Policy generale sulla protezione dei Dati personali

Società	Acetum S.B. S.p.A.
Sintesi	La presente Policy stabilisce le regole generali che disciplinano il Trattamento dei Dati personali da parte della società o di terzi per suo conto
Versione	1.0
Data di pubblicazione	
Contatti	privacy@acetum.it

Sommario

1 DEFINIZIONI

Ai fini della presente Policy, ove non diversamente specificato, i termini di seguito elencati hanno il significato per ciascuno di essi di seguito attribuito:

- «**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.
- «**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.
- «**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.
- «**Codice in materia di protezione dei Dati personali**»: D.lgs. 196/2003 così come modificato e integrato da ultimo dal D.lgs. 101/2018.
- «**GDPR**»: Regolamento (UE) 679/2016 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.
- «**Interessato**»: persona fisica cui si riferiscono i Dati personali.
- «**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.
- «**Titolare del Trattamento o Titolare**»: 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.
- «**Coordinatore per la protezione dei dati**»: la funzione individuata dal Titolare del Trattamento quale responsabile delle tematiche privacy all'interno della realtà aziendale nei termini indicati nella presente Policy. Il Coordinatore per la protezione dei dati può a sua volta individuare Referenti Privacy e Persone Autorizzate al trattamento che lo supportino nella gestione degli adempimenti privacy richiesti dalla normativa applicabile.
- «**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 e con la quale viene stipulato un contratto di nomina ai sensi dell'art. 28 del GDPR.
- «**Referente Privacy**»: responsabile di funzione / area che viene autorizzato dal Titolare al Trattamento dei dati personali ai sensi dell'art. 29 del GDPR.
- «**Persona autorizzata**» Funzione subordinata al responsabile di funzione / area che viene autorizzata dal Titolare al Trattamento dei dati personali ai sensi dell'art. 29 del GDPR.

- «**Soggetto Terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del Trattamento, il Referente Privacy, le Persone Autorizzate e il Responsabile del Trattamento.
- «**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.

I termini definiti al singolare si intendono anche al plurale ove il contesto lo richieda e viceversa.

2 INTRODUZIONE E SCOPO

Acetum S.B. S.p.A. (in seguito, la «**Società**»), in qualità di Titolare, è responsabile della protezione delle informazioni e dei Dati personali oggetto di operazioni di Trattamento effettuate per suo conto, anche da parte di Soggetti Terzi, e ai sensi del GDPR è tenuta a garantire la sicurezza e la confidenzialità dei Dati personali trattati nell'ambito delle proprie attività.
Lo scopo della presente Policy è di assicurare che il Trattamento dei Dati personali da parte della Società avvenga nel rispetto delle previsioni vigenti in tema di protezione dei dati, garantendo la protezione dei diritti e delle libertà degli Interessati fin dalla progettazione del Trattamento e dei suoi mezzi.

3 AMBITO DI APPLICAZIONE E DESTINATARI

La presente Policy si applica ai membri del Consiglio di Amministrazione e ai soggetti facenti parte del vertice aziendale della Società, ai dipendenti ed ai collaboratori («Destinatari»).

Nel caso in cui uno dei Destinatari ponga in essere azioni in violazione del GDPR o di altra normativa privacy applicabile, la Società potrebbe essere soggetta a significative sanzioni, penali o amministrative, anche pecuniarie, nonché incorrere in rilevanti danni reputazionali e di immagine.

Pertanto, il rispetto della presente Policy è obbligatorio per tutti i Destinatari e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

In caso di dubbi o criticità circa l'applicazione della presente Policy i Destinatari potranno rivolgersi al Coordinatore per la protezione dei dati ai seguenti contatti privacy@acetum.it.

4 ATTUAZIONE E PIANO DI REVISIONE

La presente Policy è immediatamente efficace e in vigore alla data della sua pubblicazione e viene messa a conoscenza dei destinatari tramite formazione e diffusione attraverso portale aziendale.

La presente Policy potrà essere oggetto di aggiornamenti o revisioni in seguito a:

(i) eventi di violazione di Dati personali;

(ii) modifiche organizzative interne alla Società;

(iii) pianificazione di nuove operazioni di Trattamento che presentano rischi diversi o ulteriori;

(iv) modifiche legislative;

(v) pubblicazioni di decisioni giudiziarie;

(vi) emissioni di nuovi pareri o linee guida da parte delle autorità competenti.

La Società si impegna in ogni caso a effettuare una revisione periodica della presente Policy al fine di verificare che siano soddisfatti gli obiettivi perseguiti dalla stessa. L'aggiornamento potrà avvenire anche indirettamente tramite aggiornamento dei documenti collegati tramite appositi link presenti all'interno della presente Policy.

