Policy generale sulla protezione dei Dati personali

Autore	Associazione Banco Alimentare della Lombardia “Danilo Fossati” ODV
Sintesi	La presente Policy stabilisce le regole generali che disciplinano il Trattamento dei Dati personali da parte dell’Associazione o di terzi per suo conto
Versione	1.0
Stato	Definitivo
Data di pubblicazione	08.10.2019

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.
- «**GDPR**»: Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).
- «**Interessato**»: persona fisica cui si riferiscono i Dati personali.
- «**Responsabile del Trattamento**» o «**Responsabile**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati personali per conto del Titolare del trattamento.
- «**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 responsabile del Trattamento e le persone autorizzate al Trattamento dei Dati personali sotto l'autorità diretta del titolare o del responsabile.
- «**Titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
- «**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.
- «**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

L'Associazione Banco Alimentare della Lombardia Danilo Fossati ODVn sede legale in Muggiò (MB), via Papa Giovanni XXIII n. 17/19 (in seguito l'«**Associazione** »), 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.
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, e attui misure 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*** la quale richiede che il Titolare, sia al momento di determinare i mezzi del Trattamento sia all'atto 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 necessari per ogni specifica finalità di Trattamento.

L'Associazione presta la massima cura e attenzione al tema della protezione dei Dati personali e della tutela dei diritti e delle libertà delle persone fisiche, e a tal fine attua le misure tecniche e organizzative necessarie al fine di evitare trattamenti in violazione del GDPR.

3 SCOPO

Lo scopo della presente Policy è di assicurare che il Trattamento dei Dati personali all'interno dell'Associazione 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.

4 AMBITO DI APPLICAZIONE E DESTINATARI

La presente Policy si applica ai membri dell'Assemblea degli Associati, al Consiglio Direttivo, ai soggetti facenti parte del vertice aziendale dell'Associazione, ai dipendenti, ai collaboratori e ai volontari («Destinatari»).

Nel caso in cui uno dei Destinatari ponga in essere azioni in violazione del GDPR o di altra normativa privacy applicabile, l'Associazione potrebbe essere soggetta a significative sanzioni, penali o amministrative, anche pecuniarie, nonché potrebbe 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 Responsabile Interno del Trattamento

5 ATTUAZIONE E PIANO DI REVISIONE

La presente Policy è immediatamente efficace e in vigore alla data della sua approvazione e tutti i responsabili aziendali dovranno assicurare che i dipendenti e collaboratori sottoposti alla loro supervisione e controllo siano a conoscenza dei contenuti previsti dalla stessa.

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

(i) eventi di violazione di dati personali;

(ii) modifiche organizzative interne all'Associazione;

(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.

6 NORMATIVA DI RIFERIMENTO

L'Associazione 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 l'Associazione compia operazioni di Trattamento, tra cui:

- Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Decreto legislativo 2003/196 (Codice in materia di protezione dei dati personali), così come modificato ed integrato, da ultimo dal Decreto Legislativo 2018/101;
- Linee guida e provvedimenti del Garante per la Protezione dei Dati personali;
- Pareri del Working Party Article 29.

7 ORGANIZZAZIONE E RESPONSABILITÀ

L'Associazione può essere Titolare, Contitolare o Responsabile del trattamento.

Il Titolare è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento, 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.

Il Titolare del trattamento dei dati personali effettuato nell'ambito della gestione delle attività connesse alla realizzazione della Giornata Nazionale della Colletta Alimentare è la Fondazione Banco Alimentare, che svolge l'attività suddetta secondo le finalità e le modalità decise dalla stessa.

8 PRINCIPI APPLICABILI AL TRATTAMENTO DI DATI PERSONALI

Le operazioni di Trattamento effettuate nell'ambito delle attività aziendali dai Destinatari devono garantire che i Dati personali siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»);

d) 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 («**esattezza**»);

e) 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; («**limitazione della conservazione**»);

f) 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 («**integrità e riservatezza**»).

9 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, 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 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) dell'Associazione può essere reperita contattando il Responsabile Interno del Trattamento.

10 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 sono previste dalla normativa vigente.

Al fine di ricevere il necessario supporto, i Destinatari sono pregati di rivolgersi sempre al Responsabile Interno del Trattamento dell'Associazione qualora debbano effettuare per la prima volta il Trattamento di categorie particolari di Dati personali.

