

**POLICY**  
**SUL TRATTAMENTO E SICUREZZA DEI DATI**

<b>Versione</b>	<b>Data di Approvazione</b>
1	27 aprile 2022

## *INDICE*

<b>1.</b>	<b><i>PREMESSA E SCOPO</i></b>	<b>3</b>
<b>2.</b>	<b><i>RIFERIMENTI NORMATIVI</i></b>	<b>4</b>
<b>3.</b>	<b><i>DEFINIZIONI</i></b>	<b>5</b>
<b>4.</b>	<b><i>IL TITOLARE DEL TRATTAMENTO</i></b>	<b>7</b>
<b>5.</b>	<b><i>RESPONSABILE DELLA PROTEZIONE DEI DATI</i></b>	<b>8</b>
<b>6.</b>	<b><i>NOMINA DEI RESPONSABILI DEL TRATTAMENTO DEI DATI</i></b>	<b>9</b>
<b>7.</b>	<b><i>PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI E FORMAZIONE</i></b>	<b>10</b>
<b>8.</b>	<b><i>MISURE DI SICUREZZA</i></b>	<b>11</b>
<b>9.</b>	<b><i>REGISTRO DEI TRATTAMENTI</i></b>	<b>12</b>
<b>10.</b>	<b><i>DATA PROTECTION IMPACT ASSESSMENT</i></b>	<b>13</b>
<b>11.</b>	<b><i>MODALITÀ DI TRATTAMENTO – INFORMATIVA E CONSENSO</i></b>	<b>14</b>
<b>11.1</b>	<b><i>Corretto Trattamento dei dati</i></b>	<b>14</b>
<b>11.2</b>	<b><i>Informativa</i></b>	<b>15</b>
<b>11.3</b>	<b><i>Consenso</i></b>	<b>15</b>
<b>11.4</b>	<b><i>Dati dei dipendenti/collaboratori</i></b>	<b>16</b>
<b>12.</b>	<b><i>MODALITÀ DI CONSERVAZIONE DEI DATI PERSONALI</i></b>	<b>17</b>
<b>13.</b>	<b><i>ESERCIZIO DEI DIRITTI DELL'INTERESSATO</i></b>	<b>18</b>
<b>13.1</b>	<b><i>Diritto di accesso</i></b>	<b>18</b>
<b>13.2</b>	<b><i>Diritto di rettifica</i></b>	<b>19</b>
<b>13.3</b>	<b><i>Diritto alla cancellazione</i></b>	<b>19</b>
<b>13.4</b>	<b><i>Diritto di limitazione del trattamento</i></b>	<b>19</b>
<b>13.5</b>	<b><i>Diritto alla portabilità dei dati</i></b>	<b>20</b>
<b>13.6</b>	<b><i>Diritto di opposizione</i></b>	<b>21</b>
<b>13.7</b>	<b><i>Richieste di esercizio dei diritti</i></b>	<b>21</b>
<b>14.</b>	<b><i>DATA BREACH</i></b>	<b>23</b>
<b>15.</b>	<b><i>CONTROLLI</i></b>	<b>25</b>
<b>16.</b>	<b><i>SANZIONI</i></b>	<b>26</b>
<b>17.</b>	<b><i>MODIFICHE ALLA POLICY</i></b>	<b>27</b>

## 1. PREMESSA E SCOPO

La presente policy (la “**Policy**”) è stata approvata dal Consiglio di Amministrazione di Quinta Capital SGR S.p.A. (la “**SGR**” o la “**Società**”) ed è stata adottata al fine di garantire che:

- il trattamento dei dati personali da parte della SGR venga effettuato, sin dalla fase di avvio del trattamento e nel corso del medesimo, in conformità alla normativa di riferimento;
- l'utilizzo dei dati personali sia pertinente e limitato a quanto strettamente necessario e sufficiente per le finalità previste e per il periodo necessario.

La Policy descrive le modalità gestionali ed operative relative all'assolvimento degli adempimenti in materia di protezione dei dati personali imposti dalla vigente normativa.

La Policy si applica nei confronti delle categorie di soggetti di seguito indicate:

- dipendenti, consulenti e collaboratori;
- candidati all'istaurazione di rapporti di lavoro/collaborazioni;
- clienti;
- persone fisiche che ricoprono cariche sociali o altri incarichi;
- *outsourcer*;
- fornitori.