5 NORMATIVA DI RIFERIMENTO

La Società è tenuta a rispettare le normative, i provvedimenti giudiziari, i pareri e le linee guida in tema di protezione di Dati personali vigenti in Italia e in Unione Europea, nonché negli eventuali Paesi Terzi in cui la società compia operazioni di Trattamento, tra cui:

- Regolamento (Ue) 679/2016 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;
- Decreto legislativo 196/2003 (Codice in materia di protezione dei Dati personali), così come modificato ed integrato, da ultimo dal Decreto Legislativo 101/2018;
- Linee guida e provvedimenti del Garante per la Protezione dei Dati personali;
- Pareri e le Linee Guida del EDPB - Comitato europeo per la Protezione dei Dati che è un organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del Regolamento generale sulla Protezione dei Dati e promuovere la cooperazione tra le autorità di protezione dei dati dell'UE.

6 ORGANIZZAZIONE, RESPONSABILITÀ E PRINCIPI APPLICABILI AL TRATTAMENTO

La Società in qualità di Titolare è tenuta a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il Trattamento è effettuato conformemente al GDPR, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del Trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà degli Interessati.

Il Titolare definisce una gerarchia di responsabilità e competenze in relazione alla protezione dei Dati personali, individuando tra i dipendenti o tra i consulenti dell'azienda, persone capaci ed affidabili a cui delegare in tutto o in parte la gestione del Trattamento dei Dati personali.

Le scelte della Società in materia di organizzazione interna sono riportate all'interno dell'organigramma privacy individuato e contenuto nell' **All.1 – Organigramma Privacy**. La Società ha individuato un unico Coordinatore per la protezione dei dati, Referenti Privacy per ogni Funzione. Il Coordinatore per la protezione dei dati ha a sua volta individuato un Referente Privacy e una Persona Autorizzata al trattamento che lo supportano nella gestione degli adempimenti privacy richiesti dalla normativa applicabile. I riferimenti al Coordinatore per la protezione dei dati sono pertanto da leggersi come riferimenti comprensivi anche delle risorse interne di cui lo stesso si avvale per la gestione degli adempimenti privacy a cui è tenuta la Società. Per ulteriori dettagli si rinvia a quanto riportato all'interno della Politica sulla protezione dei dati di ABF (Europa).

7 LICEITÀ DEL TRATTAMENTO, INFORMATIVA E CONSENSO

I destinatari della presente Policy devono sempre verificare che il Trattamento di Dati personali dagli stessi effettuato sia lecito. Il Trattamento può essere considerato lecito solo al verificarsi di specifiche condizioni previste dalla legge («**basi giuridiche del Trattamento**»), tra cui:

a) l'Interessato ha espresso il consenso al Trattamento dei propri Dati personali per una o più specifiche finalità;

b) il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il Trattamento è necessario per adempiere un obbligo legale;

d) il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare del Trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato.

Qualora il Trattamento sia basato sul consenso, è necessario che questo sia rilasciato per iscritto dal soggetto Interessato, in maniera esplicita, libera e informata.

La richiesta di consenso deve essere presentata al soggetto in modo chiaramente distinguibile, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, e l'Interessato ha il diritto di revocare il proprio consenso in qualsiasi momento con la stessa facilità con cui il consenso è stato accordato.

Qualora il Trattamento sia basato sul legittimo interesse, è necessario effettuare apposito test di bilanciamento sul legittimo interesse, seguendo quanto riportato nelle **Brief Guidance Note on Use of Legittimate Interests Assessments.**

Qualora la raccolta dei Dati personali avvenga presso l'Interessato, i Destinatari della presente Policy dovranno accertarsi, nel momento in cui i Dati personali sono ottenuti, di aver fornito all'Interessato un documento di informativa contenente tutte le informazioni relative al Trattamento (tra cui l'identità e i dati di contatto del Titolare del Trattamento, le finalità del Trattamento, gli eventuali destinatari dei Dati personali; l'intenzione del Titolare del Trattamento di trasferire Dati personali a un paese terzo o a un'organizzazione internazionale etc..).

La documentazione privacy aggiornata (documenti di informativa privacy e moduli per la richiesta del consenso) della Società può essere reperita contattando privacy@acetum.it.

8 TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

I Destinatari della presente Policy sono chiamati a prestare particolare attenzione al Trattamento di Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale delle persone.

Infatti, tale Trattamento è da considerarsi sempre **vietato** salvo il verificarsi di particolari condizioni, tra cui il consenso esplicito dell'Interessato al Trattamento di tali Dati personali per una o più finalità specifiche. Altre condizioni che legittimano il Trattamento di tali categorie particolari di Dati personali sono previste dalla normativa vigente.

Al fine di ricevere il necessario supporto, i Destinatari sono pregati di rivolgersi sempre al Coordinatore per la protezione dei dati della Società qualora debbano effettuare per la prima volta il Trattamento di categorie particolari di Dati personali.

