POLICY PER IL TRATTAMENTO DEI DATI PERSONALI

Referente del processo	Presidente
Approvata da	Consiglio di Amministrazione
Data	5 luglio 2019
Versione	02/2019

SOMMARIO

1 PREMESSA

La presente policy ha la finalità di chiarire agli, amministratori, sindaci collaboratori e consulenti esterni di 4AIM SICAF (di seguito, anche la "Società o "Titolare del Trattamento") le regole da osservare nell'ambito del trattamento dei dati personali.

All'atto di assunzione viene consegnata una copia della presente Policy, disponibile anche all'interno dell'archivio informatico della Società. La policy è tempestivamente aggiornata e diffusa tra tutti i destinatari in occasione dell'emanazione di nuove disposizioni di legge o provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali (il "Garante") che incidano sulle condotte da osservare ai fini della tutela dei dati personali trattati.

2 RIFERIMENTI

La presente policy viene redatta sulla base delle disposizioni del Regolamento Europeo Privacy UE 2016/679 (G.D.P.R.) 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 la restante normativa vigente italiana in tema privacy, tenendo conto anche delle indicazioni contenute nei provvedimenti emessi dal Garante della Privacy, quali ad esempio le linee guida n. 53 del 23 Novembre 2006 ("Linee Guida per il trattamento dei dati personali dei lavoratori da parte di datori di lavoro privati") e n. 13 del 1 Marzo 2007 ("Linee Guida del Garante per posta elettronica e internet").

3 STRUTTURA PRIVACY ADOTTATA

3.1 Titolare del trattamento

Titolare del trattamento è 4AIM SICAF S.p.A. con sede in Corso Venezia, 16 - 20121 Milano nella persona del legale rappresentante della Società.

Il Titolare, come sopra individuato, ha il compito di mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa comunitaria ed italiana vigente, provvedendo al loro riesame e relativo aggiornamento qualora necessario.

Provvede, qualora necessario per l'operatività della società, alla nomina di responsabili esterni del trattamento cosi come previsto dall'articolo 28 del G.D.P.R., i quali devono presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che lo stesso trattamento soddisfi i requisiti previsti dalla normativa e garantisca la tutela dei diritti dell'interessato.

3.2 Responsabile esterno del trattamento

La Società può dover ricorre al supporto di responsabili esterni per il presidio dei trattamenti di dati in virtù di contratto o da altro atto giuridico stipulato a norma del diritto dell'Unione o degli Stati membri.

Il responsabile esterno del trattamento, in virtù di tali accordi, sarà tenuto a:

- trattare i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di eventuale trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le misure tecniche ed organizzative richieste dalla normativa comunitaria ed italiana;
- informare la Società e richiederne l'autorizzazione nel caso intenda procedere alla nomina di un sub responsabile;
- tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile esterno del trattamento, assistere la Società con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste degli interessati per l'esercizio dei propri diritti di cui agli artt. 15 -22 del GDPR (accesso, revoca, rettifica, cancellazione, limitazione, portabilità, opposizione);
- assistere il Titolare del trattamento nel garantire il rispetto degli obblighi inerenti l'applicazione di misure di sicurezza in tema di data breach, valutazione di impatto sulla protezione dei dati e consultazione preventiva con il Garante prima di procedere con il trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Il Titolare del trattamento riporta in un documento interno (allegato al Registro dei Trattamenti) gli estremi identificativi delle persone fisiche o società nominate responsabili del trattamento per la Società.

3.3 Il Data Protection Officer

E' nominato dal Titolare del Trattamento un Data Protection Officer (D.P.O.) con l'obiettivo di assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento e agli altri obblighi di legge vigenti.

Il D.P.O. fornisce la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il Titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare.

Al D.P.O., in particolare, sono assegnati i seguenti compiti:

- informare e fornire consulenza al Titolare nonché ai collaboratori che eseguono il trattamento in merito agli obblighi previsti dal Regolamento, nonché da altre disposizioni nazionali relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, di altre disposizioni nazionali relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento.

Inoltre, il D.P.O rappresenta per la Società il punto di contatto, non solo per il Garante ma anche per gli interessati al trattamento, in merito a qualunque problematica connessa ai loro dati o all'esercizio dei loro

diritti, con la facoltà di consultare il Garante anche di propria iniziativa relativamente a qualunque questione.

La Società supporta il DPO per l'ottimale svolgimento dei compiti e delle funzioni che gli sono assegnate attraverso la messa a disposizione di risorse adeguate al fine di consentire al DPO di esercitare le proprie funzioni in autonomia e indipendenza.

Per la Società è designato quale D.P.O NEXEN S.p.A. nella persona della dott.ssa Rossana Salvatrice Corso.

I dati di contatto del DPO sono pubblicati nell'Archivio informatico privacy della Società e sul Registro dei Trattamenti.

