CFN GENERALE FIDUCIARIA S.P.A.

POLICY PRIVACY

Approvato dal Consiglio di Amministrazione
in data 29 aprile 2024
Versione 1.0

AGGIORNAMENTI

Responsabile	Data	Versione	Oggetto Modifica
Consiglio di Amministrazione	29/04/2024	1.0	Approvazione e primo rilascio

INDICE

1. Premessa

La presente policy (la "Policy") è adottata da CFN Generale Fiduciaria S.p.A.al fine di garantire che:

- il trattamento dei dati personali da parte della Fiduciaria 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. 196/03, cosiddetto "Codice in materia di protezione dei dati personali" come modificato dal D. Lgs. 101/2018 ("Codice Privacy").

Normativa aziendale:

- Policy di Business Continuity Plan
- Procedura per la gestione del sistema informativo
- Codice etico e comportamentale

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;
- **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 **CFN GENERALE Fiduciaria S.p.A..**, con sede legale in Galleria de Cristoforis 3, 20122 Milano, (di seguito, il "**Titolare**").

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 non ha ritenuto di dover designare alcun Data Protection Officer, non rientrando nel novero dei soggetti indicati dall'art. 37 del GDPR. Tale valutazione ha trovato, altresì, conforto nelle indicazioni fornite dall'associazione di categoria, Assofiduciaria, con la comunicazione PRIVACY_COM_2018_102 (a cui è allegato apposito parere legale).

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 previsti 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 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 Policy di Business Continuity Plan e alla Procedura per la gestione del sistema informativo.

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

L'articolo 30 del GDPR prevede che ogni titolare e ogni responsabile del trattamento debbano tenere un registro delle attività di trattamento svolte sotto la propria responsabilità. Il comma 5 del predetto articolo dispone in particolare che l'obbligo di tenuta del registro non si applica alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato e il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10. È altrettanto vero che, anche alla luce del considerando 82 del RGPD, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, il principio di "accountability" e, al contempo, ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso. Pertanto, dall'analisi degli articoli sopracitati ed in considerazione dei documenti richiesti in fase di valutazione di accettazione di mandato fiduciario, la Società ha deciso di redigere, in via del tutto volontaria, un registro dei trattamenti.

In merito, le strutture operative della Fiduciaria si impegnano a segnalare tempestivamente 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.

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.

Allo stato attuale non sussistono le condizioni per la obbligatorietà di tale adempimento. Tale valutazione ha trovato, altresì, conforto nelle indicazioni fornite dall'associazione di categoria, Assofiduciaria, con la comunicazione PRIVACY_COM_2018_102 (a cui è allegato apposito parere legale).

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 e prima di darvi inizio consulterà l'autorità di controllo adottando specifiche misure tecniche e organizzative per mitigare l'impatto del trattamento.

11. Modalità di Trattamento – Informativa e consenso

11.1 Corretto Trattamento dei dati

La Fiduciaria 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 posso 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.

10.3 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.

11.3 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 e-mail 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.

Per far fronte ad eventuali richieste da parte delle Autorità Giudiziarie e/o di P.S. e sulla base delle rigorose disposizioni di legge cui la Società soggiace, è stato ritenuto opportuno fissare il termine di conservazione dei dati personali in 20 anni a decorrere dalla cessazione del mandato.

13. Esercizi dei diritti dell'interessato

Il Regolamento (UE) 2016/679 (GDPR) contempla la possibilità per l'interessato, di esercitare i propri diritti sul dato personale che si sostanziano in:

> Diritto di Accesso:

L'interessato ha il diritto di richiedere al titolare del trattamento, la conferma sull'effettivo trattamento dei propri dati personali e, in caso affermativo, di ottenere l'accesso agli stessi. In tal caso, il titolare deve fornire una copia dei dati personali oggetto di trattamento.