9 TRATTAMENTO DEI DATI DELLA SOCIETÀ TRAMITE TERZE PARTI

Il GDPR attribuisce estrema rilevanza al trattamento dei dati da parte di soggetti terzi individuando le "responsabilità privacy" del Titolare e del Responsabile del Trattamento. Qualora la Società intenda avvalersi di un soggetto esterno/fornitore di servizi per l'esecuzione di attività, svolte in nome e per conto del Titolare, che richiedano il trasferimento, la comunicazione o qualsiasi altro Trattamento di Dati personali, è necessario:

- avvalersi di fornitori che forniscono idonee garanzie in merito al rispetto della normativa privacy vigente e all'adozione di adeguate misure di sicurezza tecniche e organizzative al fine di tutelare i diritti degli Interessati;
- che i fornitori si impegnino a manlevare e tenere indenne il Titolare da qualunque responsabilità o danno causato alle persone fisiche nello svolgimento del Trattamento dei Dati personali;
- che i fornitori sottoscrivano, in qualità di Responsabile del Trattamento, apposito contratto di Trattamento dei dati per conto del Titolare.

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 contenuto è definito all'interno dell'art. 28 GDPR.

La documentazione privacy aggiornata relativa ai rapporti con i fornitori (contratti, clausole privacy, contratto tra Titolare e Responsabile del Trattamento) della Società può essere reperita al seguente scrivendo a privacy@acetum.it.

Il trattamento di Dati personali della Società per il tramite di terze parti dovrà avvenire nel rispetto delle seguenti policy:

- Politica di outsourcing a terze parti della sicurezza delle informazioni del Gruppo
- Valutazione del trattamento di terze parti

10 CONSERVAZIONE DEI DATI

I documenti, sia cartacei che in formato elettronico, contenenti Dati personali devono essere conservati per il periodo di tempo eventualmente previsto da leggi o regolamenti e, comunque, per un periodo **non superiore** a quello strettamente necessario per le finalità perseguite. La Società è tenuta a individuare per ogni tipo di Trattamento e di dato trattato il periodo di conservazione dei Dati personali oppure, qualora non sia possibile, i criteri utilizzati per determinare di volta in volta tale periodo. A tale scopo i Destinatari sono tenuti a rispettare le tempistiche di conservazione dei Dati come indicate nel Registro dei trattamenti.

11 MISURE DI SICUREZZA

Ai sensi dell'art. 32 del GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, la Società deve mettere in atto misure tecniche e organizzative idonee per garantire un livello di sicurezza **adeguato** al rischio.

Con riferimento alle misure di sicurezza, la Società ha adottato procedure e policy specifiche, si richiamano in particolare la Politica sulla sicurezza delle informazioni di ABF e le misure tecniche ed organizzative indicate all'interno del Registro dei trattamenti adottato dalla Società.

12 DIRITTI DELL'INTERESSATO

Ai fini dell'applicazione della presente Policy, si considerano Interessati tutte le persone fisiche identificate o identificabili (ivi comprese le società di persone) i cui Dati personali sono trattati dalla Società nell'ambito delle sue attività o da terzi per conto della Società.

A titolo esemplificativo, Interessati possono essere i clienti, i fornitori, i consulenti e i dipendenti della Società.

Ai sensi degli articoli 15-22 del GDPR, gli Interessati possono esercitare, con richiesta rivolta senza formalità nei confronti della Società, anche per il tramite di un delegato, i seguenti diritti:

12.1 Diritto di accesso dell'Interessato

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 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 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'esistenza di un processo decisionale automatizzato, compresa la profilazione, e almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale Trattamento per l'Interessato;

i. qualora i Dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.

Il diritto di accesso comprende anche quello di ricevere copia dei Dati personali oggetto di Trattamento, salvo che l'esercizio di tale diritto non leda i diritti e le libertà altrui.

12.2 Diritto di rettifica

L'Interessato ha 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.

12.3 Diritto alla cancellazione («diritto all'oblio»)

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

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 del Trattamento;

f. i Dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Tale diritto è escluso nei limitati casi elencati nell'art. 17, comma 3 del GDPR (ad esempio, quando la conservazione dei dati è necessaria per l'adempimento di un obbligo legale o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria).

12.4 Diritto di limitazione di Trattamento

L'Interessato ha il diritto di ottenere dal Titolare del Trattamento 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 del Trattamento 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 del Trattamento 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, 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 possono essere trattati solo con il consenso dell'Interessato o nei limitati casi elencati nell'art. 18, comma 2 del GDPR. L'Interessato deve essere informato se la limitazione è revocata.

12.5 Diritto alla portabilità dei dati

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

a. il Trattamento si basi sul consenso o su un contratto di cui l'Interessato è parte (o è necessario nel contesto di misure precontrattuali per un simile contratto);

b. il Trattamento sia effettuato con mezzi automatizzati;

c. l'esercizio del diritto non leda i diritti e le libertà altrui.

L'Interessato ha il diritto di ottenere la trasmissione diretta dei Dati personali da un Titolare del Trattamento all'altro, se tecnicamente fattibile.