3.4 Persone autorizzate al trattamento

Le persone autorizzate al trattamento dei dati sono le persone fisiche che effettuano per conto del Titolare le operazioni di trattamento dei dati personali contenuti nelle banche dati informatiche del Titolare e negli archivi cartacei sotto l'autorità diretta del Titolare.

Il Titolare può designare individualmente i singoli autorizzati , a mezzo di un atto che deve elencare analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato (tale atto è consegnato al momento dell'assunzione del dipendente o collaboratore della Società).

4 INFORMATIVA AL TRATTAMENTO DEI DATI

La Società fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- l'identità e i dati di contatto del Titolare del trattamento;
- i dati di contatto del Responsabile della protezione dei dati (DPO);
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- i legittimi interessi perseguiti dal Titolare del trattamento o da terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione della Società di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione.

Qualora la Società intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Qualora i dati non siano stati ottenuti presso l'interessato, il Titolare del trattamento fornisce all'interessato le seguenti informazioni:

- l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati (DPO),;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

- le categorie di dati personali in questione;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- ove applicabile, l'intenzione della Società di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione.

In aggiunta, nel momento in cui i dati personali sono ottenuti direttamente o meno presso l'interessato, la Società fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i legittimi interessi perseguiti dal Titolare del trattamento o da terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (in caso di dati non raccolti presso l'interessato);
- la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (in caso di dati non raccolti presso l'interessato);
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).Il trattamento dei dati personali è necessario per l'adempimento degli obblighi derivanti dalla normativa vigente e funzionale allo svolgimento del rapporto con il Titolare del trattamento; l'eventuale rifiuto comporterebbe l'impossibilità di assolvere detti obblighi e di determinare le competenze di Sua spettanza.

5 MODALITA' DI TRATTAMENTO

Il trattamento deve essere effettuato nel rispetto delle norme di legge, delle disposizioni di cui alla presente policy ed, inoltre, secondo le direttive o istruzioni impartite dal Titolare o dal D.P.O.

I Dati personali oggetto dei trattamenti devono essere:

- trattati in modo lecito e secondo correttezza; ciò significa che il trattamento deve avvenire in conformità alle norme sulla privacy e, più in generale, in conformità alle norme imperative, all'ordine pubblico e al buon costume;
- trattati nel rispetto del principio di privacy by design, ossia i dati devono essere oggetto di protezione sin dalla progettazione, in fase di sviluppo, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento dei dati personali;
- trattati nel rispetto del principio della privacy by default, ossia di progettare misure e sistemi che abbiano come impostazione predefinita esclusivamente l'uso dei soli dati necessari per il perseguimento di una determinata finalità;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi. Si precisa che:

    - per scopi “determinati” si intende che la raccolta e la registrazione non sono consentite se non hanno uno scopo concreto;
    - per “espliciti” si intende che chi procede alla raccolta deve informare il soggetto interessato che sta effettuando tale attività e lo scopo per cui lo sta facendo;
    - per “legittimi” si intende quanto già espresso al punto precedente. Le altre operazioni di trattamento dovranno avvenire in termini compatibili con gli scopi per cui la raccolta e la registrazione sono avvenute.
- esatti e se necessario aggiornati; a questo proposito dovranno essere adottate tutte le misure tecniche ed organizzative adeguate per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per cui sono stati rilevati o successivamente trattati, cancellati o rettificati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati. A tale proposito:
- il concetto di pertinenza attiene all’attività che svolge il soggetto che procede alla raccolta;
- il concetto di completezza implica che non è consentito trattare solo alcuni dati ignorandone altri, pure rilevanti rispetto alle finalità del trattamento, limitandosi a considerare solo un lato della medaglia e non anche il suo rovescio;
- il concetto di non eccedenza riguarda sia l’aspetto quantitativo (non deve essere raccolta una quantità di dati eccessiva rispetto alle finalità del trattamento) sia l’aspetto temporale (i dati non devono essere conservati per un periodo di tempo superiore a quello necessario agli scopi per cui sono stati raccolti o trattati);
- conservati in una forma che consenta l’identificazione dell’interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Ciò detto occorre ricordare, inoltre, che:

- il trattamento deve essere effettuato per gli scopi determinati nelle lettere di incarico (ovvero in relazione alle rispettive mansioni di lavoro);
- il Titolare, DPO e gli autorizzati (nonché i Responsabili esterni, per i trattamenti di loro competenza) devono fare quanto ragionevolmente necessario per assicurare che i dati personali oggetto dei trattamenti siano esatti e, se necessario, aggiornati;
- al Titolare è rimesso il compito di vigilare sul puntuale rispetto della normativa da parte degli Autorizzati del trattamento;
- i dati personali oggetto del trattamento devono essere conservati per un periodo non eccedente a quello necessario per le finalità per cui gli stessi dati sono stati raccolti e trattati, salvo il rispetto di obblighi di legge che determinino termini più lunghi (es: obbligo civilistico di mantenere per dieci anni la documentazione della corrispondenza, obblighi fiscali e contabili, obblighi imposti da normative fiscali, necessità probatorie in relazione alla prescrizione e decadenza dei diritti di cui al Titolo V, Libro VI, del codice civile);
- in nessun caso i dati personali possono essere utilizzati per scopi illeciti o incompatibili con i fini per i quali sono stati raccolti e registrati.