## 2. RIFERIMENTI NORMATIVI

Normativa di carattere generale:

- Regolamento UE 2016/679 (“**GDPR**”);
- D. Lgs. n. 196/2003, cosiddetto “Codice in materia di protezione dei dati personali” come modificato dal D. Lgs. 101/2018 (“**Codice Privacy**”).

Normativa aziendale:

- Procedura di *business continuity plan*;
- Procedura di *disaster recovery*;
- Procedura per la gestione dei sistemi informativi.
- Proposta di consulenza legale per lo svolgimento di A) implementazione del sistema privacy; B) incarico di Data Protection Officer.

### 3. DEFINIZIONI

Allo scopo di agevolare la comprensione della Policy, si riportano le seguenti definizioni:

- **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;
- **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 o a un identificativo online;
- **Dato particolare:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare 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;
- **Dati relativi a condanne penali e reati:** dati relativi a condanne penali e reati, a sanzioni amministrative dipendenti da reato, alla qualità di imputato o di indagato;
- **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;
- **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;
- **Persone autorizzate al trattamento:** le persone fisiche che trattano dati personali sotto l'autorità del Titolare del trattamento o del responsabile del trattamento e sulla base delle istruzioni ricevute dal Titolare;
- **Interessato:** la persona fisica cui si riferiscono i dati personali;

- **Comunicazione:** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal rappresentante del Titolare nel territorio dello Stato, dal responsabile e dalle persone autorizzate al trattamento, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **Diffusione:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **Autorità di controllo:** il Garante per la protezione dei dati personali.

#### **4. IL TITOLARE DEL TRATTAMENTO**

Il Titolare del trattamento è **Quinta Capital SGR S.p.A.**, con sede legale in Milano, Via Palestro 6, (di seguito, il “**Titolare**”).

Il Titolare può trattare, sia con l’ausilio di strumenti elettronici, sia senza l’ausilio di tali strumenti, la seguente tipologia di dati personali:

- Dati identificativi (es., nome, cognome, codice fiscale, residenza, ecc.);
- Dati particolari, limitatamente ai dati relativi alla salute e all’appartenenza sindacale;
- Dati relativi a condanne penali e reati (ex art. 10 del Regolamento Privacy).

## 5. RESPONSABILE DELLA PROTEZIONE DEI DATI

L'articolo 37, comma 1 del GDPR prevede che il Titolare, e/o responsabile del trattamento, debbano designare un Responsabile della protezione dei dati (“**RPD**”) o *Data Protection Officer* (“**DPO**”) se:

- a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
- b) le attività principali del Titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- c) le attività principali del Titolare del trattamento o del responsabile del trattamento consistano nel trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati.

La Società ha provveduto a nominare quale RDP lo [•].

## **6. NOMINA DEI RESPONSABILI DEL TRATTAMENTO DEI DATI**

Nello svolgimento delle proprie attività, la Società potrà avvalersi di soggetti esterni in relazione alle diverse esigenze professionali, previa nomina di tali soggetti esterni quali Responsabili del Trattamento dei Dati.

Il Titolare individua responsabili “esterni” del trattamento dei dati personali tra soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR 679/2016 e sia volto a garantire la tutela dei diritti degli interessati.

I compiti affidati al responsabile del trattamento dei dati personali sono disciplinati mediante un contratto che soddisfi le disposizioni di cui all’art. 28 GDPR.

## **7. PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI E FORMAZIONE**

Le Persone autorizzate al trattamento dei dati (soggetti previsto dagli art. 29 del GDPR) sono delle figure che operano sotto la diretta autorità del Titolare o del Responsabile, il cui compito si esplica nello svolgimento materiale delle operazioni relative al trattamento dati, attenendosi alle istruzioni che vengono loro impartite.

Il Titolare nomina le Persone autorizzate al trattamento dei dati sotto la sua autorità (dipendenti/collaboratori).

La designazione delle Persone autorizzate al trattamento dei dati è effettuata per iscritto e indica puntualmente l'ambito del trattamento consentito.

Il Titolare, anche in collaborazione con il RPD, cura la formazione delle persone autorizzate al trattamento in materia di protezione dei dati personali in occasione di rilevanti novità normative oppure ove richiesto da disposizioni aziendali.

