Camera di Commercio
Gran Sasso d'Italia

Camera di Commercio, Industria, Artigianato e Agricoltura del Gran Sasso d'Italia

Procedura di gestione dei data breach

ai sensi del Regolamento UE 679/2016

OBIETTIVO E CAMPO DI APPLICAZIONE

Obiettivo della presente procedura è descrivere le attività relative al processo di segnalazione e gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali in qualsiasi modalità svolti dalla Camera di Commercio di Commercio del Gran Sasso d'Italia.

Tale processo regolamenta la gestione degli allarmi di sicurezza, la conduzione delle attività investigative funzionali alla individuazione di tutti gli elementi utili alla completa definizione di una violazione, l'attivazione delle strategie di contenimento o delle azioni correttive, la gestione degli adempimenti richiesti dalla normativa nei confronti del Garante per la protezione dei dati personali e degli interessati, le modalità per la tenuta di idonee registrazioni per documentare il rispetto degli obblighi imposti nel rispetto del principio di accountability.

Si tenga conto inoltre che:
a) nei rapporti di contitolarità ciascun contitolare attua la sua procedura per quanto attiene al trattamento dei dati che svolge. Nell'accordo di contitolarità possono tuttavia essere disposte specifiche procedure e/o modalità relativi ad obblighi di comunicazione tra le parti e tra queste ed il garante;
b) per quanto attiene ai data breach relativi alle ipotesi in cui la Camera di commercio opera in qualità di responsabile esterno del trattamento, ex art. 28 del GDPR, dovranno essere osservate anche le indicazioni ed istruzioni fornite dal Titolare nel documento di nomina/designazione.

La presente procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, Responsabili delle Unità organizzative, funzionari o, comunque, referenti delle Aree/Uffici/Servizi della Camera di Commercio.

La presente procedura è pubblicata sul sito web istituzionale nella Sezione Amministrazione Trasparente ->Disposizioni Generali ->Atti generali->Atti amministrativi generali e nella pagina Altri contenuti/Trattamento dati personali e Responsabile Protezione dei Dati.

RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Notifica di una violazione dei dati personali all'autorità di controllo (art. 33 del GDPR)
2. Comunicazione di una violazione dei dati personali all'interessato (art. 34 del GDPR)
3. WP250rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottate il 03/10/2017 e riemesse il 06/02/2018
4. Provv. del Garante 30 luglio 2019, n. 157, *sulla notifica delle violazioni dei dati personali (data breach).*

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)
RPD	Responsabile della protezione dei dati