11 TRATTAMENTO DEI DATI DELL'ASSOCIAZIONE TRAMITE TERZE PARTI

Qualora sia necessario avvalersi di un fornitore di servizi per l'esecuzione di attività che richiedano anche 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.

La documentazione privacy aggiornata relativa ai rapporti con i fornitori (contratti, clausole privacy, contratto tra titolare responsabile) dell'Associazione può essere reperita contattando il Responsabile Interno del Trattamento.

12 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. L'Associazione 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 della documentazione aziendale previste nell'Allegato alla presente policy a cui si rimanda 📎**All. 1 – Matrice periodo di conservazione**.

13 MISURE DI SICUREZZA

Le misure di sicurezza adottate dall'Associazione sono riportate nell'Allegato alla presente Policy a cui si rimanda 📎**All. 2 – Sintesi Misure di Sicurezza**.

14 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 dall'Associazione nell'ambito delle sue attività o da terzi per conto dell'Associazione.

A titolo esemplificativo, interessati possono essere i clienti, i fornitori, i consulenti e i dipendenti dell'Associazione.

Ai sensi degli articoli 15-22 del Regolamento (Ue) 2016/679, gli interessati possono esercitare, con richiesta rivolta senza formalità nei confronti dell'Associazione, anche per il tramite di un delegato, i seguenti diritti:

14.1 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 tale l'esercizio di tale diritto non leda ai diritti e le libertà altrui.

14.2 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.

14.3 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 dell'Associazione dell'informazione.

Tale diritto è escluso nei limitati casi elencati nell'art. 17, comma 3 del Regolamento.

14.4 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 Regolamento. L'interessato deve essere informato se la limitazione è revocata.

14.5 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); e

b. il trattamento sia effettuato con mezzi automatizzati; e

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.

14.6 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.

14.7 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 proprio Referente in materia di privacy (di seguito anche solo «***Referente***»).

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 dell'Associazione (autorizzato al trattamento).

2) Ricerca dei dati

Salva diversa disposizione, il Referente al quale è stata riferita la richiesta, come al par. 1) che precede, verifica la completezza e la correttezza della documentazione a supporto della richiesta, nonché l'ammissibilità della stessa.

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 (compresi i dati "sensibili") 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.

3) Verifica dell'identità dell'interessato

Il Referente verifica l'identità dell'interessato sulla base di idonei elementi di valutazione. Qualora il Referente 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 richiede copia della procura o della delega sottoscritta e presentata unitamente a copia di un documento di riconoscimento dell'interessato.

4) Piano di gestione della richiesta

Una volta verificata l'identità dell'interessato, il Referente prende in carico la richiesta avanzata dall'interessato, valutandone l'ammissibilità e la fattibilità in conformità alle disposizioni del Regolamento e individuando le competenze necessarie per darvi riscontro secondo le tempistiche previste al successivo punto 5 "*Riscontro alla richiesta dell'interessato*" del presente §14.7.

A tal fine coinvolge nella gestione della richiesta i Responsabili del trattamento eventualmente coinvolti nel trattamento e le persone autorizzate al trattamento di tali dati personali, nonché le ulteriori funzioni competenti rispetto alle richieste contenute nell'istanza.

Responsabile della Funzione IT 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, …).

I soggetti coinvolti sono chiamati a effettuare le azioni necessarie al fine di dare riscontro alle richieste dell'interessato secondo le indicazioni impartite dal Referente.

Il Referente, con il supporto della Funzione IT, provvede a raccogliere i dati da fornire al richiedente.

In caso di richiesta di **portabilità**, il Referente 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 "i dati forniti" dall'interessato sono quelli consapevolmente e attivamente forniti dall'interessato (ad esempio, indirizzo postale, nome utente, età, …) e i dati "osservati", indirettamente forniti dall'interessato attraverso la fruizione di un servizio (ad esempio, la cronologia delle ricerche effettuate, dati relativi all'ubicazione), ma non 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 al Referente le misure tecniche adottate.

Il Referente redige un report sintetico contenente **All. 3 – Riscontro richiesta dell'Interessato di esercizio dei diritti di cui al Regolamento (UE) 2016/679**:

- la richiesta dell'interessato;
- le eventuali verifiche sull'identità dell'interessato;
- il piano di gestione della richiesta formulato unitamente al Responsabile della Funzione IT;
- i compiti specifici impartiti, le persone coinvolte, i risultati ottenuti.

