CAPITOLATO DEL SERVIZIO NECROFORICO, DI PULIZIA E DI MANUTENZIONE ORDINARIA DEL CIMITERO COMUNALE DI FROSSASCO IN VIA ROLETTO, 3. BIENNIO 2022/2023

CPV: 98371110-8 - Servizi cimiteriali

CIG Z88347BE09

ART.1 - OGGETTO DEL SERVIZIO

1. L'affidamento ha per oggetto il servizio necroforico, di pulizia e di manutenzione ordinaria del cimitero comunale di Frossasco, via Roletto, 3. Le prestazioni inerenti all'appalto in oggetto devono essere effettuate interamente a spese della impresa appaltatrice, con mano d'opera, materiali e attrezzature a carico della stessa, fatto salvo quanto diversamente previsto nel presente Capitolato.
2. L'attività di necroforo in ordine alle salme comprende: le inumazioni; le tumulazioni; le esumazioni, le estumulazioni, autorizzate e/o ordinate dalle competenti autorità sia comunali che giudiziarie; le esumazione ordinarie con l'onere della raccolta delle ossa rinvenute e loro deposito in ossario comune o in loculi - ossari; le operazioni di sanatoria e ripristino delle condizioni igieniche ordinate dall'autorità sanitaria in casi straordinari e d'emergenza; la sepoltura dei nati morti, feti e parti anatomiche riconoscibili; tutti gli interventi connessi e conseguenti alle operazioni di esumazione ordinaria/straordinaria, l'estumulazione ordinaria/straordinaria relativi alla destinazione del cadavere o dei resti mortali, servizio di presidio e assistenza durante i funerali ed interventi al valere delle salme, ceneri, resti ossei.
3. Le attività di pulizia e manutenzione ordinaria del cimitero comprendono tutte le prestazioni e forniture necessarie per mantenere lo stesso in condizioni ottimali di conservazione e decoro quali taglio del manto erboso, potatura di siepi e cespugli, pulizia dei percorsi pavimentati, riordino delle attrezzature mobili, pulizia canalette di scolo acque con relativi pozzetti di raccolta e degli scarichi delle fontanelle, pulizia dei servizi igienici, pulizia locali di servizio, riassetto e pulizia dei viali in ghiaietto con eventuale reintegro dello stesso, secondo istruzioni impartite dal servizio comunale competente, spargimento in caso di gelate di sabbia granita e sale nelle zone interne del cimitero ed all'ingresso dello stesso, posizionamento ordinato di fiori lasciati a seguito della sepoltura sulle tombe, fosse e loculi , se necessario, manutenzione ordinaria delle attrezzature e accessori (quali scale ad appoggio e a carrello, ringhiere ecc.) degli impianti cimiteriali, caricare e trasportare nelle discariche autorizzate tutto il materiale di risulta eventualmente prodotto nell'esecuzione delle lavorazioni di cui ai punti precedenti, eliminazione delle nidificazioni e degli escrementi di volatili dai ballatoi, scale e pianerottoli delle strutture immobili ospitanti i loculi, dalle ringhiere e parapetti con lavaggio periodico delle superfici di tali elementi.
4. Il servizio complessivo relativo alla gestione dei Servizi Cimiteriali è classificato a tutti gli effetti "Servizio Pubblico" o di "Pubblica Utilità" e per nessuna ragione le attività oggetto del presente capitolato speciale connesse a tali servizi potranno essere sospese, interrotte o abbandonate.
5. Indipendentemente dalle indicazioni riportate nel presente capitolato speciale d'appalto, l'impresa dovrà eseguire quanto indispensabile per conservare il decoro e l'igiene degli ambienti anche nell'eventualità che alcuni dettagli non siano specificatamente previsti.
6. L' Appaltatore si obbliga a prendere visione delle aree cimiteriali interne ed esterne, nello stato di fatto in cui si trovano al momento della consegna degli stessi, si impegna a garantirne la manutenzione e a riconsegnarle al termine dell'appalto in perfette condizioni di pulizia, manutenzione e funzionalità. Al momento della consegna verrà redatto apposito verbale.
7. Il servizio comprende delle prestazioni compensate a misura (attività di necroforo) e delle prestazioni compensate a corpo (attività di pulizia e di manutenzione ordinaria del cimitero).

ART. 2 – DURATA, VALORE DELL'APPALTO E MODALITÀ DI PAGAMENTO

1. L 'appalto avrà la durata di **anni 2 (DUE) dalla data di sottoscrizione del presente contratto.** E' prevista la possibilità da parte del Committente, prima della scadenza, di richiedere la proroga del servizio, alle medesime condizioni contrattuali, per la durata di ulteriori mesi 12 (dodici), considerata la gestione a corpo delle attività relative al servizio di pulizia e lavori di manutenzione ordinaria, ai sensi dell'art. 106, comma 1, del D.Lgs 50/2016 nelle more delle procedure di individuazione di un nuovo affidatario.
Qualora, per qualsiasi motivo, alla scadenza del contratto il nuovo appaltatore non abbia dato avvio al servizio ovvero non si siano concluse le procedure di gara per il nuovo affidamento, l'aggiudicatario, se richiesto dal Comune, è tenuto a garantire il servizio fino all'insediamento della nuova impresa, alle stesse condizioni dell'appalto cessato.
2. Gli importi corrisposti per l'effettuazione dei servizi indicati in tabella sono i seguenti:

Servizio di pulizia e lavori di manutenzione ordinaria (prestazioni a corpo)			
N.	**TIPO INTERVENTO RICHIESTO**	**PERIODICITA'**	**IMPORTO**
1	risistemazione cippi posti sulle sepolture in campo comune, se sprofondati, anche solo in parte, al di sotto del livello del campo e/o ricostituzione del tumulo	in base alle esigenze - mediamente n. 3 tumuli/anno	€ _____
2	taglio e l'estirpazione delle erbe infestanti, con applicazione ove necessario del diserbante o del pirodiserbo, tenuta aree verdi, vialetti non pavimentati, all'interno del cimitero, eseguito con mezzi meccanici o a mano, compreso il trasporto dei rifiuti alla pubblica discarica. È fatto assoluto divieto di bruciare le erbe e i rifiuti. Tale lavoro va eseguito indicativamente almeno una volta al mese nel periodo da marzo ad ottobre (con particolare riguardo del periodo che precede le Festività di inizio novembre); raccolta di tutto il materiale di risulta con trasporto alla discarica, a cura dell'appaltatore; materiale occorrente al taglio e estirpazione erbe infestanti e di diserbo a carico di appaltatore	da marzo a ottobre almeno una volta al mese	€ _____
3	spargimento di ghiaia nei viali principali, vialetti interni ai riquadri, insabbiatura di tutti i tumuli nei campi comuni (ghiaia a carico dell'appaltatore)	1 volta l'anno compresa ghiaia	€ _____
4	rimozione delle cartacce e degli altri rifiuti abbandonati su tutto il territorio del cimitero, compreso lo svuotamento dei cestini porta rifiuti posti all'interno ed all'esterno dell'area cimiteriale compreso lo smaltimento delle corone di fiori poste in occasione dei funerali, il conferimento dei rifiuti alla pubblica discarica e compresa la fornitura dei sacchi neri in plastica per il contenimento dei rifiuti stessi; tale lavoro andrà eseguito almeno due volte alla settimana	1,5 ora al giorno 2 volte la settimana per tutto l'anno (per 156 ore)	€ _____
5	spalatura della neve sui vialetti interni eseguita a mano e/o spargimento di sabbia granita e sale in occasione di gelate, mediamente tre volte all'anno (materiali ed attrezzature occorrenti a carico dell'appaltatore)	3 volte l'anno compresa sabbia granita e sale	€ _____
6	pulizia dei locali di servizio, compresi quelli destinati ad uso del personale addetto ai lavori e a magazzino; pulizia bisettimanale dei servizi igienici destinati ai visitatori (materiali di pulizia a carico dell'appaltatore)	h. 0,5 al giorno per 1 volta la settimana (per 26 ore annue)	€ _____
	Totale manutenzioni A CORPO (€/ANNO)		**€ _____**

SERVIZIO NECROFORICO (TUMULAZIONI, INUMAZIONI, ESUMAZIONI, ECC.) (PRESTAZIONI A MISURA)*		
N.	**TIPO INTERVENTO**	**IMPORTO**
1	Inumazioni adulti	€ _____
2	Inumazioni bambini	€ _____
3	Esumazioni adulti manuale	€ _____
4	Esumazioni adulti con mezzo meccanico	€ _____
5	Esumazioni bambini manuale	€ _____
4	Esumazioni bambini con mezzo meccanico	€ _____
5	Tumulazioni in loculo mediante chiusura frontale	€ _____
6	Tumulazioni in loculo mediante chiusura laterale	€ _____
7	Tumulazione in cripta	€ _____
8	Tumulazione in cellette ossario/cinerarie (chiusura di celletta ossario)	€ _____
9	Estumulazioni da loculo con chiusura frontale	€ _____
10	Estumulazioni da loculo con chiusura laterale	€ _____
11	Estumulazione da cripta	€ _____
12	Estumulazioni da celletta ossario/cineraria	€ _____
13	Riapertura loculi di testa per collocazione urna ceneri	€ _____
14	Riapertura loculi laterali per collocazione urna ceneri	€ _____
15	Riapertura cripta per collocazione urna ceneri	€ _____
15	Riapertura cellette per collocazione urna ceneri	€ _____
16	Conferimento ceneri nel cinerario comune con apertura e chiusura del chiusino	€ _____
17	Conferimento ceneri nel cinerario in concessione con apertura e chiusura del chiusino	€ _____
18	Dispersione ceneri nell'area individuata all'interno del cimitero	€ _____
*I servizi necroforici dovranno essere garantiti dal lunedì al sabato compreso e in caso di necessità anche nei giorni festivi, previo avviso dell'ufficio competente		