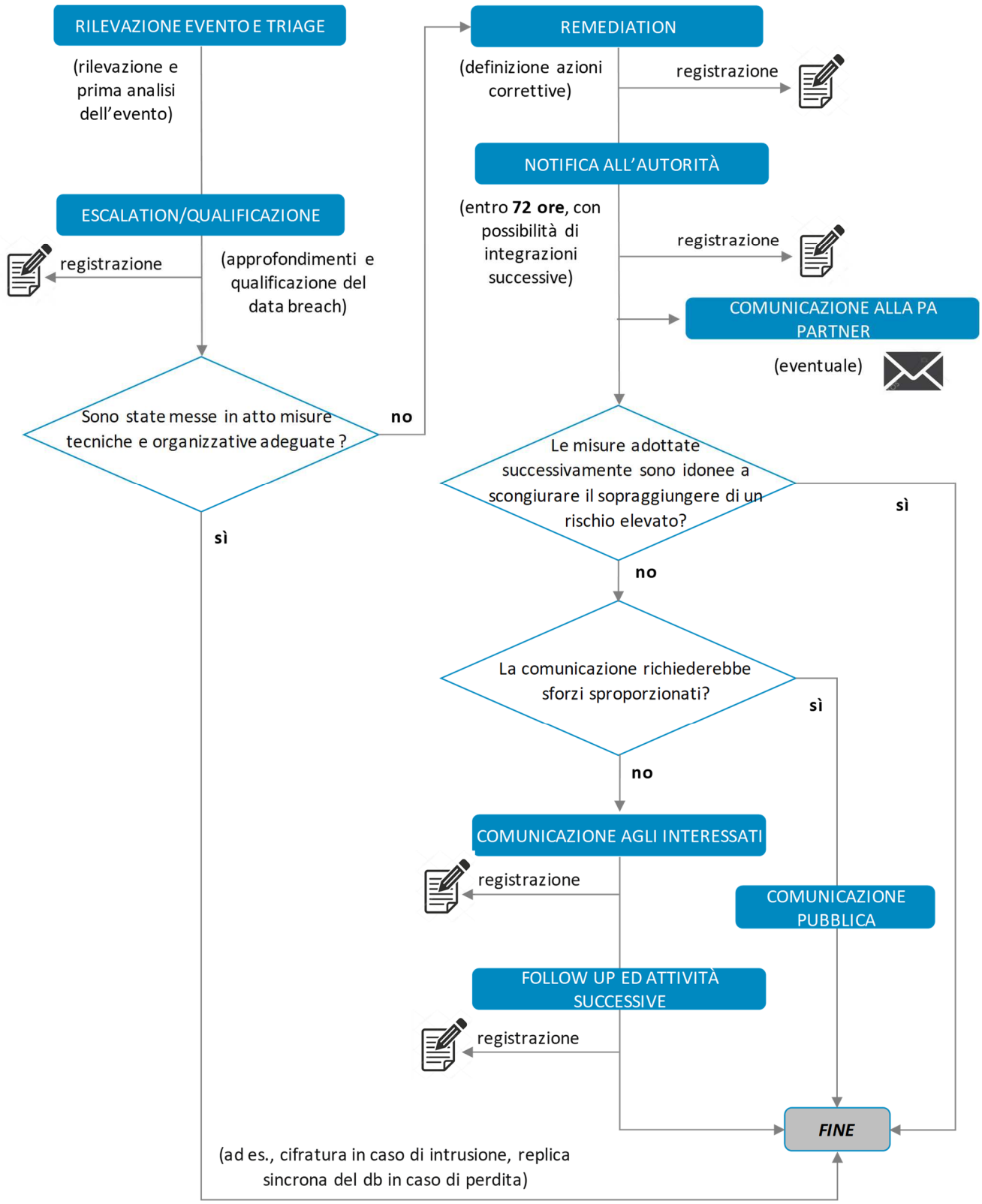
Delegato del Titolare	Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR
SG f.f.	Segretario Generale f.f. della Camera di commercio
Evento	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi
Violazione (data breach)	Qualsiasi incidente di sicurezza che comporti 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

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Stato	Descrizione	Approvazione
14 giugno 2021	Approvato	1° emissione	Determina del Conservatore – Delegato del Titolare

FASI DEL PROCESSO

La gestione di un data breach può riassumersi nelle fasi di seguito rappresentate.



RILEVAZIONE EVENTO E TRIAGE

La rilevazione di un evento può avvenire da diverse fonti:

- SEGNALAZIONE AUTOMATICA: sistemi di segnalazione automatica (es. SIEM - *Security Information and Event Management*), come le violazioni derivanti da superamento dei sistemi di Firewall della Camera di Commercio (gestiti direttamente o tramite soggetti esterni), ovvero gestiti da InfoCamere.

- SEGNALAZIONE INTERNA: attività di monitoraggio degli eventi da parte del CED/Amministratori di sistema; comunicazione di: malfunzionamenti irrituali o blocco dei sistemi, furti, smarrimenti, intrusioni fisiche nei locali archivio, [anche sulla base di quanto indicato nel Disciplinare sull'uso di internet, posta elettronica ed altri strumenti informatici e telematici], etc.

- SEGNALAZIONE ESTERNA: nell'ambito dell'attività di monitoraggio, assistenza e manutenzione da parte di fornitori esterni di applicativi, supporto sistemistico, servizi di consulenza, etc. ovvero da parte di utenti finali dei servizi della Camera di Commercio, ovvero da parte di Responsabili esterni nominati ex art. 28 del GDPR.