Il report viene condiviso con il soggetto responsabile di aggiornare il Registro dei Trattamenti adottato dall'Associazione.

5) Riscontro alla richiesta dell'interessato

La risposta, che deve essere intelligibile, concisa, trasparente e facilmente accessibile, espressa in linguaggio semplice e chiaro, va inoltrata direttamente al richiedente tramite:

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

L'Associazione deve necessariamente conservare traccia della risposta. 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, il Referente 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.

In caso di particolare complessità della richiesta, il Referente comunica all'interessato la necessità di prorogare (al più tardi, di un mese) il riscontro all'istanza inviata unitamente ai motivi della proroga.

6) 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, il Referente deve provvedere a darne comunicare a tutti i destinatari a cui, in qualsiasi modo, sono stati trasmessi i dati personali oggetto di rettifica, cancellazione o modifica, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Di tali comunicazioni viene conservata copia.

7) Richieste di accesso ai dati di videosorveglianza

In relazione alle videoregistrazioni deve essere assicurato agli interessati l'effettivo esercizio dei propri diritti in conformità al Regolamento, in particolare quello di accedere ai dati che li riguardano e di verificare le finalità e le modalità del trattamento. Tali richieste devono essere riferite seguendo le procedure qui contenute al Responsabile Interno del Trattamento che, una volta identificato l'interessato chiede al medesimo di descrivere con la maggiore precisione possibile il momento o i momenti della registrazione cui intende accedere (domandando, ad esempio, la data e la fascia oraria

della registrazione, l'eventuale abbigliamento o la presenza di oggetti particolari o di altre persone, ecc.).

Il Responsabile Interno del Trattamento, una volta espletata la verifica della documentazione inviata dal richiedente, mette in atto un piano di gestione della richiesta come dal punto 4) *Piano di gestione della richiesta*, accertando le motivazioni della richiesta, il periodo temporale di riferimento (ad esempio, la data e la fascia oraria della registrazione), unitamente ad altri particolari utili per la verifica della pertinenza della richiesta stessa (ad esempio l'eventuale abbigliamento o la presenza di oggetti particolari o di altre persone, …).

Il Responsabile Interno del Trattamento, ricevute tali informazioni, comunica la richiesta e i dettagli ricevuti al Responsabile del trattamento dei dati delle videoregistrazioni che provvederà a relazionare per iscritto il Responsabile Interno del Trattamento sulla fattibilità di quanto richiesto dall'interessato, anche alla luce sia dei brevissimi tempi di conservazione delle videoregistrazioni sia del principio che l'esercizio del diritto dell'interessato non deve ledere i diritti e le libertà altrui.

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di rettifica o di integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Il diritto di opposizione è controbilanciato dal fatto che il trattamento viene effettuato per motivi legittimi cogenti (tutela della sicurezza e del patrimonio aziendale), che possono prevalere sugli interessi, sui diritti e sulle libertà dell'interessato. Viceversa, l'interessato ha diritto di ottenere la cancellazione dei dati alle condizioni di cui all'art. 17 del Regolamento.

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.

15 VALUTAZIONE DEL RISCHIO SULLA PROTEZIONE DEI DATI PERSONALI NEI NUOVI PROGETTI

Alcuni tipi di Trattamento potrebbero presentare particolari rischi per i diritti e le libertà degli Interessati.

In particolare, potrebbero sorgere rischi specifici nei casi in cui i Dati personali siano trattati tramite l'utilizzo di un particolare tipo di nuova tecnologia, tenendo in considerazione la natura, il contesto e le finalità del Trattamento. Sono comunque da considerarsi situazioni che comportano un rischio:

- la 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;
- il Trattamento, su larga scala, di categorie particolari di Dati personali;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In questi casi, il Titolare o il Responsabile, ove preposto, esegue e mantiene una valutazione degli impatti che il Trattamento in oggetto potrà avere sul Trattamento dei Dati personali delle categorie di soggetti coinvolti.

16 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

L'Associazione mantiene un registro delle attività di trattamento dei dati personali, 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 e del responsabile della protezione dei dati;
- 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 Regolamento.