3. Rispetto al solo servizio necroforico, qualora questo, durante il periodo contrattuale, risultasse inferiore ai quantitativi preventivati, l'appaltatore non potrà richiedere la corresponsione di indennizzi o compensi di sorta; nell'eventualità invece che i quantitativi medesimi venissero superati, dovrà applicare, anche per le eventuali eccedenze, gli stessi prezzi previsti all'esito della gara ed indicati in capitolato. I prezzi indicati in sede di offerta resteranno invariati per tutta la durata del contratto nonché per l'eventuale sua proroga.
L'affidatario dovrà pertanto garantire sia lo svolgimento di tutti i servizi oggetto dell'appalto sia l'applicazione dell'elenco prezzi, così come determinato in fase di aggiudicazione, anche nel caso di modifica delle quantità. Le operazioni da eseguirsi verranno retribuite applicando i prezzi offerti in sede di offerta. L'affidatario, altresì, dovrà essere disponibile a garantire il servizio ai medesimi prezzi e condizioni, qualora si rendesse necessario, anche per eventuali nuovi ampliamenti dell'impianto cimiteriale, al momento non prevedibili.
Gli importi a base della procedura di affidamento sopra indicati sono al netto di IVA e, per il servizio necroforico sono unitari, mentre per il servizio di pulizia e manutenzione ordinaria sono canoni annuali.
4. Ai soli fini dell'art. 35 comma 4 del D.Lgs. 50/2016, il valore stimato dell'appalto, comprensivo delle eventuali proroghe succitate, non supererà la soglia comunitaria prevista all'art. 35 comma 1 lettera c) dello stesso codice.

ART. 3 – ONERI PER LA SICUREZZA

1. Sono a totale carico dell'aggiudicatario gli oneri per la sicurezza sostenuti per l'adozione delle misure necessarie per eliminare o ridurre al minimo i rischi specifici afferenti l'attività svolta.
2. L'affidatario, entro 30 giorni dall'aggiudicazione, deve predisporre e consegnare al Comune, un piano operativo di sicurezza per quanto attiene alle proprie scelte autonome e relative responsabilità nell'organizzazione del cantiere e nell'esecuzione dei lavori. Il piano operativo di sicurezza comprende il documento di valutazione dei rischi e contiene inoltre le notizie riferite allo specifico cantiere e deve essere aggiornato ad ogni mutamento delle lavorazioni rispetto alle previsioni.

3. Non si prevedono interferenze tra il personale del Committente e quello della ditta appaltatrice ma al fine di considerare i possibili rischi interferenziali con soggetti presenti nell'area cimiteriale si redige il DUVRI previsto dall'Articolo 26 del D.Lgs. 81/08 e s.m.i. sebbene non si individuano costi per le misure di prevenzione e protezione, consistenti in modalità organizzative, e di conseguenza nessun onere a carico del Committente per i costi supplementari per la sicurezza.

ART. 4 – OPERAZIONI CIMITERIALI

1. La ditta appaltatrice dovrà provvedere all'esecuzione delle prestazioni di seguito elencate nel presente articolo alle condizioni contrattuali indicate nel precedente art. 2. Il servizio di tumulazione/inumazione dovrà essere garantito dal lunedì al sabato compreso e in caso di necessità anche nei giorni festivi, previo avviso dell'ufficio competente

2. **I servizi cimiteriali necroforici** consistono, a titolo esemplificativo e non esaustivo, nelle seguenti attività a carico dell'affidatario:

A) INUMAZIONI: delle salme a sterro, in campo comune e nelle aree ventennali, in tomba di famiglia, mediante: protezione delle tombe circostanti per evitare imbrattamenti, escavazione (a mano e/o con mezzi meccanici) di fossa delle dimensioni conformi alle norme di polizia mortuaria, segnalazione e protezione dello scavo con apposita attrezzatura in modo tale da rendere l'area decorosa e accessibile in sicurezza ai familiari e agli operatori, eventuale previa foratura, da effettuare nel locale adibito, di eventuali casse contenenti l'involucro in zinco prima di essere posizionate nella fossa, deposizione del feretro sul fondo della scavo, evitando scuotimenti e scosse, chiusura della fossa, formazione e sagomatura del tumulo, collocazione del segnaposto provvisorio recante nome, cognome, data di nascita e data di morte del defunto in assenza di lapide definitiva, trasporto del terreno eccedente in luogo apposito e pulizia dell'area e successiva pulizia dell'area circostante e spandimento di ghiaino nell'area circostante il sito di inumazione dopo la sistemazione definitiva. Lo scavo di norma andrà eseguito con mezzi meccanici - che dovranno essere allontanati prima della funzione funebre - di piccola dimensione per non arrecare danno ai manufatti ed alle fosse già esistenti nel cimitero. Nel caso di impossibilità di eseguire lo scavo con mezzi meccanici, lo stesso dovrà essere eseguito a mano. Le operazioni di inumazione dovranno essere eseguite ad avvenuto allontanamento dei famigliari del defunto, salvo loro esplicita richiesta di presenziare. Preliminarmente alle operazioni di scavo dovrà procedersi con il tracciamento della fossa secondo le previsioni del Piano regolatore Cimiteriale ed in ogni caso secondo le indicazioni dettate dall'Amministrazione comunale.

B) ESUMAZIONI: comprensive di esumazioni ordinarie per completamento del ciclo di rotazione – da campi comuni e posti ventennali - e straordinarie ordinate dall'Autorità Giudiziaria ovvero autorizzate dal Sindaco o responsabile competente. Le esumazioni ordinarie da effettuarsi ai sensi del vigente regolamento di Polizia mortuaria sono disposte dal Comune che provvederà a renderne noti al pubblico modalità e tempi, previa affissione di apposito manifesto nelle bacheche cimiteriali.

Le esumazioni dovranno comprendere:

- recinzione dell'area interessata con pannelli e/o reti che non consentano la visibilità dell'operazione cimiteriale (salvo eventuale accesso in sicurezza dei parenti). La recinzione deve essere decorosa, a tenuta di vento e a norma di sicurezza per utenti e operatori;
- protezione delle tombe circostanti per evitare imbrattamenti e sistemazione del bordo fossa per consentire lo svolgimento in sicurezza delle operazioni di esumazione svolte all'interno della fossa stessa;
- escavazione della fossa fino alla cassa, pulizia del coperchio e apertura dello stesso (eccetto i casi di esumazione per traslazione a bara chiusa);
- raccolta resti conformemente al loro stato ed alla successiva destinazione (eccetto i casi di esumazione per traslazione a bara chiusa);

A terminare

- chiusura e riempimento immediato della fossa, con terra di risulta dello scavo;
- trasporto della terra eccedente nell'area cimiteriale di stoccaggio;
- trasporto dei materiali di risulta nel corrispondente cassone (per legno o marmo) presso il Cimitero
- pulizia della zona circostante l'escavazione.

Poi, a seconda dello stato dei resti e della destinazione, si procederà così:

B.1) esumazione di resti mortali completamente mineralizzati:

- tutte le operazioni al punto B);

- in caso di recupero dei resti ossei, deposito degli stessi, ove richiesto dai parenti aventi titolo, in apposita idonea cassetta fornita dai medesimi parenti, con sigillatura del coperchio ed apposizione salda di targhetta riportante cognome, nome, data di nascita e di morte;
- in caso di eventuale trasporto della cassetta ad altro spazio del cimitero comunale provvederà la ditta con propri mezzi, oppure in caso di trasporto in altro comune, consegna della casetta all'agenzia di onoranze funebri incaricata del trasporto dai parenti aventi titolo;
- se non diversamente disposto dai parenti aventi titolo, è compresa la raccolta dei resti ossei e loro collocazione nell'ossario comune in modo indistinto provvedendo, al termine dell'operazione, alla pulizia e disinfezione della zona circostante all'ossario comune.