  In particolare, in tutti i contratti che attribuiscano funzioni di amministrazione di sistemi o deleghino trattamenti di dati personali a soggetti esterni qualificati o qualificabili come responsabili esterni del trattamento ex art. 28 GDPR, devono essere inserite clausole contrattuali che prevedono l'obbligo:
  - di comunicazione immediata di eventuali eventi di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse. Nello standard contrattuale è previsto che la segnalazione pervenga al Referente contrattuale;
  - di fornire, in caso di necessità, anche attraverso il RPD eventualmente nominato, la massima disponibilità e collaborazione per l'analisi e risoluzione di eventuali criticità emergenti per l'ambito di trattamento assegnato.

Secondo il WP 29, il Regolamento "impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Inoltre, il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica". I sopra indicati sistemi di "segnalazione" dovrebbero, pertanto, essere predisposti (si pensi al SIEM) per indicare quando, con ragionevole certezza, si sia verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Le segnalazioni pervengono al Dirigente dell'Area di riferimento (o suo delegato) coinvolta dall'evento che attiva (anche in modalità videoconferenza) il team di primo intervento (T1I) composto da:
- un referente CED ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente alla Camera di Commercio[1];
- un eventuale referente delle Società in house (o esterne) coinvolte nel trattamento[2];
- [il RPD][3].

Il team di primo intervento, sotto la responsabilità del citato Dirigente, ha il compito di verificare il perimetro dell'evento, ovvero almeno le seguenti informazioni:

[1] Il termine "CED" indica, nella sua globalità, l'ufficio in cui opera l'Amministratore di sistema. L'"Amministratore di sistema" è la persona/e fisica/che (anche appartenenti a società designate Responsabili esterni del trattamento) debitamente incaricata dello svolgimento di detto ruolo, ai sensi della normativa vigente.

[2] A norma dell'art. 28, par. 3, lett. h) del GDPR, il Responsabile del trattamento "mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi… e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato".

[3] Il coinvolgimento del RPD in questa prima fase è opzionale. Ciò dipende da alcuni fattori: a) se il RPD sia soggetto interno o esterno [sebbene sia prevista anche la modalità di comunicazione in videoconferenza]; b) se sia in possesso o meno di competenze tecniche.

1. sistema, infrastruttura, base dati oggetto dell'evento;
2. tipologia dell'evento verificatosi;
3. tipologia e volume dei dati e degli interessati coinvolti:
4. misure di sicurezza applicate;
5. attività di remediation (azioni correttive) ipotizzabili.

In caso di mancato coinvolgimento di dati personali, il Team di primo intervento attribuisce le responsabilità per l'avvio delle eventuali azioni correttive e registra l'evento su una apposita scheda di rilevazione. Ad esito delle azioni correttive, la fase si chiude con il follow up di remediation (registrazione sul Service Desk)

Nel caso in cui l'evento coinvolga dai personali, viene attivata l'escalation che comporta la segnalazione della scheda di registrazione al RPD e la costituzione del Team di II intervento.

Questa fase deve concludersi entro 24 ore dalla rilevazione dell'evento.

Per una migliore chiarezza si riproducono alcune indicazioni del WP29.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione. Tuttavia, il titolare del trattamento potrebbe già disporre di una valutazione iniziale del rischio potenziale che potrebbe derivare da una violazione come parte di una valutazione d'impatto sulla protezione dei dati effettuata prima dello svolgimento del trattamento interessato. Tuttavia, tale valutazione può essere più generale rispetto alle circostanze specifiche di un'effettiva violazione e, pertanto, in ogni caso dovrà essere effettuata una valutazione aggiuntiva che tenga conto di tali circostanze.