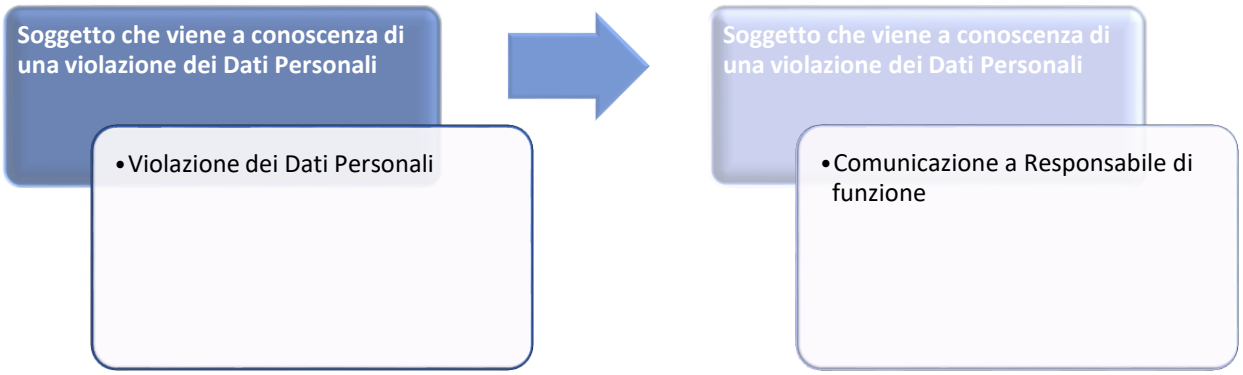
L'Associazione deputa il Responsabile Interno del Trattamento all'aggiornamento regolare del registro delle attività del trattamento, informandone tutti i Responsabili.

17 VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Quanto di seguito riportato disciplina la gestione e la notifica/comunicazione di incidenti relativi alla sicurezza dei dati che possono causare la violazione di dati personali; tra i possibili incidenti si ricordano a titolo esemplificativo:

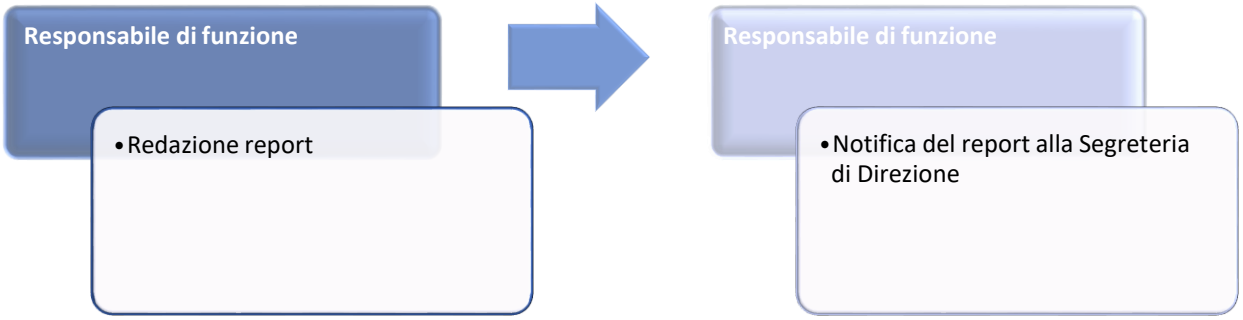
- ⇨ *perdita o furto di strumenti IT (pc, smartphone, chiavette USB, hardware);*
- ⇨ *rivelazione di informazioni a soggetti non autorizzati;*
- ⇨ *accesso non autorizzato ai dati personali;*
- ⇨ *violazione delle misure di sicurezza fisiche dei locali dove i dati personali sono archiviati;*
- ⇨ *caricamento/divulgazione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

1) <u>Scoperta o sospetta violazione dei dati</u>



Il soggetto che viene a conoscenza di una violazione dei Dati Personali, anche solo sospetta e non ancora accertata, deve informare **immediatamente** il soggetto Responsabile della funzione nel cui ambito si è verificato l'incidente relativo alla sicurezza che ha causato la violazione dei dati.