12.6 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, compresa la profilazione. Il Titolare del

Trattamento pertanto deve astenersi 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.

Qualora i Dati personali siano trattati per finalità di marketing diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al Trattamento dei Dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'Interessato si opponga al Trattamento per finalità di marketing diretto, i Dati personali non possono essere più oggetto di Trattamento per tali finalità.

Nel caso in cui l'Interessato si opponga ad una decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, l'Interessato ha diritto di ottenere l'intervento umano da parte del Titolare, di esprimere la propria opinione e di contestare la decisione.

12.7 Piano di gestione dell'istanza per l'esercizio dei diritti dell'Interessato

1) Ricezione dell'istanza dell'Interessato

Chiunque tra i Destinatari riceva, in qualsiasi formato cartaceo o elettronico, una istanza anche non formale da parte di un Interessato contenente la richiesta di esercitare uno dei diritti riconosciuti dalla normativa privacy vigente, è tenuto ad **informare tempestivamente per iscritto - entro 24 ore** il Referente Privacy dell'area alla quale appartiene il quale avvisa il Coordinatore per la protezione dei dati scrivendo a privacy@acetum.it.

In particolare, una richiesta di esercitare uno dei diritti riconosciuti dalla normativa privacy vigente può avvenire con le seguenti modalità:

- *richiesta di persona;*
- *richiesta via telefono;*
- *richiesta via posta;*
- *richiesta via fax;*
- *richiesta via mail o PEC;*

e può essere indirizzata a qualunque dipendente della Società (autorizzato al Trattamento).

1) Verifica dell'identità dell'Interessato

Il Referente Privacy verifica l'identità dell'Interessato sulla base di idonei elementi di valutazione. Qualora il Referente Privacy nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'Interessato, quali atti o documenti disponibili o richiedendo l'esibizione o l'allegazione di copia di un documento di riconoscimento. Qualora l'Interessato agisca tramite un delegato, il Referente Privacy richiede copia della procura o della delega sottoscritta e presentata unitamente a copia di un documento di riconoscimento dell'Interessato.

Nel caso di mancato riscontro alla richiesta di conferma dell'identità dell'Interessato, la Società potrà trovarsi nell'impossibilità materiale di riscontrare la richiesta. In tal caso, il Coordinatore per la protezione dei dati procederà a comunicare all'Interessato tale circostanza.

2) Ricerca dei dati

Salva diversa disposizione espressa del Coordinatore per la protezione dei dati, il Referente Privacy verifica la completezza e la correttezza della documentazione a supporto della richiesta.

La normativa privacy prevede esplicitamente che, ove non fossero precisati i Dati cui l'Interessato intende accedere, il riscontro debba essere fornito su tutti i Dati, comprese le categorie particolari di Dati, trattati dal Titolare che riguardano l'Interessato.

A tale scopo, la ricerca dei Dati nelle banche dati aziendali coinvolge anche le altre unità organizzative che trattano Dati personali.

Qualora sia presentata una richiesta di accesso ai propri Dati da parte dell'Interessato, con riferimento all'indicazione dei destinatari dei Dati, il Titolare è tenuto a indicarne le categorie. Nel caso in cui, invece, l'Interessato richieda espressamente l'indicazione dei soggetti terzi a cui sono stati comunicati i propri Dati, occorre fornirgli le seguenti informazioni riferite a ciascun destinatario:

- nome e cognome o ragione sociale;
- partita IVA;
- Dati trasferiti;
- base giuridica del trasferimento Dati;
- finalità del trasferimento Dati;
- in caso di trasferimento dei Dati al di fuori dell'Unione Europea: paese terzo in cui vengono trasferiti e garanzie poste alla base di tale trasferimento ai sensi degli artt. 45 e ss. del GDPR.

3) Piano di gestione della richiesta

Una volta verificata l'identità dell'Interessato, il Referente Privacy trasmette la documentazione annessa alla richiesta al Coordinatore per la protezione dei dati.

Il Coordinatore per la protezione dei dati, unitamente al Referente Privacy (dell'area IT) e al Responsabile della Funzione IT, (in seguito anche collettivamente «***Unità Privacy***») prende in carico la richiesta avanzata dall'Interessato valutandone l'ammissibilità in conformità alle disposizioni del GDPR, nonché la fattibilità e individuando le competenze necessarie per darvi riscontro secondo le tempistiche previste al successivo punto 5) "*Riscontro alla richiesta dell'Interessato"* del presente paragrafo.

La stima della fattibilità e della complessità della richiesta è condotta valutando parametri che comprendono, a titolo esemplificativo, le fonti da cui reperire i dati personali e la tipologia di operazioni da svolgere per soddisfare la richiesta (anche dal punto di vista tecnico).