ESCALATION, QUALIFICAZIONE DELLA VIOLAZIONE E REMEDIATION

Alla ricezione della scheda di segnalazione, il Dirigente dell'Area di riferimento costituisce il Team di secondo intervento (T2I) costituito da:

- il RPD della Camera di Commercio;
- il Responsabile dell'Ufficio/Capo Progetto/etc. responsabile del processo in relazione al quale si ipotizza la violazione di dati;
- il responsabile o un referente dell'Ufficio legale;
- il responsabile del CED ove l'evento riguardi l'infrastruttura, sistemi informativi/banche dati gestite internamente alla Camera;
- lo specialista della società o soggetto che ha realizzato/fornito il prodotto/servizio interessato dall'incidente e/o il RPD (ove nominato) o altro referente specializzato della Società in house coinvolta nel trattamento[4]
- l'eventuale consulenza tecnica o giuridica qualora necessaria.

Il Team ha il compito di verificare, a norma dell'art. 33, par. 1, del GDPR, la probabilità che la violazione dei dati personali presenti un rischio (soprattutto se questo può qualificarsi come "elevato") per i diritti e le libertà delle persone fisiche e, di conseguenza, decidere le misure di risposta all'emergenza.
A tal fine:

a) sono raccolte o consolidate/approfondite le informazioni di cui al format per la comunicazione al Garante **(All. 1),** ove disponibili, anche al fine di minimizzare i tempi di risposta;
b) sono effettuate le seguenti valutazioni[5]:
   - natura della violazione e potenziale esposizione degli interessati (c.d. gravità dell'accadimento);
   - priorità, in funzione dell'urgenza (valutata sulla base di quanto velocemente potrebbero verificarsi danni);
   - impatto potenziale dell'esposizione degli interessati (valutazione dell'entità dei danni agli interessati)[6];
   - adeguatezza delle misure di sicurezza già implementate rispetto al potenziale danno arrecabile agli interessati.

Per un quadro delle valutazioni dei rischi si rinvia anche a quanto contenuto nelle Linee guida del WP29 (WP250rev.01).

Ad esito dell'analisi:

A. nel caso in cui la violazione – in funzione dell'adeguatezza delle misure implementate – non costituisca un rischio per gli interessati, il Dirigente o suo delegato provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD; copia del verbale deve essere inviato:
   - al RPD che provvede ad aggiornare il "Registro dei Data Breach" come da format allegato **(All. 4)**
   - al Dirigente Delegato del Titolare del trattamento per la condivisione finale sull'esito delle valutazioni

B. nel caso in cui sia stato valutato che le misure implementate siano insufficienti alla tutela degli interessati:
   1. il team provvede ad identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata ed il miglior esito ai fini della minimizzazione del possibile danno agli interessati
   2. il Dirigente provvede a:
      - definire ed assegnare responsabilità e tempistiche per la remediation, compresi i soggetti esterni coinvolti;
      - verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD;

---

[4] Cfr. nota n. 1.

[5] Per la valutazione qualitativa degli impatti è possibile partire dai parametri di gravità/probabilità utilizzati nell'ambito dell'assessment dei trattamenti della Camera di commercio e dai valori ivi rilevati, procedendo per successivi affinamenti fino a focalizzare l'analisi sull'asset colpito dalla violazione.

[6] Ovvero danno fisico, materiale o immateriale, in particolare: perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti; discriminazioni; furto o usurpazione d'identità; perdite finanziarie; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale; decifratura non autorizzata della pseudonimizzazione; qualsiasi altro danno economico o sociale significativo" cfr. considerando 75 e 85 GDPR.

- compilare o completare il Modello per la notificazione al Garante (riportato nell'Allegato al presente documento), indicando se le azioni correttive (c.d. attività di remediation) sono già concluse od ancora in itinere;
- inviare entrambi i documenti al Dirigente delegato del Titolare per la condivisione finale sull'esito delle valutazioni e la decisione se procedere o meno alle notificazioni;
- predisporre, qualora ne ricorrano le condizioni, la comunicazione da inviare all'interessato (ovvero la comunicazione pubblica), contenenti le indicazioni riportate **nell'All. 2**.

Questa fase deve concludersi entro ulteriori 36 ore dalla rilevazione dell'evento.