2) **<u>Report interno della violazione</u>**



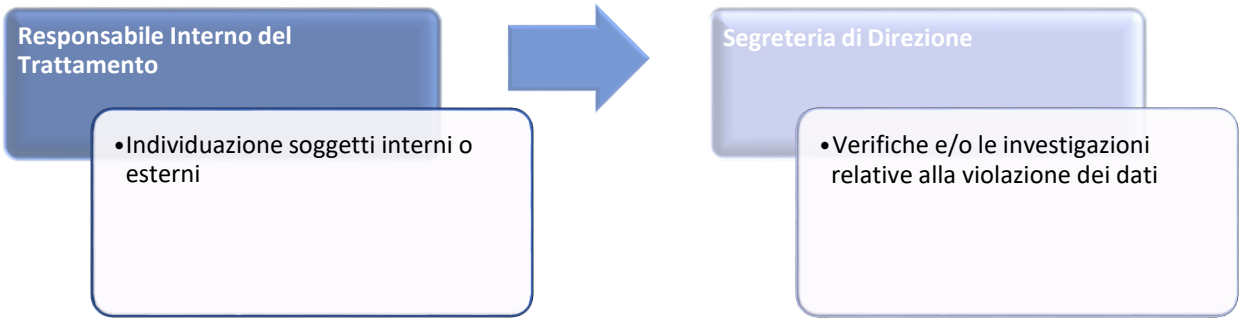
Il Responsabile di funzione, informato dell'evento di violazione dei dati deve, se possibile **entro 24 ore** dalla notifica ricevuta:

a) redigere un report interno relativo all'evento accaduto, eventualmente supportato dal Responsabile IT se la violazione coinvolge sistemi IT. Il report interno deve contenere i dettagli noti della violazione:

- data e ora;
- soggetti aziendali coinvolti;
- descrizione dell'incidente;
- dati personali apparentemente violati;
- sistemi IT/archivi/database coinvolti;
- azione eventualmente intraprese per mitigare gli effetti della violazione.

b) notificare quanto accaduto e il relativo report interno al Responsabile Interno del Trattamento.

3) Valutazione del rischio per i diritti e le libertà delle persone



Il Responsabile Interno del Trattamento, per conto del Titolare, sulla base delle circostanze concrete della violazione verificatasi o sospettata e del potenziale rischio per i diritti e le libertà degli interessati, se necessario individuerà tempestivamente i soggetti, interni o esterni all'Associazione, dotati delle necessarie competenze al fine di eseguire le verifiche e/o le investigazioni relative alla violazione dei dati e valutare gli eventuali danni provocati dalla stessa.

I dipendenti non devono mai condurre personalmente verifiche o investigazioni al fine di non distruggere le prove eventualmente esistenti, salvo che siano stati formalmente incaricati di tali compiti.

Le verifiche poste in essere devono valutare se la violazione dei dati abbia comportato o meno un rischio per i diritti e le libertà delle persone fisiche, il quale è da considerarsi sicuramente presente laddove la violazione possa causare danni materiali o immateriali alle persone fisiche, tra cui a titolo esemplificativo: perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Nel valutare il rischio, è necessario tenere in considerazione i seguenti fattori: il tipo di violazione, la natura, la gravità, il volume di dati personali, la facilità di identificazione degli interessati, le caratteristiche particolari degli interessati o del titolare, oltre che il numero di persone interessati coinvolti.

Tali verifiche devono essere svolte e, se possibile, concluse **entro 24 ore** dal momento in cui il Responsabile Interno del Trattamento ha ricevuto la notifica da parte del responsabile di funzione.

4) Esito valutazione

a) Valutazione del rischio: esito negativo ➔ chiusura report interno

Qualora all'esito di tali valutazioni risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Responsabile Interno del Trattamento, per conto del Titolare:

i. integra il report interno ricevuto dal responsabile di funzione con le risultanze delle verifiche e della valutazione del rischio effettuate sotto il suo controllo, specificando i criteri adottati per il giudizio di probabilità del rischio e descrivendo le ulteriori azioni poste in essere per mitigare gli effetti della violazione;

ii. annota nel registro interno delle violazioni (si veda § 9.0 che segue) tutti i dettagli della violazione oggetto di valutazione del rischio.

b) Valutazione del rischio: esito positivo ➔ Notifica al Garante Privacy

Qualora invece all'esito di tali verifiche e valutazioni risulti probabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ove possibile, **entro 24 ore** dalla chiusura delle verifiche e valutazioni in merito alla violazione dei dati verificatasi e dalla redazione del relativo report interno, il Responsabile Interno del Trattamento, per conto del Titolare:

i. notifica la avvenuta violazione all'autorità di controllo competente (Garante per la protezione dei dati personali) tramite apposito modulo di notifica rilasciato dal Garante e allegato alla presente Policy 📎 **All. 4 – Modulo di notifica *data breach***.