6 DIRITTI DELL’INTERESSATO

La Società agevola l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica ed organizzativa) a ciò idonea.

L'interessato ha la facoltà di esercitare i diritti di cui agli artt. 15-22 del Regolamento UE di seguito riportati:

- esercitare l'opposizione al trattamento in tutto o in parte;

- ottenere la cancellazione dei dati in possesso del Titolare;
- ottenere l'aggiornamento o la rettifica dei dati conferiti;
- chiedere ed ottenere in forma intellegibile i dati in possesso del Titolare (diritto di accesso);
- chiedere ed ottenere trasformazione in forma anonima dei dati;
- chiedere ed ottenere la trasmissione diretta dei dati dal Titolare ad un altro (diritto di portabilità);
- chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento.

L'interessato può rivolgersi direttamente alla Società per l'esercizio dei suoi diritti, scrivendo all'apposito indirizzo dpo@4aim.it; la richiesta verrà presa in carico e gestita tempestivamente dal D.P.O.

Il D.P.O. valuterà la legittimità (dopo aver identificato l'interessato) della richiesta prima di procedere al suo accoglimento. Qualora la risposta fosse complessa, manifestamente infondata o eccessiva o ripetitiva, può chiedere all'interessato di pagare un contributo stabilendone l'ammontare.

Il Titolare del Trattamento, con il supporto del D.P.O., fornisce un riscontro all'interessato entro un mese dalla data di ricezione della richiesta. Tale termine può essere esteso a tre mesi in casi di particolare complessità. In questo caso il Titolare avvertirà l'interessato entro un mese tramite comunicazione (ad esempio, tramite mail).

Il D.P.O. provvederà a comunicare agli uffici/servizi l'esito della valutazione e le conseguenti modalità e tipologia di intervento (ad esempio, cancellazione).

La risposta, chiara, coincisa e facilmente accessibile e comprensibile, è fornita in forma scritta, anche attraverso strumenti elettronici (ad esempio, tramite mail). Può essere orale solo se espressamente richiesta in tal senso dall'interessato.

Le attività su elencate (quali, ad esempio, data ricezione richiesta, sua valutazione, data riscontro e sua modalità) devono essere tracciate e archiviate a cura del D.P.O.

7 MISURE DI SICUREZZA

La Società adotta misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente alla normativa GDPR ed italiana vigente (principio di accountability).

Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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, le misure tecniche e organizzative possono comprendere, ad esempio, una procedura per provare, verificare e valutare regolarmente l'efficacia di tali misure.

8 VALUTAZIONE DELL'IMPATTO

La Società effettua – quando un tipo di trattamento di dati prevede l'uso di nuove tecnologie e considerati, inoltre, la natura, l'oggetto, il contesto e le finalità del trattamento, presentando, pertanto, un rischio elevato per i diritti e le libertà delle persone fisiche – una valutazione dell'impatto dei trattamenti, con il supporto del D.P.O.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. Tale valutazione deve essere effettuata prima di procedere con il trattamento.

In particolare, la valutazione d'impatto sulla protezione dei dati è effettuata in ogni caso dalla Società nei seguenti casi:

- 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;
- il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dalla Società;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Qualora la valutazione di impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio, il Titolare è tenuto a consultare preventivamente in merito il Garante prima di procedere con il trattamento.

9 DATA BREACH

Il Titolare del trattamento è tenuto alla notifica al Garante per la protezione dei dati personali della violazione di dati personali o *data breach.*

A tal proposito la Società 4AIM ha formalizzato una procedura di *Data breach.*

Per “Violazione di dati” 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.

Si possono distinguere tre tipi di violazioni:

- violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- violazione di integrità, ovvero quando si verifica un’alterazione di dati personali non autorizzata o accidentale;
- violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Il collaboratore che per primo riscontrala violazione comunica il *data breach* al D.P.O., che provvederà a coinvolgere per supporto gli uffici necessari.

Sono, quindi, individuati e qualificati i rischi connessi a violazioni di dati personali; qualora tali rischi riguardino i diritti e le libertà delle persone fisiche, la Società procede ad una valutazione del livello di rischio, per poi procedere entro settantadue ore dal momento in cui ne viene a conoscenza alla notificazione della violazione al Garante per la privacy. Se il rischio valutato risulti essere elevato così come previsto dalla normativa, si procede alla comunicazione della violazione agli interessati coinvolti nelle forme di volta in volta concordate.

Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza qualora richiesto.