DIREZIONE DIDATTICA STATALE
2° CIRCOLO "E.Celentano" - POMPEI -
Via Civita Giuliana n. 26 - ☎ 081/8506209
Codice Scuola : NAEE220002 - C.F. 82015230632
Posta ordinaria: naee220002@istruzione.it
Posta PEC: naee220002@pec.istruzione.it
Sito WEB: www.pompeisecondocircolo.edu.it
Codice univoco IPA: UFJ5EW

Prot. 2962 / 1.4 Pompei, 05/06/2023

SITO WEB

LINEE GUIDA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

Il Regolamento Generale sulla Protezione dei Dati (Reg. UE 679/2016), di seguito il Regolamento, introduce l'obbligo di notificare una violazione dei dati personali (in appresso: "violazione") all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio 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.

Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Al fine di identificare e, se necessario, notificare correttamente un data breach all'autorità garante competente e/o agli interessati, il Dirigente Scolastico intende definire nel presente documento le procedure da seguire qualora avvenga un presunto data breach all'interno dell'amministrazione.

Le presenti linee guida sono state redatte sulla base di quelle relative alla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, redatto dal gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017 e nella versione emendata e adottata in data 6 febbraio 2018. Tali linee guida sono reperibili sul sito del garante per la protezione dei dati personali al link https://www.garanteprivacy.it/regolamentoue/databreach.

DEFINIZIONE DI VIOLAZIONE

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come segue:

> "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".

Di seguito una descrizione della terminologia, come descritto dal Garante per la Protezione dei Dati personali:

- **Distruzione:** il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento.
- **Perdita:** Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.
- **Divulgazione o accesso:** un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.
- **Modifica:** si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi.

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso. Ulteriori esempi possono essere visionati nell'allegato B al presente regolamento.

Inoltre, le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni1:

- **"violazione della riservatezza"**, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- **"violazione dell'integrità"**, in caso di modifica non autorizzata o accidentale dei dati personali;
- **"violazione della disponibilità"**, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Va altresì osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.

(effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34.

PROCEDURA DA ADOTTARE IN CASO DI PRESUNTA VIOLAZIONE DEI DATI PERSONALI

Qualora un dipendente dell'amministrazione rilevi una possibile violazione dei dati personali, esso è tenuto ad informarne il Dirigente Scolastico o, qualora esso non sia immediatamente disponibile, il Responsabile della Protezione dei Dati ed altre eventuali figure che gestiscono i sistemi informatici o che forniscono servizi di assistenza e consulenza informatica e normativa in modo da garantire la massima tempestività di intervento.

A questo punto il D.S., in concerto con l'RPD e l'amministratore di sistema informatico (qualora si tratti di una violazione informatica), provvederà ad effettuare una prima indagine interna e a definire la gravità dell'eventuale violazione. In particolare, si dovrà procedere a identificare i possibili rischi da essa derivanti e a definire le ulteriori azioni da intraprendere per minimizzare questi rischi. In questa fase il dirigente scolastico dovrà valutare l'opportunità o la necessità di fare la comunicazione al Garante, che dovrà intervenire entro le 72 ore dalla conoscenza del fatto, ed eventualmente alle persone fisiche minacciate nei loro diritti dall'evento. In merito alla scelta dovranno essere coinvolti ed esprimeranno il proprio parere il RPD ed eventuali altri consulenti informatico/normativi ma la decisione finale dovrà essere del dirigente scolastico che risponderà di fronte alla legge della scelta operata in base al principio della responsabilizzazione. Nel momento in cui il titolare del trattamento dovesse decidere in modo difforme dal parere del RPD è opportuno che rediga un documento in cui in cui illustri le motivazioni che l'hanno indotto alla scelta.

Il presente documento ha lo scopo di fornire al titolare del trattamento dei riferimenti nel momento in cui deve decidere le azioni da intraprendere in caso di violazione dei dati personali e deve valutare l'opportunità di fare la comunicazione al Garante o agli interessati (vedasi anche allegato B).

MODALITÀ DI NOTIFICA AL GARANTE E AGLI INTERESSATI

Qualora il dirigente scolastico ritenesse di dover fare la segnalazione al Garante dovrà inviare, dalla casella PEC istituzionale dell'amministrazione, una mail indirizzata alla casella protocollo@pec.gpdp.it con oggetto **notifica data breach** e contenente in allegato una relazione effettuata sulla base del modello messo a

Esempio

Nell'ambito della notifica all'autorità di controllo, il titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

In ogni caso, l'autorità di controllo può richiedere ulteriori dettagli nel contesto dell'indagine su una violazione.

Notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto:

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

Ciò significa che il regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. È più probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un'indagine forense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali. Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1. Il Gruppo di lavoro raccomanda che, all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'autorità di controllo dovrebbe concordare le modalità e le tempistiche per la fornitura delle informazioni supplementari. Questo non impedisce al titolare del trattamento di trasmettere ulteriori informazioni in qualsiasi altro momento, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che devono essere forniti all'autorità di controllo.

L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo. La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette.