B.2) esumazione di resti mortali non completamente mineralizzati e destinati all'inumazione in campo:
- tutte le operazioni al punto B);
- raccolta dei resti mortali non completamente mineralizzati e, qualora non sia possibile recuperare il feretro esistente, collocazione dei medesimi in nuovo feretro o in contenitore di materiale biodegradabile a cura e spese dell'aggiudicatario; qualora il servizio sia richiesto da privati, il feretro e/o il contenitore di materiale biodegradabile per l'inumazione, se necessario, è fornito a cura e spese del richiedente;
- procedere come indicato per le inumazioni nel medesimo luogo;

B.3) esumazione di resti mortali non completamente mineralizzati e destinati alla cremazione:
- tutte le operazioni al punto B);
- sistemazione dei resti mortali non mineralizzati in apposito idoneo contenitore se non fornito dalla ditta di onoranze funebri, e consegna del contenitore con i resti mortali all'agenzia di onoranze funebri incaricata dai parenti aventi titolo per il trasporto al crematorio.

C) TUMULAZIONI: in loculi, cellette ossario e cinerarie comunali, dati in concessione, in tombe di famiglia.
C.1) Tumulazione in loculo di tipo tradizionale;
C.2) Tumulazioni in loculo e realizzazione di tramezzo divisorio/tumulazione in loculo laterale;
C.3) tumulazioni in loculi ossario;
Per tumulazione di feretri, si intende:

C.1) Tumulazione in loculo di tipo tradizionale;
- protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori se necessari;
- inserimento del feretro nel loculo;
- chiusura immediata del loculo (con lastra prefabbricata in calcestruzzo o mattoni pieni), stuccatura ed intonacatura della chiusura, esclusa la scritta;
- rimozione di eventuali impalcature e pulizia e disinfezione della zona circostante.

C.2) Tumulazioni in loculo e realizzazione di tramezzo divisorio/Tumulazioni in loculo trasversale:
Questa operazione consiste nelle stesse operazioni previste per il punto C.1) con l'unica variante, dopo l'apertura del loculo e prima dell'inserimento del feretro, di realizzare uno o più tramezzi divisori erigendo un muro di mattoni, qualora lo spazio di accoglimento dei feretri non sia separato. Tale fase di lavorazione deve essere realizzata prima dell'arrivo dei parenti per la tumulazione.
Quando la tumulazione è in loculi di tipo laterale si ripetono le stesse operazioni previste per il punto C.1) con l'unica variante che l'ingresso del feretro è sul lato lungo del loculo, invece che sul lato corto.

C.3) Tumulazioni in loculi ossari:
La cassetta o l'urna cineraria possono provenire sia da altre contestuali operazioni cimiteriali collegate oppure no. In quanto applicabile, si effettua quanto previsto al punto C.) ma con riferimento ai loculi ossari.

D) ESTUMULAZIONI: comprendono:
D.1) Estumulazioni di resti mortali completamente mineralizzati;
D.2) Estumulazioni di resti mortali non completamente mineralizzati e destinati all'inumazione per completamento della mineralizzazione.
D.3) Estumulazioni di resti mortali non completamente mineralizzati e destinati alla cremazione.
Quando è possibile sono programmate, comunicandole e pianificandole di volta in volta con il Fornitore. Sono possibili singole estumulazioni legate a situazioni particolari.
Per estumulazione si intende:
- protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori se necessari;
- apertura del loculo;

- spostamento del feretro nel luogo preposto alla sua apertura, presso il Cimitero.
- pulizia del coperchio, apertura del feretro, prosecuzione dell'attività a seconda dello stato dei resti mortali;

A terminare:
- rimozione e trasporto dei materiali di risulta nel corrispondente cassone presso il Cimitero;
- pulizia del loculo vuotato che dovrà anche essere imbiancato a calce e chiusura completa dello stesso con mattoni a secco o comunque con materiale idoneo;
- rimozione di eventuali impalcature o sollevatori precedentemente collocati e pulizia e disinfezione della zona circostante;

Poi, a seconda dello stato dei resti, si procederà così:

D.1) estumulazioni di resti ossei completamente mineralizzati:
- tutte le operazioni al punto D);
- stesse operazioni previste al punto B.1), ad eccezione del suo primo alinea;

D.2) estumulazioni di resti mortali non completamente mineralizzati e destinati all'inumazione per completamento della mineralizzazione:
- tutte le operazioni al punto D;
- stesse operazioni previste al punto B.2) (ad eccezione di primo alinea);

D.3) estumulazione di resti mortali non completamente mineralizzati e destinati alla cremazione:
- tutte le operazioni al punto D);
- stesse operazioni previste dal punto B.3) (ad eccezione di primo alinea);

E) TRASLAZIONE di feretri

Questa attività è fatta per trasferire feretri all'interno del cimitero o in altro cimitero situato anche in altro comune.

Per trasferimento si intende:
- protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori se necessari;
- apertura del loculo o loculo ossario o celletta cineraria o tomba di famiglia e prelevamento del feretro o della cassetta e spostamento con idonei mezzi al luogo di destinazione;
- pulizia del loculo vuotato con spandimento di calce (non necessario in caso di loculo ossario o celletta cineraria);
- chiusura completa del loculo o loculo ossario o celletta cineraria o tomba di famiglia oggetto della traslazione vuotati con mattoni a secco o comunque con materiale idoneo
- pulizia della zona di lavoro circostante al luogo di attività, con materiali e disinfettanti idonei;
- rimozione dei rottami e loro trasporto nel relativo cassone presso il cimitero;
- collocazione del feretro o della cassetta nel loculo o loculo ossario o cappella privata di destinazione e successiva chiusura con le medesime modalità descritte nell'operazione sotto la lettera C1);
- in caso di traslazione in altro comune, consegna del feretro o della cassetta all'agenzia di onoranze funebri incaricata dai parenti aventi titolo;
– pulizia della zona di lavoro circostante l'area di lavoro, con materiali e disinfettanti idonei;

F) APERTURA E CHIUSURA loculi o loculi ossari per inserimenti/ricognizioni, comprende:

F1) Apertura/chiusura loculi per INSERIMENTI:

La cassetta o l'urna cineraria possono provenire sia da altre contestuali operazioni cimiteriali collegate oppure no.
- nell'eventuale loculo di partenza protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori, se necessari;
- eventuale estumulazione della cassetta o urna cineraria da collocare;
- pulizia dell'area liberata, della zona circostante e chiusura completa dello stesso con mattoni a secco o comunque con materiale idoneo;
- nell'eventuale loculo di destinazione protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori, se necessari;
- eventuale spacco del muro del loculo o loculo ossario di destinazione, con inserimento della cassetta o urna cineraria;
- chiusura del loculo o loculo ossario di destinazione con le medesime modalità descritte nell'operazione **sotto la lettera C.1);**
- rimozione dei rottami e loro trasporto nel relativo cassone presso il cimitero;

– pulizia della zona di lavoro circostante al loculo o loculo ossario di destinazione, con materiali e disinfettanti idonei;

F2) apertura/chiusura loculi per RICOGNIZIONI:

L'apertura e chiusura di loculi o di loculi ossari per ricognizione è fatta quando sia necessario valutarne la capienza rimanente o, in generale, quando sia necessaria una ricognizione. Si intende:

- protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori se necessari;
- apertura del loculo;
- valutazione della capienza o altro tipo di valutazione;
- chiusura del loculo o loculo ossario con le medesime modalità descritte nell'operazione sotto la lettera **C1**);
- rimozione dei rottami e loro trasporto nel relativo cassone presso il cimitero;

– pulizia della zona di lavoro circostante al loculo o loculo ossario di destinazione, con materiali e disinfettanti idonei;

G) COLLOCAZIONE NELL'OSSARIO/CINERARIO COMUNE DI RESTI/CENERI:

Estumulazione resti da loculo ossario/cinerario e collocazione nell'ossario/cinerario comune in modo indistinto provvedendo, al termine dell'operazione, alla pulizia e disinfezione della zona circostante all'ossario comune.

Le collocazioni nell'ossario/cinerario comune conseguenti ad operazioni cimiteriali sono comprese nelle operazioni cimiteriali stesse.

H) DISPERSIONE DELLE CENERI NEGLI SPAZI RISERVATI ALL'INTERNO DEL CIMITERO

a) trasporto dell'urna dall'ingresso del cimitero o dal luogo di sosta nel cimitero all'apposito spazio riservato;
b) svuotamento delle ceneri nell'apposito spazio riservato;
c) riconsegna dell'urna ai privati o smaltimento dell'urna;
d) posa della targa (fornita dai famigliari del defunto) contenente i dati del defunto negli appositi spazi; la posa di tale targhetta è a carico dell'affidatario anche per i defunti, residenti nel Comune di Frossasco al momento del decesso, le cui ceneri siano state affidate o disperse nel territorio del Comune ma al di fuori del cimitero, ovvero in altri comuni;
e) eventuale pulizia della zona circostante.

I) INTERVENTI DI RIPRISTINO DELLA USABILITÀ DEL MANUFATTO

La presente operazione è prevista in casi straordinari quali percolazioni, cedimenti della bara con fuoriuscita di liquidi organici, ecc...