INVIO DELLE NOTIFICAZIONI

Il Garante, con il provv. 30 luglio 2019, n. 157, ha definito il Modello per la notifica delle violazioni dei dati personali, ai sensi dell'art. 33 del GDPR e dell'art. 26 del D.Lgs. n. 51/2018. Il Modello, secondo le modalità di cui all'art. 65 del D.Lgs. n. 82/2005 (CAD), è riprodotto nell'Allegato 1 al presente documento.

La notifica avviene mediante la compilazione del Modello nell'ambito dei sistemi telematici indicati nel sito istituzionale del Garante.

Il Modello deve essere sottoscritto con firma digitale dal Dirigente delegato del Titolare e trasmesso al Garante nel più breve tempo possibile, **possibilmente entro 72 ore** dall'avvenuta conoscenza da parte del Titolare, di un evento qualificabile come Data breach[7].

Ove avvenga oltre tale limite temporale è necessario corredarla dei motivi del ritardo[8].

Qualora non si disponga di tutte le informazioni è possibile inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni.

Il Dirigente dell'Area di riferimento invia il verbale e copia del Modello sottoscritto dal dal Dirigente delegato del Titolare:

- al RPD che aggiorna o provvede a far aggiornare il "Registro dei Data Breach";
- al referente dell'Amministrazione Pubblica da cui eventualmente la Camera di Commercio ha ricevuto l'incarico di trattare i dati personali[9], previa valutazione di opportunità condotta congiuntamente con il dal Dirigente delegato del Titolare ed a seguito dell'avvenuta notifica al Garante.

Ove le misure di cui al punto B) del paragrafo precedente siano adottate immediatamente, la fase si chiude con il follow up di remediation (mediante verbalizzazione degli esiti da parte del Dirigente dell'Area di riferimento)[10]

Nel caso in cui tali misure necessitino di maggior tempo per l'implementazione ovvero non siano in grado di minimizzare i rischi per gli interessati, il Dirigente dell'Area di riferimento:

a) provvede a definire i contenuti della comunicazione agli interessati, che – con linguaggio semplice e chiaro - deve contenere almeno i seguenti elementi:
   - la natura della violazione dei dati personali;
   - le probabili conseguenze della violazione dei dati personali;
   - le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione;

[7] Nelle fasi indicate in precedenza sono disponibili 12 ore che possono essere distribuite come si ritenga maggiormente opportuno.

[8] ad es., data breach particolarmente complesso, serie di attacchi/violazioni consecutive che necessitano di una reazione complessa.

[9] Ad es., sulla base di una convenzione/protocollo d'intesa.

[10] "Non è richiesta la comunicazione all'interessato… se il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati" (art. 34, par. 3, lett. b del GDPR).

- il nome e i dati di contatto del responsabile della protezione dei dati.

La comunicazione – un cui esempio è riportato nell'All. 2 – è sottoposta a parere del RPD e ad approvazione del dal Dirigente delegato del Titolare.

b) verifica la fattibilità di reperimento dei dati di contatto degli interessati coinvolti o potenzialmente coinvolti; nel caso in cui si valuti che la comunicazione agli interessati possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec), provvede all'invio massivo della comunicazione.

c) Ove non vi sia disponibilità di dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati, provvede a darne pubblicità nelle modalità concordate con il Dirigente delegato del TitolareD e RPD (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc.).

La comunicazione agli interessati deve essere formalizzata "senza ingiustificato ritardo".

Dell'avvenuta comunicazione è data informazione al RPD.

E' bene ricordare che:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche.

ATTIVITA' SUCCESSIVE

Se durante le fasi precedenti si sospetta che la violazione possa essere stata provocata in maniera intenzionale da un esterno o da un utente interno si attiva il processo di raccolta delle evidenze o prove con ulteriori investigazioni anche difensive.

L'attività, ove necessario, può essere gestita secondo quanto previsto dall'art. 391 nonies[11] o dall'art. 327 bis c.p.p.[12] e deve rispettare gli standard e le normative (raccolta e "catena di custodia") in termini di analisi forense, al fine di poter intraprendere successivamente un'azione legale nei confronti dell'eventuale responsabile.