Dall'analisi della richiesta potrebbero verificarsi le seguenti ipotesi:

- Nel caso in cui il Titolare non sia in grado di ottemperare alla richiesta dell'interessato, perché non fattibile, il Coordinatore per la protezione dei dati 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.
- Nel caso in cui il tempo previsto per l'evasione sia inferiore o pari ad un mese, il Coordinatore per la protezione dei dati comunica all'interessato che il Titolare fornirà le informazioni richieste entro un mese dal ricevimento della stessa.
- Nel caso in cui il tempo previsto sia superiore al mese, il Coordinatore per la protezione dei dati comunica all'interessato che il Titolare prorogherà di due mesi il termine previsto per fornire le informazioni richieste.

Il Coordinatore per la protezione dei dati coinvolge nella gestione della richiesta i Referenti Privacy e le Persone Autorizzate eventualmente coinvolti nel Trattamento, nonché le ulteriori funzioni competenti rispetto alle richieste contenute nell'istanza e, qualora necessario e se presente, il Responsabile del Trattamento nominato ai sensi dell'art. 28 del GDPR.

L'Unità Privacy individua un piano di gestione della richiesta tenendo conto delle competenze, anche tecniche, necessarie a darvi riscontro e impartisce per iscritto compiti specifici alle funzioni coinvolte (a titolo esemplificativo: cancellare i dati contenuti in uno specifico database; eliminare e-mail del cliente da una specifica mailing list; preparare supporto contenente i Dati di un cliente per la portabilità a un nuovo Titolare, etc.).

I soggetti coinvolti sono chiamati a effettuare le azioni necessarie al fine di dare riscontro alle richieste dell'Interessato secondo le indicazioni impartite dall'Unità Privacy.

L'Unità Privacy provvede a raccogliere i Dati da fornire al richiedente.

In caso di richiesta di **portabilità**, l'Unità Privacy deve fare una preliminare valutazione per verificare che la trasmissione dei Dati ad un altro Titolare non leda i diritti e le libertà altrui. Previo esito positivo di tale verifica, la Funzione IT provvederà ad estrarre dalla banca dati tutti i Dati forniti dall'Interessato direttamente su un file (formato .txt, .xls, .pdf, etc.) da consegnare allo stesso.

È importante tener presente che oggetto del diritto di portabilità sono i Dati consapevolmente e attivamente forniti dall'Interessato (ad esempio, indirizzo postale, nome utente, età, …) e i Dati "osservati" ossia quelli indirettamente forniti dall'Interessato attraverso la fruizione di un servizio (ad esempio, la cronologia delle ricerche effettuate, dati relativi all'ubicazione). Non sono oggetto del diritto di portabilità i cosiddetti Dati "inferenziali e derivati" creati dal Titolare sulla base dei Dati forniti dall'Interessato.

Quindi, sono inclusi nel diritto alla portabilità i Dati personali relativi ad attività compiute dall'Interessato o derivante dall'osservazione del comportamento del medesimo, ma sono esclusi quei Dati creati dal Titolare nell'ambito del Trattamento, per esempio attraverso procedure di personalizzazione, di categorizzazione o profilazione.

Una volta espletate tutte le azioni necessarie al fine di ottemperare alle richieste dell'Interessato, i soggetti coinvolti comunicano per iscritto all'Unità Privacy le misure tecniche adottate.

4) Riscontro alla richiesta dell'Interessato

La risposta deve essere intelligibile, concisa, trasparente e facilmente accessibile, espressa in linguaggio semplice e chiaro.

Dovendo la Società conservare traccia della risposta, quest'ultima va inoltrata direttamente al richiedente tramite:

- posta raccomandata con ricevuta di ritorno;
- fax:
- e-mail.

Non è pertanto consentito comunicare i dati in forme che non permettano di provare la comunicazione fornita.

Una volta espletate tutte le azioni necessarie al fine di dare riscontro alle richieste dell'Interessato, l'Unità Privacy comunica per iscritto all'Interessato - ove possibile con mezzi elettronici, salvo diversa indicazione dell'Interessato – i Dati eventualmente richiesti e le informazioni relative alle azioni intraprese, **entro un mese** dal ricevimento della richiesta stessa.

La risposta ad una richiesta di accesso a Dati conservati deve riguardare tutti quelli attinenti al richiedente identificabile e può comprendere eventuali Dati riferiti a terzi solo nei limiti in cui la scomposizione dei Dati trattati o la privazione di alcuni elementi renda incomprensibili i Dati personali relativi al terzo.

In caso di particolare complessità della richiesta, l'Unità Privacy comunica all'Interessato la necessità di prorogare (**al più tardi, di due mesi**) il riscontro all'istanza inviata unitamente ai motivi della proroga.

Ai sensi dell'art. 12 del GDPR il Titolare, in caso di richieste manifestamente infondate o eccessive, 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.

5) Notifica in caso di rettifica o cancellazione di Dati personali o limitazione del Trattamento

In caso di rettifica o cancellazione di Dati personali o limitazione del Trattamento, l'Unità Privacy deve provvedere a comunicare a ciascuno dei destinatari cui sono stati trasmessi i Dati personali le eventuali rettifiche o cancellazioni o limitazioni del Trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Qualora l'Interessato lo richieda, si provvede a comunicare al medesimo tali destinatari.