## **8. MISURE DI SICUREZZA**

Nel quadro generale degli obblighi di protezione dei dati personali, la disciplina richiede l'adozione di misure di sicurezza tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio del trattamento, al fine di prevenire i rischi che possono derivare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il Titolare adotta misure di sicurezza diversificate a seconda che il trattamento avvenga con o senza l'ausilio di strumenti elettronici.

Il Titolare, al fine di garantire la sicurezza dei dati trattati, adotta policy e misure che regolano la gestione degli accessi ai sistemi informativi, l'uso della posta elettronica e degli strumenti elettronici, l'accesso ad Internet e la continuità operativa.

A tal proposito, si rimanda alla procedura Processi Amministrativi.

Quanto al trattamento senza l'ausilio di strumenti elettronici, il Titolare assicura la protezione dei dati trattati conformemente alle misure previste nella presente Policy.

## **9. REGISTRO DEI TRATTAMENTI**

Il Titolare, avvalendosi del RPD, tiene il registro delle attività di trattamento e delle categorie di attività trattate che contiene le informazioni richieste dall'art. 30, commi 1 e 2 del GDPR ed è redatto in conformità allo schema di cui all'Allegato 1 (Registro).

In merito, le strutture operative della SGR si impegnano a segnalare tempestivamente al RDP i nuovi Trattamenti e/o le modifiche dei Trattamenti esistenti che dovessero occorrere, tempo per tempo, nell'ambito delle attività proprie della Direzione/Funzione aziendale di riferimento.

Nella compilazione del registro delle attività di trattamento viene effettuata una valutazione relativa al livello di rischio che i singoli trattamenti posti in essere dal Titolare comportano. La metodologia utilizzata prevede la valutazione dell'impatto e delle conseguenze che una possibile violazione di tali dati avrebbe sui diritti e le libertà fondamentali degli interessati, associando tre livelli di impatto:

- basso: conseguenze irrilevanti in caso di violazione dei dati trattati dal Titolare;
- medio: conseguenze significative in caso di violazione dei dati trattati dal Titolare;
- alto: gravi conseguenze in caso di violazione dei dati trattati dal Titolare.

## **10. DATA PROTECTION IMPACT ASSESSMENT**

L'articolo 35 del GDPR ha introdotto l'istituto della "valutazione d'impatto sulla protezione dei dati" o "data protection impact assessment" (nel seguito "DPIA"). Tale istituto rappresenta un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. L'art. 35, comma 1 del GDPR prevede che il processo di DPIA sia obbligatorio quando un trattamento di dati personali, allorché preveda in particolare l'uso di nuove tecnologie, "presenti un rischio elevato per i diritti e le libertà delle persone fisiche". Inoltre, il comma 3 del suddetto articolo dispone che la valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Qualora un trattamento comportasse un rischio elevato per i diritti e le libertà degli Interessati, il Titolare, in relazione ai trattamenti dallo stesso effettuati, svolgerà una valutazione di impatto (DPA) e prima di darvi inizio consulterà l'autorità di controllo adottando specifiche misure tecniche e organizzative per mitigare l'impatto del trattamento. L'attività è condotta con il coinvolgimento del RPD.

## **11. MODALITÀ DI TRATTAMENTO – INFORMATIVA E CONSENSO**

### **11.1 Corretto Trattamento dei dati**

La SGR si impegna a rispettare i principi generali applicabili al trattamento; per tale ragione tutti i dati personali devono essere:

- i. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di liceità, correttezza e trasparenza);
- ii. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo non incompatibile con tali finalità (principio di limitazione della finalità);
- iii. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di minimizzazione dei dati);
- iv. esatti e, se necessario, aggiornati. Devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di esattezza);
- v. 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 (principio di limitazione della conservazione);
- vi. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principi di integrità e riservatezza).

Il trattamento è lecito solo se ricorre, almeno una delle seguenti condizioni:

- i. l'interessato ha espresso il proprio consenso;
- ii. il trattamento è necessario per eseguire un contratto di cui l'interessato è parte o per adempiere ad un obbligo precontrattuale;
- iii. il trattamento è necessario per adempiere ad un obbligo di legge;
- iv. il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- v. il trattamento è necessario per perseguire un legittimo interesse del titolare di terzi, salvo che prevalgano gli interessi o i diritti e le libertà dell'interessato.

## **11.2 Informativa**

L'art. 13 del GDPR prevede che il Titolare fornisca all'Interessato, dal quale vengono raccolti i dati personali, una serie di informazioni ivi tassativamente indicate, anche al fine di garantire un trattamento corretto e trasparente dei dati.