- protezione lapidi circostanti per evitare imbrattamenti ed erezione di eventuali impalcature o posizionamento di sollevatori se necessari;
- apertura del loculo;
- estrazione del feretro, sigillatura del feretro con materiali idonei forniti dalla ditta e temporanea collocazione in apposito locale di sosta.
- pulizia e disinfezione del pavimento e delle pareti del loculo con detergenti idonei e a norma.
- sistemazione del feretro in apposito idoneo contenitore e ritumulazione dello stesso;
- chiusura del loculo con le medesime modalità descritte nell'operazione sotto la lettera **C1**);
- rimozione dei rottami e loro trasporto nel relativo cassone presso il cimitero;

– pulizia della zona di lavoro circostante al loculo o loculo ossario di destinazione, con materiali e disinfettanti idonei;

3. L'appaltatore dovrà effettuare le operazioni inerenti o correlate a movimenti di salme, di resti e di ceneri, disposte dal/la concessionario/a nelle cappelle private, solamente a seguito di preventiva autorizzazione del Comune, ovvero disposte dall'autorità sanitaria, con applicazione delle tariffe comunali e secondo le modalità previste del presente capitolato.

4. L'appaltatore dovrà altresì:

- riportare i servizi svolti di cui al presente comma, relativi alle lett. da A ad I all'interno di "SCHEDE TRIMESTRALI OPERAZIONI CIMITERIALI SVOLTE" riassuntive degli interventi svolti da consegnarsi all'ufficio anagrafe del Comune al termine di ogni trimestre in concomitanza dell'invio della fattura;
- segnalare, tramite apposizione di cartello, ai proprietari di lapidi e monumentini posti sulle sepolture in campi di inumazione, dell'eventuale necessità di sistemazione di tali manufatti e fornire contestuale informazione alla Stazione Appaltante;
- ritirare la documentazione amministrativa per ogni ingresso o uscita al/dal cimitero con la consegna della medesima presso l'Area anagrafica dell'ente entro il giorno successivo;

- provvedere regolarmente al ritiro dei documenti di trasporto funebre da trasmettere agli uffici comunali e alla tenuta dei registri cimiteriali, con le modalità che saranno comunicate dall'Ufficio Anagrafe del Comune di Frossasco;
- garantire il rispetto di tutte le normative igienico sanitarie con particolare riferimento al regolamento di polizia mortuaria vigenti;
- rispettare le norme vigenti per la prevenzione degli infortuni sul lavoro di cui al D.lgs. 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" e s.m.i..

5. Le **prestazioni inerenti alla manutenzione ed alla pulizia ordinaria del cimitero (servizio a corpo) includono:**
- risistemazione cippi posti sulle sepolture in campo comune, se sprofondati, anche solo in parte, al di sotto del livello del campo e/o ricostituzione del tumulo;
- taglio e l'estirpazione delle erbe infestanti, con applicazione ove necessario del diserbante, tenuta aree verdi, vialetti non pavimentati, all'interno del cimitero, eseguito con mezzi meccanici o a mano, compreso il trasporto dei rifiuti alla pubblica discarica. E' fatto assoluto divieto di bruciare le erbe e i rifiuti. Tale lavoro va eseguito indicativamente almeno una volta al mese nel periodo da marzo ad ottobre (con particolare riguardo del periodo che precede le Festività di inizio novembre) e raccolta di tutto il materiale di risulta dei lavori di cui ai punti a-b-c-d-e-f-g-h-i del comma 2, con trasporto alla discarica a cura dell'appaltatore;
- spargimento di ghiaia nei viali principali, vialetti interni ai riquadri, insabbiatura di tutti i tumuli nei campi comuni;
- rimozione delle cartacce e degli altri rifiuti abbandonati su tutto il territorio del cimitero, compreso lo svuotamento dei cestini porta rifiuti posti all'interno ed all'esterno dell'area cimiteriale compreso lo smaltimento delle corone di fiori ammalorati poste in occasione dei funerali, il conferimento dei rifiuti alla pubblica discarica e compresa la fornitura dei sacchi neri in plastica per il contenimento dei rifiuti stessi; tale lavoro andrà eseguito almeno due volte alla settimana;
- spalatura della neve sui vialetti interni eseguita a mano e/o spargimento di sabbia granita e sale in occasione di gelate, mediamente tre volte all'anno (compresi materiali ed attrezzature occorrenti);
- pulizia dei locali di servizio, compresi quelli destinati ad uso del personale addetto ai lavori e a magazzino; pulizia bisettimanale dei servizi igienici destinati ai visitatori;
- raccolta di tutto il materiale di risulta con trasporto alla discarica, a cura dell'appaltatore;
- messa a disposizione degli utenti di idonee attrezzature di proprietà comunale (secchi, scope, annaffiatoi) per la pulizia e il mantenimento delle tombe e loculi;
- prestare l'osservanza dell'orario di apertura e chiusura, che in attualmente, fatte salve eventuali successive modifiche il seguente:

a) periodo invernale: (dal 01 novembre al 31 marzo): tutti i giorni dalle ore 8.00 alle ore 17:00;
b) periodo estivo: (dal 01 aprile al 31 ottobre): tutti i giorni dalle ore 8.00 alle ore 19.00;

- avvertire tempestivamente l'Area tecnica tecnico manutentiva del Comune di Frossasco in caso di rottura dell'impianto di chiusura automatica del cancello di ingresso;
- garantire il rispetto di tutte le normative igienico sanitarie con particolare riferimento al regolamento di polizia mortuaria vigenti;
- rispettare le norme vigenti per la prevenzione degli infortuni sul lavoro di cui al D.lgs. 9 aprile 2008 , n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro" e s.m.i..

6**.** La spesa per eventuali prestazioni connesse alle operazioni di sepoltura, manutenzione e pulizia previste nei regolamenti in vigore e non contemplate espressamente nel presente capitolato, devono intendersi incluse nel prezzo pattuito delle singole operazioni.

ART. 5 – TEMPI E MODALITA' DI ESECUZIONE DEL SERVIZIO NECROFORICO, DI PULIZIA E DI MANUTENZIONE ORDINARIA DEL CIMITERO COMUNALE

1. I servizi necroforici, di pulizia e di manutenzione ordinaria del cimitero comunale, intesi nella loro globalità, devono essere espletati con la maggior accuratezza e diligenza in conformità agli orari prestabiliti dal Committente.
2. Il personale dell'Affidatario dovrà attendere l'effettivo arrivo dei cadaveri e/o dei parenti, senza alcun compenso ulteriore a quanto indicato nell'elenco prezzi per l'effettuazione del servizio. Quindi si dovrà

presentare in anticipo sull'orario indicato sui relativi permessi. L'orario indicato è pertanto da considerarsi indicativo in quanto potranno esservi anticipi e/o ritardi per problemi di traffico, delle pratiche religiose o altro imprevisto. Gli oneri relativi all'attesa si intendono e sono già ricompresi nelle singole voci di elenco sopra indicate. L'anticipo minimo con il quale il personale della ditta deve presentarsi per effettuare le operazioni cimiteriali deve essere congruo in modo da consentire in ogni caso la puntuale esecuzione delle medesime agli orari stabiliti e non creare attesa ai familiari.
3. La ditta affidataria deve, con proprio personale, mezzi e organizzazione garantire lo svolgimento dei funerali programmati dall'Ente comunale anche per più funerali programmati contemporaneamente nello stesso cimitero senza costi supplementari per il committente.
4. Il servizio dovrà essere effettuato praticando la massima disponibilità e collaborazione con il Committente.
5. La ditta appaltatrice deve essere in grado di organizzare ed eseguire in autonomia tutte le operazioni previste nel capitolato.
6. In particolare durante i funerali è fatto divieto nel modo più drastico di utilizzare l'aiuto dei parenti e/o del personale delle agenzie di pompe funebri, anche per il semplice sollevamento della cassa.
7. In caso di abbandono o sospensione ed in genere per ogni inosservanza degli obblighi e delle condizioni del presente capitolato, il Committente potrà sostituirsi all'affidatario per l'esecuzione d'ufficio del servizio, con rivalsa delle spese a carico dell'affidatario e ciò indipendentemente dalle sanzioni a questo applicabili e l'eventuale risarcimento dei danni e salvo quanto disposto in merito dagli altri articoli del presente capitolato. Per l'esecuzione d'ufficio il Committente potrà avvalersi di qualsiasi impresa che non sia l'affidatario, oppure provvedervi direttamente.
8. L'affidatario è tenuto a dare al Comune, di volta in volta, immediata comunicazione telefonica e per posta elettronica di tutti gli incidenti verificatisi nell'esercizio del servizio, qualunque importanza essi rivestano ed anche quando nessun danno si sia verificato.

ART. 5 BIS - INTERVENTI URGENTI

In caso di interventi di particolare urgenza e gravità, si richiede la reperibilità e la disponibilità della ditta ad eseguire I' intervento entro il lasso di tempo di ore 8 (otto) dalla chiamata effettata dal Comune.