Qualora non si riscontrasse questa condizione, l'analisi post-violazione sarà finalizzata all'apprendimento delle cause che hanno generato l'evento al fine di imparare dai propri errori e per fornire ulteriori informazioni per la risoluzione di eventuali criticità collegate o ricorrenti.

Ad esito delle notificazioni al Garante ed agli interessati, il RPD deve:

- gestire in prima persona le relazioni e gli eventuali feedback pervenuti dal Garante e dalle altre Istituzioni coinvolte, coordinando – con l'ausilio della sua struttura di supporto – l'aggiornamento del "Registro dei Data Breach" (un cui modello è riportato nell'All. 4);
- gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente della Segreteria generale, ovvero dell'Ufficio legale o, ancora, dell'Area/Ufficio di riferimento interessata dalla la violazione.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati

[11] Se precedente all'instaurazione di un procedimento penale.

[12] Se già instaurato il procedimento.

personali, L'Ente svolge attività di informazione e formazione con riferimento ai contenuti del presente documento.

MATRICE DELLE RESPONSABILITA'

Legenda

- R = Responsabile
- C = Coinvolto
- I = Informato

Fase	*Attività*	*Soggetto/ Struttura*	Dirigente dell'Area coinvolta	Dirigente Delegato del Titolare	Responsabile della Protezione dei Dati	Ufficio Legale	CED|Amministratore di sistema	Società esterne Responsabili del trattamento	
RILEVAZIONE E TRIAGE	Rilevazione evento		**R**				**C**	**C**	
	Triage		**R**				**R**	**R**	
	Escalation		**R**		**I**	**I**	**I**	**I**	
QUALIFICAZIONE	Raccolta informazioni		**R**		**C**	**C**	**C**	**C**	
	Valutazione d'impatto		**R**		**C**	**C**	**C**	**C**	
	Verbalizzazione esiti		**R**	**I**	**I**				
	Tracciamento su Registro Data Breach				**R**				
	Identificazione azioni correttive		**R**		**C**				
	Implementazione azioni correttive		**R**				**R**	**R**	
	Compilazione format notifica		**R**		**C**				
	Monitoraggio azioni correttive		**R**		**C**		**C**	**C**	
NOTIFICAZIONI	Sottoscrizione ed invio format notifica		**I**	**R**	**C**				
	Informativa a PA partner		**R**	**I**					
	Predisposizione comunicazione Interessati		**R**	**C**	**C**				
	Approvazione comunicazione			**R**	**C**				
	Invio o pubblicazione comunicazione		**R**	**I**	**I**				
ATTIVITÀ SUCCESSIVE	Avvio indagini difensive		**I**	**C**		**R**			
	Rapporti con il Garante		**I**	**C**	**R**				
	Rapporti con Interessati		**R**		**C**				

ALLEGATO 1 – MODELLO DI NOTIFICA AL GARANTE

Nel file allegato al presente documento è riportato il Modello di notifica, approvato dal Garante con il Provv. 30 luglio 2019, n. 157.

ALLEGATO 2 – MODELLO DI COMUNICAZIONE ALL'INTERESSATO (*)

Denominazione del Titolare del trattamento	
Dati di contatto	
Soggetto che effettua la notifica	
Ruolo del soggetto che effettua la notifica	
Responsabile della Protezione dei dati	
Dati di contatto del RPD	

Interessato destinatario della comunicazione	

Modalità della comunicazione

☐ Raccomandata A/R
☐ PEC
☐ Posta elettronica
☐ Fax
☐ Altro: _____

Spett. Società/Egr. Sig……./

siamo spiacenti di informare che in data …….. abbiamo rilevato di aver subito una violazione dei dati personali la riguardano.

Nel prosieguo, in termini sintetici, è fornito – ai sensi di quanto previsto dall'art. 34 Regolamento UE n. 679/2016 (GDPR) – un quadro di quanto è accaduto.

La violazione è stata anche notificata al Garante.