La Società, quando ottiene dati personali dai soggetti indicati per le diverse finalità da essa perseguite, fornisce ai medesimi l'informativa stabilita dal GDPR. L'informativa deve sempre indicare:

- i dati di contatto del titolare del trattamento e, ove designati, del responsabile del trattamento e del RDP;
- la finalità e le basi giuridiche del trattamento;
- i legittimi interessi perseguiti dal titolare del trattamento qualora costituiscano la base giuridica del trattamento;
- i diritti che gli Interessati possono esercitare;
- i destinatari o le categorie di destinatari cui i dati personali possono essere trasferiti;
- l'eventuale trasferimento dei dati in un territorio al di fuori dell'UE corredato dalle informazioni circa le misure che sono state o saranno attuate al fine di garantire un trattamento lecito e sicuro dei dati in conformità a quanto stabilito dal GDPR.

Il Titolare tiene aggiornata la modulistica relativa all'informativa sul trattamento dei dati personali di propria competenza.

Per quelle attività per cui la SGR agisce in qualità di Responsabile del trattamento, la Società non fornisce all'Interessato alcuna informativa. In tali casi, la Società, prima di cominciare a svolgere le proprie attività, si assicura che il Titolare del trattamento per il quale opera abbia ottemperato a tutti gli obblighi informativi richiesti dal GDPR.

## **11.3 Consenso**

Il consenso al trattamento dei dati personali è richiesto solo nei casi in cui il trattamento non abbia già una propria base giuridica ai sensi dell'art. 6 del GDPR. In particolare, il consenso è richiesto nel caso in cui i dati personali siano acquisiti per finalità diverse dall'adempimento di un obbligo di legge o dalla esecuzione di un contratto.

Ove acquisiti in formato cartaceo, i moduli relativi al consenso vengono archiviati unitamente alla documentazione cui essi si riferiscono e comunque nel pieno rispetto delle misure di sicurezza di cui alla presente Policy.

#### **11.4 Dati dei dipendenti/collaboratori**

Nel caso dei curricula che i soggetti in cerca di occupazione inviano spontaneamente alla Società in formato cartaceo o a mezzo e-mail, il Titolare di concerto con la Persona Autorizzata al trattamento che si occupa della candidatura, invia al candidato, al più tardi al momento del primo contatto utile del candidato, all'indirizzo email indicato sul curriculum, l'apposita informativa con la quale si informa il candidato dei diritti di cui gode ai sensi del GDPR.

## **12. MODALITÀ DI CONSERVAZIONE DEI DATI PERSONALI**

Gli atti e i documenti contenenti dati personali sono archiviati e conservati, a cura delle Persone di volta in volta a ciò autorizzate, in cartelle elettroniche a cui può accedere esclusivamente, oltre alle persone autorizzate stesse, il Titolare per lo svolgimento delle attività di propria competenza.

I documenti cartacei sono archiviati e conservati dalle Persone di volta in volta a ciò autorizzate in armadi muniti di serratura a cui possono accedere esclusivamente, oltre alle persone autorizzate stesse, il Titolare.

### **13. ESERCIZIO DEI DIRITTI DELL'INTERESSATO**

L'Interessato ha diritto di esercitare i propri diritti, così come previsto dal GDPR ovvero:

#### **13.1 Diritto di accesso**

L'Interessato ha diritto di ottenere 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 seguenti informazioni:

- a) le finalità del Trattamento;
- b) le categorie di Dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i Dati personali sono stati o saranno eventualmente comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei Dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'Interessato di chiedere al Titolare del Trattamento la rettifica o la cancellazione dei dati personali o la limitazione del Trattamento dei Dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un'autorità di controllo.
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'eventuale esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, del GDPR e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il Titolare, su richiesta dell'Interessato, fornisce una copia dei dati personali oggetto del trattamento.

In caso di ulteriori copie, ove richiesto, dall'Interessato, il Titolare può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'Interessato, le informazioni sono fornite in un formato elettronico di uso comune.

### **13.2 Diritto di rettifica**

L'Interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Tenuto conto della finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

### **13.3 Diritto alla cancellazione**

L'Interessato ha il diritto di ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei seguenti motivi:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'Interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
- c) l'Interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare.