ART. 6 – PRESTAZIONI ACCESSORIE

1. Il Comune potrà ordinare all'aggiudicatario i servizi o le forniture sotto riportate ai prezzi medi correnti al momento dell'ordinazione:
- interventi di modesta entità quali, a titolo esemplificativo e non esaustivo, pulizie straordinarie, sistemazione e/o sostituzione di rubinetteria di lieve entità, posa di lapidi, etc.
- pulizia di concessioni revocate o di concessioni soggette a procedura di revoca.
2. Qualora, nello svolgimento dei servizi oggetto del presente capitolato, l'aggiudicatario dovesse ravvisare situazioni di pericolo che possono arrecare danno ai visitatori o alle strutture del cimitero, lo stesso è tenuto a darne tempestiva comunicazione al settore lavori pubblici ed all'area tecnica tecnico-manutentiva del Comune nonché a mettere in sicurezza l'area, delimitandola in modo idoneo (ad esempio con transenne o nastri di segnalazione).

ART. 7 – ATTREZZATURE E MACCHINARI

1. La scelta delle attrezzature e delle macchine da utilizzare deve essere fatta dall'aggiudicatario tenendo in debita considerazione la compatibilità delle stesse in rapporto alla struttura del cimitero cittadino. In particolare, le attrezzature devono essere tecnicamente efficienti, dotate di tutte le caratteristiche, conformità e gli accessori necessari a proteggere e salvaguardare l'operatore e i terzi da eventuali infortuni, secondo quanto prescritto dalle normative vigenti in Italia e nella Comunità Europea, con l'obbligo di mantenerle nel tempo in perfetto stato di funzionalità.
2. La stazione appaltante mette a disposizione dell'aggiudicatario, se richieste, in comodato d'uso gratuito, a supporto del servizio e nello stato d'uso in cui si trovano, le seguenti attrezzature:
a) n. 1 montaferetri elettrico;
b) n 1 portantina fissa;
c) n. 1 portantina con ruote;

d) n. 2 carriole.
Relativamente al montaferetri elettrico, di cui alla precedente lett. a), le verifiche periodiche volte a valutarne l'effettivo stato di conservazione e di efficienza ai fini della sicurezza, previste dall'art. 71, comma 11, del d.lgs. 81/2008 sono curate dall'area tecnica del Comune di Frossasco. L'affidatario in caso di utilizzo dell'attrezzatura comunale resta ad ogni modo l'unico responsabile del suo corretto utilizzo e si impegna a comunicare immediatamente, per iscritto, all'area tecnica dell'ente ogni informazione ritenuta rilevante ai fini della manutenzione del medesimo.
Rispetto alle attrezzature di cui alle precedenti lett. b), c) e d) tutti gli interventi atti ad assicurare il funzionamento o la riparazione di tali attrezzature fornite in dotazione dal Comune, ove richiesto, nonché la relativa manutenzione ordinaria e straordinaria delle stesse, da effettuarsi secondo le prescrizioni del costruttore, sono ad esclusivo e completo carico dell'aggiudicatario; non sono previste a carico del Comune ulteriori implementazioni o sostituzioni di queste attrezzature, né eventuali adeguamenti richiesti in sede di manutenzione. Pertanto l'aggiudicatario dovrà, a sua cura e spese, assicurare i servizi con propria adeguata attrezzatura aziendale.
Della consegna di tutte le attrezzature indicate nel presente comma, se richieste in utilizzo, sarà predisposto apposito verbale di consegna da parte dell'area tecnica dell'ente.
3. Il Comune concede inoltre all'Impresa affidataria, a titolo gratuito, per il periodo di durata del presente appalto, l'uso di un locale per il deposito del materiale e delle attrezzature da utilizzarsi nell'appalto, nonché la fornitura di energia elettrica ed acqua.
4. L'aggiudicatario ha l'obbligo di mantenere in buono stato di manutenzione e pulizia i locali e le attrezzature di cui sopra, ove richieste, e di riconsegnarli alla scadenza del contratto nello stato in cui li aveva ricevuti, salvo deterioramento d'uso.

ART. 8 – PRODOTTI PER LE PULIZIE, DISINFEZIONE E IGIENE IMPIEGATI NELL'APPALTO

1. Tutti i prodotti di pulizia e sanificazione occorrenti per svolgere il servizio in oggetto ed i prodotti ausiliari in tessuto carta da posizionare presso i servizi igienici (es carta igienica, rotoli o salviette di carta asciugamani), dovranno essere forniti dall'Aggiudicatario, a proprie cura e spese, e dovranno essere idonei al tipo di operazione richiesta dal presente capitolato.
2. In particolare per:
A) Prodotti per le pulizie ordinarie (detergenti multiuso, per finestre e servizi sanitari):
l'Aggiudicatario ha l'obbligo di utilizzare prodotti per l'igiene, detergenti multiuso destinati alla pulizia di ambienti interni, detergenti per finestre e detergenti per servizi sanitari per le pulizie ordinarie conformi alle specifiche tecniche indicate nel D.M. 51 del 29.01.2021, recante i criteri ambientali minimi per l'affidamento del servizio di pulizia e sanificazione di edifici e ambienti ad uso civile, sanitario e per i prodotti detergenti.
I detergenti devono essere usati solo con sistemi di dosaggio o apparecchiature (per esempio, bustine e capsule idrosolubili, flaconi dosatori con vaschette di dosaggio fisse o apparecchi di diluizione automatici) che evitino che la diluizione sia condotta arbitrariamente dagli addetti al servizio
B) Prodotti disinfettanti:
I prodotti disinfettanti utilizzati devono essere conformi al regolamento (CE) n. 528/2012 del Parlamento e del Consiglio del 22 maggio 2012 relativo alla messa a disposizione sul mercato e all'uso dei biocidi, così come modificato dal Regolamento (UE) n. 334/2014 autorizzati:
- dal Ministero della Salute come presidi medico-chirurgici, ai sensi del DPR n. 392/1998; in tal caso devono riportare in etichetta le seguenti diciture: "Presidio medico-chirurgico" e "Registrazione del Ministero della salute n. …...,
- come prodotti biocidi, ai sensi del regolamento (CE) n. 528/2012. In tal caso devono riportare in etichetta le seguenti diciture: "Prodotto biocida" e "Autorizzazione/Registrazione del Ministero della Salute n. …..", oppure devono essere in possesso dell'autorizzazione dell'Unione Europea, prevista ai sensi del capo VIII sezione 1, del citato Regolamento.
C) Fornitura di materiali igienico-sanitari per servizi igienici e/o fornitura di detergenti per l'igiene delle mani:
I prodotti di carta tessuto eventualmente forniti (carta igienica, salviette monouso etc.) devono essere in possesso del marchio di qualità ecologica Ecolabel (UE) o di equivalenti etichette ambientali conformi alla norma tecnica UNI EN ISO 14024.

I saponi eventualmente forniti devono essere liquidi ed in possesso del marchio di qualità ecologica Ecolabel (UE) o di equivalenti etichette ambientali conformi alla norma tecnica UNI EN ISO 14024.
Laddove non siano già impiegati distributori per l'erogazione di saponi per le mani in forma schiumosa, questi, che devono essere in grado di trasformare il prodotto in schiuma senza l'uso di gas propellenti, devono essere forniti. Tali apparecchiature possono essere anche mobili, ovvero non necessariamente da fissare alla parete.

ART. 9 – PERSONALE IMPIEGATO

1. La ditta affidataria deve con proprio personale, mezzi e organizzazione garantire lo svolgimento dei servizi previsti nel presente capitolato.
2. Il personale dovrà essere adeguato per numero e competenze professionali al tipo di lavorazione da eseguire di volta in volta.
3. L'impresa aggiudicataria dovrà assicurare la presenza con immediata e tempestiva sostituzione in caso di assenza per qualsiasi motivo, degli operatori necessari ad eseguire le attività previste ed intervenire.
4. Il personale in servizio dovrà tenere un contegno riguardoso e corretto anche nei confronti dell'utenza e conformarsi alle disposizioni del vigente codice di polizia mortuaria, nonché essere convenientemente abbigliato, in modo omogeneo ed uniforme, con vestiario di servizio e cartellino di riconoscimento, e a norma della vigente legislazione antinfortunistica e igienico-sanitaria.
5. Il personale impiegato dovrà essere formato relativamente agli atteggiamenti da tenere in conseguenza a valenze etiche e sociali dei luoghi nei quali si trova ad operare, svolgendo le proprie mansioni con ordine, serietà e diligenza e operando in modo da non violare le disposizioni normative in vigore.
6. Il personale impiegato è tenuto al segreto d'ufficio su fatti e circostanze di cui venga a conoscenza nell'espletamento dei propri compiti.
7. L'affidatario si impegna a richiamare, e se del caso, sostituire i dipendenti che non osservassero una condotta irreprensibile.
8. Le segnalazioni e le richieste del Comune in tal senso saranno impegnative per l'affidatario. In ogni caso, quindi è in facoltà del Committente richiedere in qualunque momento l'allontanamento immediato del personale che, a suo insindacabile giudizio, non sia idoneo a svolgere le mansioni richieste o tenga un comportamento non idoneo con il luogo di lavoro, compreso il personale tecnico-amministrativo stesso della ditta appaltatrice. La ditta appaltatrice non potrà in ogni caso chiedere indennizzi, sovrapprezzi o richiesta alcuna a qualsiasi titolo nel caso il Committente appaltante richieda l'allontanamento di personale della ditta appaltatrice stessa.
9. Qualora qualche addetto al servizio dovesse risultare non idoneo dal punto di vista sanitario, dovrà essere sospeso o sostituito, a seconda dei casi; il controllo sanitario e l'eventuale allontanamento sono a totale responsabilità ed a carico della ditta appaltatrice.
10. Il vestiario, il materiale di prevenzione infortuni e di tutela igienico-sanitaria per gli operatori è a cura e con costi a carico dell'impresa aggiudicatrice.
11. L'impresa è tenuta a rispettare e a far rispettare al proprio personale impiegato nel presente appalto, in quanto compatibili, gli obblighi di condotta previsti dal codice di comportamento dei pubblici dipendenti, approvato ai sensi del DPR n. 62 del 16/04/2013, e dal codice di comportamento dei dipendenti del Comune di Frossasco, approvato con Deliberazione di G.C. n. 4 del 13/02/2014 e pubblicato sul sito internet comunale, raggiungibile all'URL sul sito istituzionale www.comunefrossasco.it, sezione Amministrazione trasparente, Disposizioni generali, atti generali. La violazione dei suddetti obblighi comporterà per l'Amministrazione la facoltà di risolvere il contratto, qualora, in ragione della natura o della reiterazione della violazione, la stessa sia ritenuta grave.