> Diritto di cancellazione / diritto all'oblio

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano nei seguenti casi:

- se l'interessato revoca il consenso che abbia costituito e costituisca l'unico fondamento giuridico per il trattamento;
- se l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente o per finalità di marketing diretto;
- se i dati siano stati trattati in maniera illecita;
- se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati;
- se i dati devono essere cancellati perché richiesto da un obbligo legale incombente sul titolare del trattamento;

> Diritto alla portabilità dei dati:

L'interessato ha diritto di ricevere i propri dati personali in un formato strutturato, comunemente utilizzato e leggibile, e di trasmettere i predetti dati ad un altro titolare, senza alcun ostacolo. Tale diritto si applica ai trattamenti basati sul consenso o su un contratto quale base giuridica ed effettuati con mezzi automatizzati. La portabilità può riguardare dati forniti consapevolmente ed attivamente dall'interessato nonchè dati generati dalla sua attività. La trasmissione di dati personali oggetto di portabilità all'interessato deve essere adeguatamente protetta tramite l'implementazione di misure tecniche per assicurare il trasferimento sicuro dei dati dell'interessato, nonché l'integrità degli stessi.

> Diritto di rettifica:

L'interessato ha il diritto di ottenere dal titolare del trattamento conferma sull'avvenuta rettifica di dati personali inesatti. L'interessato ha altresì il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione supplementare.

> Diritto di limitazione al trattamento:

L'interessato può richiedere di limitare il trattamento dei propri dati personali e di non eseguire alcuna ulteriore modifica degli stessi.

> Diritto di opposizione:

L'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano solamente per motivi connessi alla sua situazione particolare connessi a ragioni di interesse pubblico o all'esercizio di pubblici poteri.

Si tratta di un diritto che trova la sua ragione di essere nella tutela dell'individuo dal controllo eccessivo dello Stato.

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.

> Processo decisionale automatizzato di trattamento dei dati:

L'interessato può opporre rifiuto ad un processo decisionale automatizzato di trattamento dei propri dati.

La Società ha predisposto un sistema di gestione per l'esercizio dei diritti dell'interessato che è in grado di dare riscontro in modo tempestivo, corretto e trasparente, senza ingiustificato ritardo e al più tardi entro un mese, motivando la sua eventuale intenzione di non accogliere tali richieste.

Si rammenta che la facoltà di esercitare i propri diritti è contemplata nell'informativa fornita all'interessato al momento di raccolta del dato o comunque al primo contatto utile avuto con lo stesso.

I dati acquisiti e archiviati dai soggetti tenuti all'adeguata verifica ai fini antiriciclaggio prevalgono sul diritto alla Privacy e all'oblio.

L'articolo 17, paragrafo 3, lettera b) del Regolamento GDPR dispone che il diritto alla cancellazione, anche nella forma rafforzata del diritto all'oblio, 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 (UE o Stato) o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Pertanto, le istanze di tutela della privacy non possano intralciare l'interesse pubblico alla lotta contro il riciclaggio e il finanziamento del terrorismo.

Con riferimento alle modalità operative di gestione dell'esercizio dei diritti dell'interessato si rinvia alle istruzioni operative declinate nella Procedura operativa per l'esercizio dei diritti dell'interessato.

14. Data Breach

Il GDPR prevede, in ipotesi di violazione dei dati personali, a determinate condizioni e, in particolare, ove tale violazione determini un probabile rischio per i diritti degli interessati, l'obbligo per il Titolare del trattamento di notificare la violazione al Garante per la protezione dei dati personali entro 72 ore dal momento in cui ne è venuto a conoscenza.

Secondo le definizioni contenute nel GDPR (cfr. art. 4, comma 1, n. 12) per "violazione dei dati personali" si intende "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".

Tale violazione incide sulla perdita di riservatezza, sul danneggiamento e sulla indisponibilità dei dati.

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

La violazione può essere rilevata da ogni dipendente della CFN Generale Fiduciaria SpA che individui o sospetti un'anomalia che possa determinare un impatto di sicurezza sui dati personali.

La notifica dovrà avvenire tramite comunicazione mail da inviare all'Amministratore di Sistema che dalla data del CdA del 29/04/2024 è il Responsabile dell'Area Organizzazione, IT e HR.

Con riferimento alle modalità operative di gestione del Data Breach si rinvia alle istruzioni operative declinate nella Procedura per la Segnalazione delle violazioni dei dati personali.

15. Sanzioni

La violazione delle disposizioni del GDPR rilevanti per la Fiduciaria (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 in relazione all'inosservanza di adempimenti organizzativi e tecnici;
- fino a 20.000.000 di euro o fino al 4% del fatturato totale annuo dell'esercizio precedente, se superiore per il mancato rispetto dei principi ed obblighi generali, dell'adempimento dell'informativa e del riscontro ai diritti degli interessati.