Tuttavia, lo scopo della notifica all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte (cfr. sezione III). In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta. È opportuno inoltre precisare che se, dopo la notifica iniziale, una

fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'allegato B delle presenti linee guida fornisce un elenco non esaustivo di esempi di casi in cui una violazione può presentare un rischio elevato per le persone fisiche e, di conseguenza, in cui il titolare del trattamento deve comunicarla agli interessati.

Informazioni da fornire nelle notifiche agli interessati

Ai fini della comunicazione alle persone fisiche, l'articolo 34, paragrafo 2, specifica che:

> "La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".

Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

Contattare l'interessato

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni

libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

ALLEGATI

Vengono di seguito riportate le istruzioni schematiche relative alla notifica della violazione (allegato A), ed una lista non esaustiva delle possibili violazioni (allegato B), come indicato dall'autorità Garante per la Protezione dei Dati Personali.

distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	**Notifica all'autorità di controllo?**	**Comunicazione all'interessato?**	**Note/raccomandazioni**
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un	Sì, effettuare la segnalazione	Sì, effettuare la segnalazione alle	Se fosse stato disponibile un backup e i dati

vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.
vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

ALLEGATO A

Al

(Indirizzare al titolare o al responsabile del trattamento)

OGGETTO: **ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI**
(artt. 7 e 8 del Codice)

Il/La sottoscritto/a
nato/a a il ,
esercita con la presente richiesta i suoi diritti di cui all'articolo 7 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196):

(BARRARE SOLO LE CASELLE CHE INTERESSANO)

Accesso ai dati personali

(art. 7, comma 1, del Codice)

Il sottoscritto intende accedere ai dati che lo riguardano e precisamente:

- ☐ chiede di confermargli l'esistenza o meno di tali dati, anche se non ancora registrati, e/o
- ☐ chiede di comunicargli i medesimi dati in forma intelligibile (art. 10 del Codice).

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

(BARRARE SOLO LE CASELLE CHE INTERESSANO)

Richiesta di conoscere alcune notizie sul trattamento

(art. 7, comma 2, del Codice)

Il sottoscritto chiede di conoscere:

- ☐ l'origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- ☐ le finalità del trattamento dei dati che lo riguardano;
- ☐ le modalità del medesimo trattamento;
- ☐ la logica applicata al trattamento effettuato con strumenti elettronici;
- ☐ gli estremi identificativi del titolare del trattamento (ovvero della pubblica amministrazione, della persona giuridica pubblica o privata, dell'associazione od organismo che li tratta);
- ☐ gli estremi identificativi del/i responsabile/i del trattamento (nel caso in cui siano designati ai sensi dell'art. 29 del Codice);
- ☐ i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o di incaricati o di rappresentante designato nel territorio dello Stato;
- ☐ gli estremi identificativi del rappresentante del titolare nel territorio dello Stato (se designato ai sensi dell'art. 5 del Codice).

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

(BARRARE SOLO LE CASELLE CHE INTERESSANO)

Richiesta di intervento sui dati

(art. 7, comma 3, del Codice)

Il sottoscritto chiede di effettuare le seguenti operazioni:

- ☐ aggiornamento dei dati;
- ☐ rettificazione dei dati;
- ☐ integrazione dei dati;
- ☐ cancellazione dei dati trattati in violazione di legge (compresi quelli di cui non è necessaria la conservazione);
- ☐ trasformazione in forma anonima dei dati trattati in violazione di legge (compresi quelli di cui non è necessaria la conservazione);
- ☐ blocco dei dati trattati in violazione di legge (compresi quelli di cui non è necessaria la conservazione);
- ☐ attestazione che tale intervento sui dati è stato portato a conoscenza, anche per quanto riguarda il suo contenuto, di coloro ai quali i dati sono stati comunicati o diffusi.

La presente richiesta riguarda *(indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*:

Opposizione al trattamento per fini pubblicitari

(art. 7, comma 4, del Codice)

- ☐ Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Opposizione al trattamento per motivi legittimi

(art. 7, comma 4, del Codice)

- ☐ Il sottoscritto si oppone al trattamento dei dati per i seguenti motivi legittimi:

La presente richiesta riguarda *(indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento)*:

Il sottoscritto si riserva di rivolgersi all'autorità giudiziaria o al Garante (con segnalazione, reclamo o ricorso: artt. 141 ss. del Codice) se entro 15 giorni dal ricevimento della presente istanza non perverrà un riscontro idoneo.

Recapito per la risposta:

☐ Indirizzo postale:
Via/Piazza .....
Comune .....
Provincia ..... Codice postale .....

oppure
☐ *e-mail*: .....
oppure
☐ telefax: .....
oppure
☐ telefono*: .....

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

.....

.....

.....

.....

Estremi di un documento di riconoscimento**:

.....

.....

(Luogo e data) *(Firma)*

* Le richieste in esame e la relativa risposta possono essere anche orali. Tuttavia, se l'interessato si rivolge al Garante con un ricorso, occorre allegare copia della richiesta rivolta al titolare (o al responsabile, se designato) del trattamento.

** Esibire o allegare copia di un documento di riconoscimento, se l'identità del richiedente non è accertata con altri elementi.