ART. 10 - ASSUNZIONE DI PERSONALE DELL'IMPRESA CESSANTE

1. Al fine di promuovere la stabilità occupazionale nel rispetto dei principi dell'Unione Europea e ferma restando la necessaria armonizzazione con l'organizzazione dell'operatore economico subentrante e con le esigenze tecnico-organizzative e di manodopera previste nel nuovo contratto, l'aggiudicatario del contratto di appalto è tenuto ad assorbire prioritariamente nel proprio organico il personale già operante alle dipendenze dell'aggiudicatario uscente, come previsto dall'articolo 50 del Codice, garantendo l'applicazione dei CCNL di settore, di cui all'art. 51 del D. Lgs. n. 81/2015.

ART. 11 - RESPONSABILITA'

1. L'aggiudicatario si impegna ad adempiere, con la diligenza richiesta dalla natura delle prestazioni oggetto dell'affidamento, a tutte le obbligazioni derivanti dal presente capitolato speciale.
2. L'aggiudicatario è responsabile per eventuali danni eventualmente arrecati a terzi in dipendenza di colpa o negligenza nell'esecuzione delle prestazioni oggetto del presente capitolato, e pertanto solleva il Comune da qualsiasi responsabilità.
3. Il Comune non si assume alcuna responsabilità per danni, infortuni od altro che dovessero derivare all'aggiudicatario o ai suoi addetti ai lavori nell'esecuzione delle prestazioni oggetto del presente capitolato o per qualsiasi altra causa.
4. L'aggiudicatario si impegna altresì ad ottemperare a tutti gli obblighi verso i propri lavoratori in base alle disposizioni legislative e regolamentari vigenti in materia di lavoro e di assicurazioni sociali assumendo a proprio carico tutti gli oneri relativi.
5. L'aggiudicatario sarà comunque tenuto a risarcire il Comune del danno causato da ogni inadempimento alle obbligazioni derivanti dal presente capitolato.
6. E' fatto obbligo all'aggiudicatario di comunicare tempestivamente al Comune il nominativo del rappresentante legale in carica e ogni eventuale variazione di ragione sociale.

ART. 12 - POLIZZA ASSICURATIVA

1. Tutti gli obblighi assicurativi, antinfortunistici, assistenziali e previdenziali sono a carico dell'affidatario che ne è il solo responsabile, con esclusione del diritto di rivalsa e con manleva nei confronti del Comune.
2. Per la copertura degli eventuali danni di cui all'articolo precedente l'aggiudicatario deve stipulare, prima di prendere servizio, idonea polizza assicurativa R.C., comprensiva della responsabilità civile verso terzi, con riferimento al servizio in questione, con massimale non inferiore a Euro 2.500.000,00 per sinistro, senza limiti al numero di sinistri e al massimale annuo e con validità non inferiore alla durata del servizio.
In caso di presenza di franchigie nel contratto, resta inteso che l'onere di pagamento delle stesse resterà comunque a carico del solo aggiudicatario.
In alternativa alla stipulazione della suddetta polizza l'aggiudicatario potrà dimostrare di possedere una polizza R.C., già attivata, avente le medesime caratteristiche; in tal caso dovrà stipulare un'appendice alla stessa, nella quale si espliciti che la polizza in questione copre anche il servizio svolto per conto del Comune di Frossasco, il quale dovrà essere esplicitamente inserito nel novero dei terzi. Copia di tale polizza, unitamente all'ultima quietanza di pagamento del premio, dovrà essere consegnata prima di prendere servizio, su richiesta dell'amministrazione, al servizio anagrafe del Comune di Frossasco.
La copertura delle predette garanzie assicurative deve coprire tutta la durata del contratto d'appalto.

ART. 13 - OBBLIGHI E RESPONSABILITA' A CARICO DELL'AGGIUDICATARIO

1. L'aggiudicatario si obbliga altresì, prima dell'inizio della gestione, a dichiarare il rispetto degli obblighi assicurativi e previdenziali previsti dalla legge e dai contratti e di aver ottemperato ai requisiti previsti dal D.Lgs. n.81/2008 e s.m.i., nonché a tutta la normativa inerente all'igiene ed alla sicurezza dei luoghi di lavoro.
2. L'aggiudicatario assume l'obbligo di dotare il proprio personale di tutti i macchinari, gli attrezzi manuali, le attrezzature protettive antinfortunistiche, anche ai sensi del D.Lgs. 81/2008 e s.m.i., nonché i prodotti detergenti, i disinfettanti e quanto altro possa servire all'espletamento dei compiti previsti dal presente capitolato.
3. L'aggiudicatario ha l'obbligo di servirsi di macchinari ed attrezzature conformi alle norme nazionali e comunitarie in materia di sicurezza. Deve utilizzare solo macchine ed attrezzature conformi alle prescrizioni antinfortunistiche vigenti in Italia e nell'Unione Europea. Le macchine e gli attrezzi di proprietà dell'aggiudicatario usati all'interno della struttura comunale devono essere contraddistinti con targhette indicanti il nome ed il contrassegno dell'affidatario.
4. L'aggiudicatario è responsabile della custodia sia delle macchine che delle attrezzature.
5. L'aggiudicatario è responsabile nel caso di eventuali danni o furti delle macchine e attrezzature.

6. L'onere e la manutenzione delle attrezzature meccaniche utilizzate, l'acquisto dei materiali protettivi, dei prodotti e materiali di consumo (es. sabbia, ghiaia, terra ecc.) da utilizzare per l'esecuzione degli obblighi derivanti dal presente capitolato speciale di appalto sono ad esclusivo e completo carico dell'aggiudicatario.
7. L'aggiudicatario si obbliga a far utilizzare dal proprio personale prodotti detergenti altamente biodegradabili ed a bassa concentrazione per il lavaggio, prodotti sgrassanti biodegradabili, disinfettanti efficaci, a base di ammoniaca e ipoclorito di sodio, nei casi in cui sono indicati, con divieto d'uso di prodotti infiammabili od erosivi.
8. L'aggiudicatario assume l'onere di eseguire, nel rispetto del D.Lgs. 81/2008 e s.m.i., tutte le opere provvisionali, di difesa e di segnalazione, assicurando in tal modo l'incolumità non solo degli addetti, ma anche dei terzi e della pubblica utenza.
9. Prima dell'inizio dell'attività di servizio, l'aggiudicatario dovrà presentare all'area tecnica tecnico-manutentiva del Comune il piano delle misure per la sicurezza fisica dei lavoratori (nel quale vengono analizzati in maniera dettagliata i processi di costruzione e di esecuzione e le modalità di lavoro con diretto riferimento alla sicurezza dei lavoratori impiegati ed ai dispositivi di protezione individuali dei lavoratori).
10. Le macchine e le attrezzature di proprietà o in disponibilità dell'aggiudicatario eventualmente utilizzate dovranno essere dotate di certificazione CE e/o dichiarazione di conformità al D.Lgs n. 81/2008 e s.m.i..
11. L'aggiudicatario dovrà trasmettere all'area tecnica tecnico-manutentiva del Comune, i seguenti documenti:

- piano operativo e di sicurezza;
- documento di valutazione dei rischi di cui all'art.26 del D.Lgs n.81/2008;
- elenco delle attrezzature utilizzate;
- elenco nominativo del personale che opererà nelle aree cimiteriali con relative mansioni.