Il Titolare, se ha reso pubblici dati personali ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'Interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Il diritto alla cancellazione non si applica nella misura in cui il trattamento sia necessario per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

### **13.4 Diritto di limitazione del trattamento**

L'Interessato ha il diritto di ottenere dal Titolare la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- a) l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare per verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) benché il Titolare non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- d) l'Interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, del GDPR in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'Interessato che ha ottenuto la limitazione del trattamento è informato dal Titolare prima che detta limitazione sia revocata.

### **13.5 Diritto alla portabilità dei dati**

L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, ove possibile, i dati personali che lo riguardano forniti al Titolare e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare che li ha forniti qualora:

- a) il trattamento si basi sul consenso o su un contratto;
- b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali dal Titolare ad un altro Titolare, se tecnicamente fattibile.

L'esercizio del diritto alla portabilità dei Dati lascia impregiudicato il diritto alla cancellazione.

### **13.6 Diritto di opposizione**

L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

### **13.7 Richieste di esercizio dei diritti**

Le richieste di esercizio dei propri diritti da parte dell'Interessato possono essere trasmesse mediante lettera raccomandata o posta elettronica come indicato nelle informative consegnate agli interessati.

Nel caso di ricezione di una richiesta di esercizio dei propri diritti, la stessa viene trattata con l'ausilio delle eventuali Persone Autorizzate al trattamento dei dati, provvedendo ad elaborare una proposta di riscontro.

Tale proposta viene sottoposta al RPD per le opportune verifiche ed eventuali integrazioni.

La risposta così elaborata viene inviata all'Interessato via PEC o raccomandata A/R. Se l'Interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salva diversa indicazione dell'Interessato.

Il Titolare trasmette la risposta all'Interessato senza ritardo e, al più tardi, entro un mese dal ricevimento della richiesta. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Titolare informa l'Interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Se non ottempera alla richiesta dell'Interessato, il Titolare informa l'Interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'Autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ed eventuali comunicazioni e azioni intraprese sono gratuite. Se le richieste dell'Interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare può:

- a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
- b) rifiutare di soddisfare la richiesta. Incombe sul Titolare l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Qualora il Titolare nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta per l'esercizio di un diritto, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'Interessato.

Il Titolare comunica agli eventuali destinatari cui sono stati trasmessi i dati personali, le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate ai sensi della presente Policy, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

## **14. DATA BREACH**

In caso di violazione dei dati personali, il Titolare notifica la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche la notifica di una violazione di dati personali, tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità pubblicato all'indirizzo <https://servizi.gpdp.it/>.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il Responsabile informa il Titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica deve almeno:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. comunicare il nome e i dati di contatto del responsabile della protezione dei dati, ove nominato, o di altro punto di contatto presso cui ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio anche al fine di consentire all'Autorità di controllo di effettuare le verifiche del caso in un apposito registro comprese le violazioni comunicate dai Responsabili del trattamento.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (come, ad esempio, quando tale violazione ha ad oggetto i dati

giudiziari di un Interessato), il Titolare comunica la violazione all'Interessato senza ingiustificato ritardo.

La comunicazione all'Interessato descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del Regolamento Privacy.

Non è richiesta la suddetta comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

- I. il Titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione;
- II. il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- III. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

## **15. CONTROLLI**

La verifica sull'applicazione delle misure di sicurezza per la protezione dei dati personali adottate dalla Società è effettuata dal Titolare con il supporto del RPD.

## **16. SANZIONI**

La violazione delle disposizioni del GDPR rilevanti per la SGR (come, a titolo esemplificativo, quelle concernenti i principi base del trattamento, l'adozione delle misure di sicurezza, la nomina del responsabile del trattamento, la tenuta del registro dei trattamenti, la notifica delle violazioni dei dati personali e dell'esercizio dei diritti degli interessati) può comportare, a seconda dei casi, l'applicazione di sanzioni amministrative pecuniarie:

- fino a 10.000.000 di euro o fino al 2% del fatturato totale annuo dell'esercizio precedente, se superiore;
- fino a 20.000.000 di euro o fino al 4% del fatturato totale annuo dell'esercizio precedente, se superiore.

## **17. MODIFICHE ALLA POLICY**

Il Titolare provvede, ove necessario, alla revisione della presente Policy con il supporto del RPD.

## ALLEGATI

Allegato 1 – Schema di registro dei trattamenti