Di tali comunicazioni viene conservata copia dal Coordinatore per la protezione dei dati.

6) Registro delle richieste di esercizio dei diritti da parte degli Interessati

Il Titolare del Trattamento deve essere in grado di documentare tutte le richieste ricevute, al fine di poter dimostrare che il trattamento dei dati è effettuato conformemente alla normativa privacy applicabile.

A tal fine il Coordinatore per la protezione dei dati deve compilare altresì l'**All. 2 – Registro delle Richieste di esercizio dei diritti da parte degli Interessati** in cui devono di volta in volta essere registrati tutti i dati, le informazioni e le circostanze riguardanti le richieste di esercizio dei diritti da parte degli Interessati.

13 VALUTAZIONE DEL RISCHIO SULLA PROTEZIONE DEI DATI PERSONALI NEI PROGETTI

Nel caso di analisi e successiva implementazione di un progetto o di un'attività, si rende necessario verificare l'impatto che tale iniziativa ha sulle tematiche privacy. In particolare, a fronte di un nuovo trattamento di dati personali o di modifiche sostanziali a trattamenti esistenti, la normativa richiede di valutare il livello di rischio e le misure idonee a mitigarlo.

La Funzione responsabile delle attività di cui ai paragrafi 14.1 e 14.2 che seguono è il Coordinatore per la protezione dei dati, unitamente al Referente Privacy dell'area interessata dal Progetto, in coordinamento con il responsabile IT.

13.1 Privacy by design e privacy by default

Il GDPR prevede che, al fine di proteggere i diritti e le libertà degli Interessati e prevenire trattamenti in violazione del GDPR, il Titolare del Trattamento:

- valuti i rischi inerenti al Trattamento effettuato nell'ambito delle attività aziendali, sia direttamente che per conto di terzi;
- attui misure di sicurezza organizzative e tecniche idonee a limitare tali rischi e ad assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi presenti nei trattamenti e alla natura dei Dati personali da proteggere.

In particolare, il Titolare del Trattamento è tenuto a rispettare i seguenti principi:

- **privacy by design** richiede che il Titolare, sia nella fase di studio che di progettazione sia nell'esecuzione del Trattamento stesso, adotti misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati;
- **privacy by default** la quale presuppone che il Titolare metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i Dati personali strettamente necessari al perseguimento delle finalità specifiche del Trattamento.

Di seguito si riportano le fasi in cui è possibile dare attuazione ai principi di Data Protection by Design / Data Protection by Default. A fronte di

- **una nuova attività o servizio**
- **modifica significativa ad attività e servizi esistenti**

che comportino un trattamento di dati personali (in seguito il "**Progetto**"), occorre porre in essere le azioni di cui alle fasi in seguito descritte.

Fasi	**Obiettivo**
1) Analisi di contesto del Progetto	Assicurare la raccolta di tutte le informazioni relative al possibile trattamento dei dati, in particolare: – tipologie di interessati; – tipologie di dati trattati; – finalità del trattamento; – modalità del trattamento; – funzioni che trattano i dati; – categorie di destinatari; – eventuale trasferimento dei dati extra UE; – tempi di conservazione dei dati; – base giuridica del trattamento.
2) Individuazione misure tecniche e organizzative	Individuare le misure di sicurezza tecniche e organizzative necessarie per assicurare la conformità ai requisiti di protezione dei dati personali e predisporre un piano degli eventuali interventi.
3) Determinazione della necessità di una DPIA	Assicurare la corretta valutazione della necessità o meno di effettuare una DPIA sul trattamento di dati personali di cui al Progetto e valutare il livello di rischio e le misure idonee a mitigarlo. Questa fase è maggiormente dettagliata nel paragrafo 14.2 che segue denominato "*Valutazione D'Impatto*".
4) Report	Definizione di un report da cui risultino descritte le attività effettuate nelle fasi precedenti, le azioni intraprese e/o da intraprendere nonchè l'approvazione o meno del progetto
5) Implementazione del piano di interventi	Assicurare la realizzazione delle misure di sicurezza tecniche e organizzative per la protezione dei dati personali, identificate nelle fasi precedenti, prevedendo che l'implementazione di tali misure sia effettuata in maniera integrata con gli interventi di realizzazione e avvio del Progetto.