12. Nel caso in cui, nel corso dell'affidamento, le attrezzature utilizzate vengano sostituite, l'aggiudicatario dovrà comunicare la sostituzione all'area tecnica tecnico manutentiva dell'ente.

ART. 14 - DISPOSIZIONI RELATIVE AI SUBAPPALTI

1. Il concorrente deve indicare all'atto dell'offerta le parti del servizio che intende subappaltare o concedere in cottimo in conformità a quanto previsto dall'art. 105 del D.Lgs. 50/2016; in mancanza di tali indicazioni il subappalto è vietato.
2. La stazione appaltante provvederà a corrispondere direttamente al/ai subappaltatore/i l'importo dovuto per le prestazioni dal/dagli stesso/i eseguite, nei casi previsti dall'art. 105, comma 13, del D.Lgs. 50/2016.
3. L'indicazione di cui sopra al comma precedente lascia impregiudicata la responsabilità dell'aggiudicatario.
4. Per quanto non meglio specificato nel presente articolo si rimanda alle disposizioni di cui all'art. 105 del D.Lgs. 50/2016.

ART. 15 – PENALITÀ

1. L'aggiudicatario del servizio sarà sottoposto all'applicazione delle seguenti penali, nei casi elencati:
a) per la mancata esecuzione di ciascuna delle operazioni descritte nell'art. 4, comma 2, verrà applicata una penale di € 200,00 (duecento/00);
b) per la mancata esecuzione di ciascuna delle operazioni descritte nell'art. 4, comma 5, verrà applicata una penale di € 200,00 (duecento/00);
c) per la mancata esecuzione delle operazioni di pulizia in occasione della annuale commemorazione dei defunti, verrà applicata una penale di € 1.000,00 (mille/00);
d) per inadempimenti che pregiudichino la funzionalità del servizio la penale ammonta a € 300,00 (trecento/00);
e) per la mancata comunicazione al servizio anagrafe dell'ente dei nominativi del personale impiegato presso la sede cimiteriale e gli eventuali aggiornamenti entro due giorni dal loro verificarsi, con l'indicazione della qualifica professionale con la quale ciascun addetto è stato assunto e la posizione previdenziale ed assicurativa, verrà applicata una penale di € 200,00 (duecento/00);
f) per la mancata comunicazione all'area tecnica tecnico-manutentiva ed al servizio anagrafe del Comune di situazioni di pericolo che possono arrecare danno ai visitatori o alle strutture del cimitero, ravvisate dall'aggiudicatario nello svolgimento dei servizi oggetto del presente capitolato, nonché per la mancata

messa in sicurezza dell'area con transenne entro 24 ore dal verificarsi, verrà applicata una sanzione di € 300, 00 (trecento/00);
g) qualora il personale occupato non sia munito dell'apposita tessera di riconoscimento come previsto all'art. 9 del presente capitolato, verrà applicata una penale di € 100,00 (cento/00);
2. La riscossione delle suddette penali avverrà mediante trattenuta sull'importo mensile fatturato da liquidare.
3. L'infrazione verrà contestata per iscritto all'aggiudicatario dal responsabile dell'area amministrativa del Comune a seguito di relazione del personale comunale preposto o su segnalazione o reclamo di terzi. L'aggiudicatario potrà controdedurre entro il termine di giorni dieci, scaduti i quali il responsabile, ove non accolga le controdeduzioni, procederà ad applicare la penale.

ART. 16 - CLAUSOLE RISOLUTIVE ESPRESSE

1. Ai sensi dell'art. 1456 del c.c. il contratto si intenderà risolto di diritto, salvo in ogni caso il diritto al risarcimento dei danni arrecati al Comune di Frossasco, nei seguenti casi:
a) in caso di scioglimento, liquidazione, fallimento o ammissione a procedure concorsuali in genere dell'aggiudicatario. In tal caso il contratto si intenderà risolto di diritto a far data dall'inizio di dette procedure;
b) mancata assunzione del servizio alla data stabilita;
c) sospensione del servizio per un periodo superiore a ore 24 esclusi i casi di forza maggiore, che comunque dovranno essere riconosciuti dall'Ente;
d) abituali deficienze o negligenze del servizio quando la gravità e le frequenze delle infrazioni, debitamente accertate e contestate, compromettano, a giudizio dell'Ente, il servizio;
e) quando l'aggiudicatario si renda colpevole di frodi o versi in accertato stato di insolvenza;
f) in caso di inosservanza per i propri lavoratori delle leggi sulla prevenzione ed assicurazione degli infortuni sul lavoro e sulla legge di previdenza ed assistenza dei lavoratori;
g) mancata presentazione entro 1 mese dalla data di assunzione del servizio del piano delle misure per la sicurezza all'area tecnica tecnico-manutentiva del Comune, come richiesto dall'art. 19 del presente capitolato;
h) mancata presentazione della polizza assicurativa R.C., di cui all'art. 12 entro 5 giorni dalla data stabilita per l'assunzione del servizio ovvero mancato adeguamento annuale della polizza;
i) mancata sostituzione del personale entro 5 giorni dalla richiesta del Comune, ai sensi dell'articolo 9 del presente capitolato;
l) mancata manutenzione dei mezzi ricevuti in dotazione dal Comune o esecuzione della stessa in difformità dalle prescrizioni del costruttore;
m) quando l'importo complessivo delle penali applicate nel corso dell'appalto superi il 10% dell'importo dell'affidamento;
n) per non aver presentato o adeguato la cauzione definitiva stabilita dall'art. 20 per l'effettuazione del servizio;
o) per subappalto effettuato in difformità alle previsioni di legge;
p) ai sensi dell'art. 3, comma 9 bis, della Legge 13.08.2010 n. 136, costituisce altresì causa di risoluzione del contratto il mancato utilizzo del bonifico bancario o postale ovvero degli altri mezzi idonei a determinare la piena tracciabilità delle operazioni finanziarie, disposto dall'aggiudicatario per approvvigionamenti od altro relativi all'appalto.
In tali casi l'amministrazione comunale provvederà a risolvere il contratto con proprio provvedimento, comunicato tramite raccomandata A.R. o PEC, senza necessità di atti giudiziari e conseguentemente procederà, senza bisogno di messa in mora, all'incameramento del deposito cauzionale definitivo, salva l'azione di risarcimento del maggior danno subito.
2. In caso di risoluzione del contratto, l'aggiudicatario dovrà comunque garantire la gestione dei servizi fino al subentro del nuovo aggiudicatario o all'attuazione di altro sistema gestionale e comunque per un periodo massimo di mesi tre. Nel caso di risoluzione del contratto prima della scadenza naturale dello stesso all'aggiudicatario nulla sarà dovuto per il periodo intercorrente tra la data della risoluzione e quella della scadenza naturale.
3. La decadenza sarà notificata all'aggiudicatario mediante lettera raccomandata con avviso di ricevimento o PEC.

ART. 17 - DIFFIDA AD ADEMPIERE

1. Qualora si verificassero altri tipi di inadempimento contrattuale, o comunque violazioni degli obblighi derivanti dal presente capitolato o degli impegni assunti dall'aggiudicatario in sede di offerta, il Comune di Frossasco, ai sensi dell'art. 1454 c.c., intimerà per iscritto all'aggiudicatario di adempiere entro un congruo termine, con dichiarazione che, decorso inutilmente detto termine, il contratto si intenderà senz'altro risolto.
2. Il Comune si avvarrà in ogni caso della descritta diffida ad adempiere qualora l'aggiudicatario non si adoperi di svolgere il servizio nelle migliori condizioni possibili.
3. In caso di risoluzione la cauzione definitiva di cui al successivo articolo 20 verrà incamerata a titolo di penale e/o di indennizzo, salvo il risarcimento dei maggiori danni.

ART. 18 - ALTRE IPOTESI DI INADEMPIMENTO

1. Resta salva la facoltà del Comune di Frossasco di avvalersi della risoluzione giudiziale del contratto per inadempimento ai sensi dell'art. 1453 del c.c. e degli altri rimedi previsti dalla legge in caso di inadempimento, salvo in ogni caso il risarcimento dei danni.

ART. 19 - RECESSO DAL CONTRATTO

1. Il Comune di Frossasco avrà facoltà di recedere dal contratto in qualsiasi momento per giusta causa con un preavviso di 30 giorni, comunicato con lettera raccomandata A/R o PEC, senza corresponsione all'aggiudicatario d'indennizzo o corrispettivo alcuno per il recesso. In tal caso verranno pagate solamente le prestazioni svolte fino al momento del recesso.
2. La stazione appaltante si riserva altresì di non procedere all'aggiudicazione qualora, nelle more dello svolgimento della procedura di affidamento, Consip S.p.A. attivi una convenzione per un servizio corrispondente a quello oggetto di affidamento ed avente parametri prezzo-qualità più convenienti. In tal caso i concorrenti non hanno diritto a compensi, indennizzi, rimborsi o altro, tenuto conto che, ai sensi dell'art. 1, comma 1, del D.L. 6 luglio 2012, n. 95, convertito con modificazioni nella Legge 7 agosto 2012, n. 135, gli atti e i contratti posti in essere in violazione delle disposizioni sui parametri contenute nell'art. 26, comma 3, della legge 23 dicembre 1999 n. 4888 sono nulli.
3. In applicazione dell'articolo 1, comma 13 del D.L. 95/2012, convertito con modificazioni nella L. 135/2012, la stazione appaltante dopo la stipula del contratto può esercitare, in qualunque momento, il diritto di recesso:
a) quando i parametri delle convenzioni stipulate da Consip S.p.A. dopo la stipula del contratto siano migliorativi rispetto a quelli del contratto stipulato;
b) previa formale comunicazione all'aggiudicatario con un preavviso non inferiore a quindici giorni;
c) rifiuto dell'aggiudicatario ad una modifica delle condizioni contrattuali tale da consentire il rispetto del limite posto dalla convenzione Consip;
d) pagamento delle prestazioni già eseguite oltre ad un decimo delle prestazioni non ancora eseguite.