La notifica al Garante della violazione dei dati personali deve contenere almeno i seguenti dati:

a) una descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie (quali, ad esempio, minori, clienti o dipendenti) e il numero approssimativo di

interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali oggetto di violazione (quali, ad esempio, archivi di dati relativi alla salute o contenenti dati relativi a conti correnti bancari);

b) una descrizione delle misure di sicurezza già implementate o che il Titolare del Trattamento propone di implementare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;

c) qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, i motivi del ritardo.

Qualora e nella misura in cui non sia possibile fornire tutte le informazioni richieste nel Modulo contestualmente, il Responsabile Interno del Trattamento potrà fornire inizialmente sommarie informazioni in relazione alla violazione verificatasi, purché ciò avvenga immediatamente dopo l'avvenuta conoscenza della stessa, integrando poi la comunicazione in un momento successivo. Tali sommarie informazioni devono in ogni caso consentire al Garante di effettuare una prima valutazione dell'entità della violazione. Ulteriori dettagli potrebbero essere richiesti dal Garante durante l'attività istruttoria relativa alla violazione.

c) Valutazione del rischio: esito positivo ➔ Comunicazione della violazione all'interessato

Qualora all'esito delle suddette verifiche e valutazioni risulti che la violazione la violazione dei dati personali presenti un rischio ***elevato*** per i diritti e le libertà delle persone fisiche, **non appena possibile**, il Responsabile Interno del Trattamento:

i. comunica la avvenuta violazione **anche** alle persone fisiche cui i dati si riferiscono tramite apposito format allegato 📎 **All. 5 – Modello di comunicazione della violazione all'interessato**.

Le violazioni devono essere comunicate ai soggetti interessati direttamente con modalità di comunicazione dedicate e trasparenti, tali da garantire che essi comprendano le informazioni loro fornite.

Tale comunicazione ha infatti lo scopo di fornire ai soggetti interessati le informazioni specifiche sulle azioni che dovrebbero nel caso specifico implementare per proteggersi dalla violazione.

Ad esempio, la comunicazione deve contenere consigli pratici per le persone fisiche per mitigare le conseguenze di una violazione (ad esempio, effettuare un reset delle password).

La comunicazione ai soggetti interessati non è necessaria quando:

a) il Titolare del Trattamento abbia messo in atto, prima della violazione, misure tecniche ed organizzative appropriate per proteggere i dati personali (quali, ad esempio, una crittografia all'avanguardia);

b) il Titolare del Trattamento abbia, immediatamente dopo la violazione, implementato contromisure per assicurare che l'elevato rischio per i diritti e le libertà delle persone fisiche non sia più suscettibile di verificarsi;

c) contattare i soggetti interessati richiederebbe uno sforzo sproporzionato per il titolare.

Il Titolare del trattamento, per mezzo del Responsabile Interno del Trattamento, deve documentare tutte le violazioni verificatesi o anche solo sospettate, indipendentemente dal fatto che esse siano state notificate o meno, al fine di poter dimostrare che il trattamento di dati è effettuato conformemente alla normativa privacy applicabile.

A tal fine, il Responsabile Interno del Trattamento deve tenere un registro interno delle violazioni **All. 6 – Modello di registro delle violazioni** in cui vengano di volta in volta registrati tutti i dati, le informazioni e le circostanze riguardanti le violazioni di dati personali, anche solo sospette, verificatesi nell'ambito dei trattamenti effettuati dall'Associazione (tra cui, ad esempio, le sue cause, le circostanze dell'incidente e quali dati personali siano stati compromessi, le conseguenze della violazione e le contromisure adottate dal Titolare del Trattamento). Il Titolare, per mezzo della Segreteria di Direzione, attua le misure di sicurezza tecnologiche e organizzative al fine di garantire la protezione dei dati contenuti nel Registro (es. che il registro sia accessibile solo da personale preventivamente autorizzato, dotato di accesso riservato e protetto tramite credenziali riservate etc.).

18 FORMAZIONE

La formazione delle Persone Autorizzate è obbligo di legge e deve essere evasa tramite corsi interni 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.

La formazione è di competenza del Responsabile Interno del Trattamento.

19 SANZIONI

Il mancato rispetto di quanto previsto nella presente Policy può comportare l'avvio di procedure disciplinari sulla base di quanto previsto dallo Statuto dei Lavoratori e dal CCNL applicato e, in determinate circostanze, potranno essere intraprese opportune azioni legali.