13.2 Data Protection Impact Assessment

Alcuni tipi di Trattamento potrebbero presentare particolari rischi "**elevati**" per i diritti e le libertà degli Interessati, tali da dover giustificare la predisposizione di una Valutazione d'Impatto sulla protezione dei dati. Per ulteriori dettagli si rimanda a:

Valutazione d'impatto sulla protezione dei dati

Data Protection Impact assessment guidance notes

14 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

La Società mantiene un registro delle attività di Trattamento dei Dati personali in qualità di Titolare, che contiene le seguenti informazioni:

- il nome e i dati di contatto del Titolare del Trattamento e, ove applicabile, del conTitolare del Trattamento, del rappresentante del Titolare del Trattamento;
- le finalità del Trattamento;
- una descrizione delle categorie di Interessati e delle categorie di Dati personali;
- le categorie di destinatari a cui i Dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di Dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di Dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR;
- le basi giuridiche del trattamento individuate ai sensi degli artt. 6 e 9 del GDPR

La Società incarica il Coordinatore per la protezione dei dati all'aggiornamento del registro delle attività del Trattamento svolte in qualità di Titolare.

Le Funzioni della Società sono tenute a comunicare tempestivamente qualsiasi modifica / aggiornamento in merito alle attività di trattamento che interessano le proprie mansioni.

15 VIOLAZIONE DEI DATI PERSONALI (*DATA BREACH*)

La gestione e la notifica/comunicazione di incidenti relativi alla sicurezza dei Dati che possono causare la violazione di Dati personali è disciplinata all'interno:

Politica di gestione delle violazioni della protezione dei dati ABF

Quadro di risposta agli incidenti sulla sicurezza delle informazioni di ABF

Tra i possibili incidenti si ricordano a titolo esemplificativo:

- ⇨ *perdita o furto di strumenti IT (pc, smartphone, chiavette USB, hardware);*
- ⇨ *rivelazione di informazioni a soggetti non autorizzati;*
- ⇨ *accesso non autorizzato ai Dati personali;*
- ⇨ *violazione delle misure di sicurezza fisiche dei locali dove i Dati personali sono archiviati;*

- ⇨ *caricamento/divulgazione per errore di Dati personali in rete;*
- ⇨ *errore umano (per esempio: perdita di Dati personali archiviati presso luoghi non sicuri);*
- ⇨ *mancata previsione di eventi di rischio per la sicurezza dei dati quali allagamenti o incendi;*
- ⇨ *attacco esterno ai sistemi IT aziendali;*
- ⇨ *reati informatici.*

16 TRASFERIMENTO DI DATI EXTRA UE

Il legislatore europeo, considerata la crescita di flussi transfrontalieri di dati, ovvero di trasferimenti di dati personali verso destinatari soggetti a una giurisdizione differente da quella europea, e per garantire comunque un livello di sicurezza adeguato, impone con gli artt. 44 e seguenti del GDPR determinate condizioni affinché un trasferimento di dati verso paesi terzi possa essere effettuato.

Nel caso di un nuovo progetto, un nuovo trattamento di dati, la scelta di un fornitore e/o comunque di un soggetto esterno, la funzione coinvolta dovrà verificare se le attività comportano un trasferimento dei dati al di fuori dell'unione europea. Tale attività di verifica dovrà coinvolgere anche gli eventuali soggetti terzi di cui il fornitore si avvale per l'esecuzione dell'incarico.

Tale verifica dovrà essere sottoposta al successivo controllo del Coordinatore per la protezione dei dati per individuare gli adempimenti da porre in essere.

In particolare, il trasferimento dei dati personali verso Paesi terzi non è mai consentito, ad eccezione di situazioni ordinarie ed eccezionali elencate nel seguito.

Il trasferimento dei dati personali dell'Interessato in paesi diversi da quello di raccolta può avvenire, ad esempio, nei seguenti casi:

a) se il trasferimento avviene verso paesi che garantiscano un adeguato livello di protezione dei dati personali. In particolare, ai sensi dell'art. 45 del GDPR, il trasferimento è ammesso e non necessita di autorizzazioni specifiche se la Commissione, mediante atti di esecuzione, decide che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato (**Decisione di adeguatezza sul livello di protezione**). Al seguente link sono presenti le Decisioni di adeguatezza in vigore: https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero. In particolare, per il trasferimento dei dati dall'Unione Europea agli Stati Uniti, è in vigore la Decisione di adeguatezza del 10 luglio 2023. Pertanto, per ciascun fornitore con sede negli Stati Uniti, il Coordinatore per la protezione dei dati deve verificare che sia iscritto al Data Privacy Framework di cui al seguente link https://www.dataprivacyframework.gov/s/participant-search.

b) se il trasferimento è soggetto a garanzie adeguate. Possono considerarsi garanzie adeguate ai sensi dell'art. 46 par. 2 del GDPR **le norme vincolanti di impresa** (in seguito "BCR" – Binding Corporate Rules) qualora il trasferimento avvenga tra società facenti parte dello stesso gruppo d'impresa, le **clausole contrattuali standard** adottate dalla Commissione o dalle autorità di controllo, **codici di condotta** o **certificazioni**.

