari Nexi, quale aderente al circuito di Target 2 Securities, privilegia l'utilizzo di Local ed International Central Securities Depository (CDS) come Monte Titoli e Euroclear. Inoltre, per garantire la copertura globale su tutti i mercati utilizzati dalla clientela, si avvale di ulteriori sub-depositarie di volta in volta comunicate alle SGR.

A garanzia del patrimonio del fondo, gli strumenti di pertinenza dello stesso sono rubricati su conti intestati a Nexi, tenuti separati da quelli relativi agli strumenti finanziari di proprietà della medesima.

Per i controlli di Depositario, relativi all'area partecipanti, al valore della quota nonché ai limiti d'investimento, la Banca si è dotata di un sistema denominato DIOGENE, fornito da Unione Fiduciaria, con il quale è in grado di svolgere i suoi compiti di controllo e di riconciliazione. In tale sistema vengono gestiti i certificati cumulativi rappresentativi delle quote dei fondi, il registro degli altri beni ed i controlli contabili e sui limiti di investimento.

Si avvale inoltre del sistema “Galileo” di Sintea per la gestione delle anagrafiche e dei prezzi che gestisce e storicizza i dati finanziari di mercato provenienti dai principali Info provider definiti dalla policy aziendale necessari ai controlli del Depositario.

Infine, per monitorare i propri conti, il Depositario mette a disposizione un’applicazione di remote banking (internet based), denominata LEWIS. Tramite tale strumento la SGR può consultare i movimenti e i saldi dei conti in tempo reale nonché estrarre reportistica in formato xls o pdf. Con tutti i fornitori informatici sono previsti “SLA” che regolano i tempi di risposta dei sistemi e di presa in carico e della risoluzione delle anomalie e che garantiscono procedure di back up e di Disaster Recovery conformi alle policy adottate di Nexi.

4.1 .MISURE DI SICUREZZA INFORMATICA POSTE IN ESSERE DA NEXI

Al fine di assicurare l'integrità, la segregazione e la tutela della riservatezza dei dati e delle informazioni acquisiti nell'espletamento delle sue attività, Nexi adotta la policy e le procedure di gruppo volte a garantire :

- la sicurezza degli accessi alle Sedi e dei dati;
- la sicurezza dei locali;
- la sicurezza delle apparecchiature;
- la sicurezza logica;
- integrità dei dati e back-up;
- disaster Recovery.

In particolare le procedure di back up e di Disaster Recovery Plan rientrano nel Business Continuity Plan del gruppo Nexi. I documenti che illustrano nel dettaglio gli argomenti di cui sopra sono riservati e Nexi li rende disponibili presso la propria sede in occasione di Audit richiesti dai clienti.

5 FORMAZIONE DEL PERSONALE

Il piano di formazione rappresenta un aspetto essenziale dell’intero programma di sicurezza e costituisce elemento irrinunciabile al fine di ottimizzare l’utilizzo delle tecnologie a disposizione degli intermediari finanziari. Un’adeguata formazione, anche senza la predisposizione di particolari strumenti tecnologici di supporto, è in grado di far compiere notevoli passi avanti sul piano della sicurezza. Al fine dunque di formare ed informare i propri dipendenti, ovvero gli incaricati del trattamento dei dati, la SGR ha posto particolare attenzione alla diffusione della normativa interna in materia di tutela privacy.

La valutazione e la rilevazione dei rischi riveste un ruolo di sempre maggiore importanza nell’attività delle SGR. Si tratta di un monitoraggio che viene costantemente perseguito al fine di garantire un’assunzione di rischi consapevole e correlata alle condizioni economico-patrimoniali delle aziende medesime.

Il controllo periodico delle misure e degli accorgimenti adottati per il monitoraggio dei rischi è un aspetto essenziale per verificare la validità del piano di sicurezza predisposto, o per porre in essere gli eventuali correttivi. Del resto, l’attività di controllo sull’attività aziendale in genere è un elemento da sempre presente nella realtà finanziaria.

Il Sistema dei Controlli Interni è costituito dall’insieme delle regole, delle procedure e delle strutture organizzative che mirano ad assicurare il rispetto delle strategie aziendali ed il conseguimento delle seguenti finalità:

- performance, intesa come efficacia, efficienza ed ottimizzazione dei processi aziendali;

- salvaguardia dei valori delle attività e protezione dalle perdite;
- informazione, ovvero affidabilità ed integrità delle informazioni contabili e gestionali;
- conformità delle operazioni con la Legge, la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne;
- miglioramento, ovvero garanzia di azioni correttive per l'eliminazione delle deficienze rilevate e di coerente evoluzione dei presidi organizzativi rispetto alle strategie aziendali ed al contesto di riferimento.

La normativa inerente al Sistema dei Controlli Interni prevede una serie di adempimenti e controlli a carico delle funzioni interessate della SGR. Per ogni adempimento è definito l'oggetto del controllo, la periodicità, l'adempimento (scopo) e gli strumenti da utilizzare. Semestralmente le funzioni Internal Audit, Compliance e Risk Management redigono una relazione sui controlli svolti, evidenziando, se del caso, le anomalie riscontrate ed i correttivi da apportare in tema di tutela della privacy.