Breve descrizione della violazione di dati personali e delle sue modalità

(*) Qualora la comunicazione richieda – ex art. 34, par. 3, lett. c) del GDPR – uno sforzo proporzionato (in relazione, per es. alle attività da svolgere e/o ai costi da sostenere), "(…) si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

Dispositivo oggetto della violazione

☐ Computer
☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di un file
☐ Strumento di back-up
☐ Rete
☐ Altro:

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari
☐ Ancora sconosciuto
☐ Altro:

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

Indicare:

A) Numero approssimativo di registrazioni dei dati personali oggetto della violazione
B) Categoria e numero approssimativo degli interessati coinvolti dalla violazione
C) Livello di gravità elevato della violazione per i diritti e le libertà delle persone fisiche
D) Possibili conseguenze della violazione.

(secondo le valutazioni del Titolare)

Misure tecniche e organizzative applicate preventivamente e quelle applicate successivamente alla violazione per porre rimedio alla violazione o per attenuarne le conseguenze

Per ulteriori informazioni, può essere contattato ……

ALLEGATO 3 – CONTATTI DI EMERGENZA DEI SOGGETTI COINVOLTI NELLA PROCEDURA

RPD	dpo@gransasso.camcom.it
CED/Amministratore di sistema	servizi.informatici@gransasso.camcom.it
HELP DESK INFOCAMERE	account.manager.dars@infocamere.it
ISWEB	supporto@isweb.it
ALTRO	

ALLEGATO 4 – REGISTRO DEI DATA BREACH

N. record/anno	Banca dati/Archivio coinvolto dalla violazione	Processo/progetto ed Ufficio di riferimento	Cause della violazione (vulnerabilità)	Tipologia e modalità di realizzazione	Conseguenze della violazione	Azioni correttive adottate	Follow up azioni correttive	Notifica al Garante (sì/no) [indicare protocollo comunicazione]	Notifica agli Interessati (sì/no) [indicare protocollo comunicazione]	Prescrizioni specifiche del Garante

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).
Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1] ○ Completa ◉ Integrativa [2] rif.

Effettuata ai sensi del ◉ art. 33 RGPD ○ art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.
2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)
3 Indicare nome e cognome nel caso di persona fisica

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

◉ Responsabile della protezione dei dati[4] - prot. n.

○ Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile ○ Rappresentante

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ○ Contitolare ○ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**
   - (•) Il
   - ( ) Dal (la violazione è ancora in corso)
   - ( ) Dal al
   - ( ) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**
   Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**
   - ( ) Il titolare è stato informato dal responsabile del trattamento
   - ( ) Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?**[9]

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali oggetto di violazione**
   - ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
   - ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
   - ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…)
   - ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

- ◯ N.
- ◯ Circa n.
- ◯ Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

- ☐ Dipendenti/Consulenti
- ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ Associati,soci, aderenti, simpatizzanti, sostenitori
- ☐ Soggetti che ricoprono cariche sociali
- ☐ Beneficiari o assistiti
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- ◯ N. interessati
- ◯ Circa n. interessati
- ◯ Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità: [17]

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

b) In caso di perdita di integrità:[18]

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

c) In caso di perdita di disponibilità:[19]

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. Potenziali effetti negativi per gli interessati

☐ Perdita del controllo dei dati personali
☐ Limitazione dei diritti
☐ Discriminazione
☐ Furto o usurpazione d'identità
☐ Frodi
☐ Perdite finanziarie
☐ Decifratura non autorizzata della pseudonimizzazione
☐ Pregiudizio alla reputazione
☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
☐ Conoscenza da parte di terzi non autorizzati
Qualsiasi altro danno economico o sociale significativo (specificare)

3. Stima della gravità della violazione

○ Trascurabile
○ Basso
○ Medio
○ Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati**

2. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

- ◯ Sì, è stata comunicata il
- ◯ No, sarà comunicata il
  in una data da definire
- ◯ No, sono tuttora in corso le dovute valutazioni[21]
- ◉ No e non sarà comunicata perché:
  - ☐ a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
    Spiegare le motivazioni
  - ☐ b) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
    Descrivere le misure applicate
  - ■ c) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
    Descrivere le misure adottate
  - ☐ d) detta comunicazione richiederebbe sforzi sproporzionati.
    Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia
[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679
[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: protocollo@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.