In tale ultimo caso il trasferimento potrà avvenire se accompagnato da una valutazione sull'impatto dello stesso. Sul punto si rimanda a: **Guidance on the use of Transfer Impact Assessments.**

Inoltre, in **via eccezionale** e in mancanza di una decisione di adeguatezza o di garanzie adeguate, comprese le norme vincolanti d'impresa, il trasferimento dei dati personali al di fuori dell'UE può avvenire ai sensi dell'art. 49 del GDPR nei seguenti casi:

a) se il trasferimento dei dati personali si basa sul consenso espresso dell'Interessato e, se si tratta di dati particolari, in forma scritta;

b) se il trasferimento risulta essere necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'Interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'Interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'Interessato;

c) se il trasferimento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto Aziendale e industriale.

In mancanza delle condizioni che legittimano il trasferimento extra UE sopra elencate e di cui agli artt. 45 e ss., tale operazione di trattamento è ammessa solo se non è ripetitiva, se riguarda un numero limitato di Interessati ed è necessaria per il perseguimento di interessi legittimi cogenti del Titolare del Trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'Interessato, e qualora il Titolare del Trattamento abbia valutato tutte le circostanze relative al trasferimento e, sulla base di tale valutazione, abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. In tali occasioni, il Titolare informa comunque l'Autorità Garante e, oltre all'informativa "standard", mette a conoscenza l'Interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

17 PRESIDI DA ATTUARE IN OCCASIONE DI EVENTUALI ISPEZIONI DEL GARANTE PRIVACY

Nel caso in cui la Società sia oggetto di ispezione, di verifica o di richiesta di accertamento da parte del Garante Privacy, si specificano, quali ulteriori e specifici presidi di controllo, le seguenti modalità:

a) il soggetto incaricato di intrattenere rapporti con il Garante Privacy è il Titolare del Trattamento dei dati, in persona del legale rappresentante della Società nella persona del Coordinatore per la protezione dei dati;
b) deve essere fornita da parte di tutta la struttura aziendale la massima e trasparente collaborazione agli ispettori e deve essere tenuta evidenza degli incontri avvenuti con il Garante o con suoi delegati, delle richieste dagli stessi ricevute e della documentazione consegnata;
c) alla luce degli esiti dell'ispezione, della verifica o della richiesta di accertamento, il Titolare assieme al Coordinatore per la protezione dati deve definire le eventuali iniziative da assumere o le azioni correttive da intraprendere.

18 FORMAZIONE

La formazione dei Referenti Privacy e delle Persone Autorizzate al Trattamento è obbligo di legge e deve essere evasa tramite corsi interni da tenersi almeno periodicamente sui seguenti argomenti:

- le norme applicabili alla protezione dei Dati personali ed ogni altra normativa pertinente anche a specifiche attività di Trattamento;
- le modalità operative riportate nella presente Policy nonché i documenti allegati.

Ogni corso sarà seguito da una prova. In caso di non superamento della prova, il corso dovrà essere ripetuto fino al superamento della prova.

19 ALLEGATI E DOCUMENTI COLLEGATI

Sono allegati alla presente Policy:

- All.1 – Organigramma Privacy
- All.2 – Registro delle Richieste di esercizio dei diritti da parte degli Interessati

Gli allegati sono parte integrante della presente Policy ma potranno essere aggiornati autonomamente senza dover avviare iter di aggiornamento e approvazione della presente Policy.

I seguenti documenti costituiscono parte integrante della presente Policy:

- Politica sulla protezione dei dati di ABF (Europa)
- Politica sulla sicurezza delle informazioni di ABF
- Politica di gestione delle violazioni della protezione dei dati ABF
- Quadro di risposta agli incidenti sulla sicurezza delle informazioni di ABF
- Politica di outsourcing a terze parti della sicurezza delle informazioni del Gruppo
- Valutazione del trattamento di terze parti
- Brief Guidance Note on Use of Legittimate Interests Assessments
- Guidance on the use of Transfer Impact Assessments
- Data Protection Impact Assessment Guidance Notes
- Valutazione d'impatto sulla protezione dei dati
- Retention Guidelines for Personal Data- Italy
- ITALY Functional Guide Payroll (It) v. June 2019
- ITALY Functional Guide HR (It) v. June 2019
- Italy – Functional Guide IS-IT (It) v. June 2019
- 8a_Italy Functional Guide CCTV (It) v. June 2019
- 8b_ Italy FG Annex CCTV (It) v. June 2019
- 9a_Italy Functional Guide Sales & Marketing (It) v.June 2019
- 9b_Italy- FG Annex – Sales&Marketing (It) v. June 2019

20 SANZIONI

In caso di violazione da parte delle disposizioni della presente Policy, potranno essere applicate le sanzioni previste dal contratto collettivo nazionale di lavoro applicabile nonché dal sistema disciplinare aziendale.

Le violazioni da parte di soggetti terzi saranno sanzionate sulla base di specifiche clausole contrattuali che prevedono, nei casi più gravi, la risoluzione di diritto del contratto ai sensi di quanto disposto all'art. 1456 del codice civile.