ART. 20 - GARANZIA DEFINITIVA

1. L'appaltatore per la sottoscrizione del contratto deve costituire, ai sensi dell'articolo 103 del D.Lgs. 50/2016 una garanzia, denominata "garanzia definitiva" a sua scelta sotto forma di cauzione o fideiussione con le modalità di cui all'articolo 93, commi 2 e 3, pari al 10 per cento dell'importo contrattuale. La garanzia deve prevedere espressamente la rinuncia al beneficio della preventiva escussione del debitore principale, la rinuncia all'eccezione di cui all'articolo 1957, secondo comma, del codice civile, nonché l'operatività della garanzia medesima entro quindici giorni, a semplice richiesta scritta della stazione appaltante.
2. Il Comune ha il diritto di valersi della cauzione, nei limiti dell'importo massimo garantito, per l'eventuale maggiore spesa sostenuta per il completamento dei lavori, servizi o forniture nel caso di risoluzione del contratto disposta in danno dell'esecutore e ha il diritto di valersi della cauzione per provvedere al pagamento di quanto dovuto dall'esecutore per le inadempienze derivanti dalla inosservanza di norme e prescrizioni dei contratti collettivi, delle leggi e dei regolamenti sulla tutela, protezione, assicurazione, assistenza e sicurezza fisica dei lavoratori comunque presenti in cantiere o nei luoghi dove viene prestato il servizio nei casi di appalti di servizi; l'incameramento della garanzia avviene con atto unilaterale del Comune senza necessità di

dichiarazione giudiziale, fermo restando il diritto dell'affidatario di proporre azione innanzi l'autorità giudiziaria ordinaria.
La garanzia fideiussoria è tempestivamente reintegrata nella misura originaria qualora, in corso d'opera, sia stata incamerata, parzialmente o totalmente, dal Comune.
3. La garanzia cessa di avere effetto ed è svincolata automaticamente allo spirare del terzo mese successivo alla scadenza del contratto di appalto.

ART. 21 – COMUNICAZIONI

1. Le comunicazioni tra i Responsabili dell'Amministrazione aggiudicatrice e l'Appaltatore e dei collaboratori della Amministrazione aggiudicatrice, potranno essere fatte verbalmente e per iscritto a mezzo lettera, posta elettronica o pec.
2. Le comunicazioni riguardanti l'interpretazione del contratto di appalto, le modalità di svolgimento delle prestazioni, le comunicazioni delle visite ispettive con preavviso, le penali e le contestazioni, dovranno in ogni caso, essere fatte per iscritto e trasmesse a mezzo lettera raccomandata o pec.
Le comunicazioni dovranno avvenire per iscritto anche negli altri casi espressamente previsti dal Capitolato.
3. Eventuali contestazioni che l'Appaltatore intendesse avanzare su una comunicazione ricevuta dovranno essere presentate alla Amministrazione aggiudicatrice entro 3 (tre) giorni lavorativi dalla data di ricevimento della comunicazione; scaduto il suddetto termine, la comunicazione è da intendersi accettata integralmente senza alcuna eccezione.
Tutte le comunicazioni scritte tra le parti dovranno esser verranno inviate o a mezzo raccomandata A/R alle sedi legali delle stesse ovvero a mezzo PEC rispettivamente:

- per l'appaltatore all'indirizzo PEC: _____;
- per il Comune all'indirizzo PEC: comune.frossasco.to@legalmail.it.

ART. 22 - RESPONSABILE DEL PROCEDIMENTO E DIRETTORE DEL SERVIZIO

1. Il Responsabile unico del procedimento nonché Direttore del servizio è individuato nel Responsabile del Servizio Amministrativo, che potrà avvalersi dei propri collaboratori per quanto attiene alle richieste di intervento, diffide, comunicazioni in genere ed a cui spettano pertanto le seguenti competenze:
• seguire l'esecuzione del servizio, verificando il rispetto delle condizioni contrattuali;
• evidenziare e verbalizzare le disfunzioni, i ritardi e le altre eventuali inadempienze al fine dell'applicazione delle penali;
• esprimere il parere di congruità tecnico-economica sulle fatture emesse dall'Appaltatore per il pagamento delle prestazioni;
• istruire gli atti e i diversi provvedimenti amministrativi derivanti dall'esecuzione del contratto.
2. In materia di esecuzione del contratto si fa rinvio alla generale disciplina di cui all'art. 30 del D.Lgs. 50/2016.

Art. 23 CONTROLLI

1. Nel corso del contratto l'Amministrazione aggiudicatrice può disporre, in qualsiasi momento, tramite i suoi funzionari ispezioni e controlli, senza obbligo di preavviso, finalizzati alla verifica dei corretti adempimenti contrattuali da parte dell'Appaltatore.
2. Si rinvia alla disciplina generale in materia di attività di verifica richiamata dagli artt. 102 e 111 del D. lgs. n. 50/2016 s.m.i.
3. In sede di liquidazione finale del servizio, l'onere da porre a carico dell'Appaltatore è determinato anche in relazione alla maggiore spesa sostenuta per affidare ad altra impresa il servizio ove la stazione appaltante non si possa avvalere della facoltà prevista dall'articolo 110, comma 1 del Codice.

ART. 24 - CORRISPETTIVO E PAGAMENTI

1. Il corrispettivo per le prestazioni di cui al presente capitolato consiste nell'importo di aggiudicazione del servizio.
2. Per quanto attiene alle prestazioni a misura (servizio necroforico), queste saranno riconosciute e liquidate

con riferimento al numero di prestazioni effettivamente svolte ed al costo unitario risultante dall'elenco prezzi riportato nel presente capitolato. L'importo derivante dalle prestazioni a misura verrà liquidato in rate trimestrali posticipate.
3. Relativamente al servizio di pulizia e lavori di manutenzione ordinaria (compensate a corpo) il canone d'appalto annuo verrà liquidato in rate trimestrali ed al costo unitario risultante dall'elenco prezzi riportato nel presente capitolato comprensivo del ribasso percentuale offerto in sede di presentazione dell'offerta. Con tale corrispettivo l'appaltatore s'intende compensato di qualsiasi suo avere per il servizio di cui trattasi o ad esso connesso o conseguente, senza alcun diritto a pretendere dal Comune nuovi o maggiori compensi.
4. Nella fattura dovranno essere differenziati i servizi di cui al comma 2 dell'art. 4 pagati a misura, in base alle prestazioni effettivamente eseguite, i servizi di cui al comma 5 dell'art. 4, pagati a corpo, e gli eventuali interventi urgenti e le prestazioni accessorie di cui agli artt. 5 e 6.
5. In ogni caso sull'importo netto progressivo delle prestazioni è operata una ritenuta dello 0,50 per cento; le ritenute possono essere svincolate soltanto in sede di liquidazione finale, dopo l'approvazione da parte della stazione appaltante del certificato di collaudo o di verifica di conformità, previo rilascio del documento unico di regolarità contributiva.
6. Le fatture, in formato elettronico, inviate attraverso il Sistema nazionale d'Interscambio (SdI) saranno liquidate entro e non oltre 30 (trenta) giorni dalla loro presentazione, a seguito dell'emissione del provvedimento di liquidazione da parte del Responsabile dell'area amministrativa, previa verifica di conformità del servizio e previa acquisizione di D.U.R.C. in corso di validità, ai sensi del D.M. 24/10/2007, attestante la regolarità contributiva della ditta e che sarà acquisito dall'Amministrazione, ex art. 16 bis comma 10 della L. 28.1. 2009 n. 2.
7. L'IVA è soggetta a scissione dei pagamenti da versare direttamente all'Erario ai sensi dell'art. 17 ter del D.P.R. n. 633/1972 ss.mm.ii. (cd. Split payment). Le fatture emesse dovranno pertanto indicare la frase "scissione dei pagamenti". I pagamenti avverranno sul conto dell'Appaltatore.
8. Ai sensi dell'articolo 25 del D.L. n. 66/2014, convertito con legge n. 89/2014, nelle fatture dovrà essere indicato, pena l'impossibilità di procedere al pagamento delle medesime, il CIG (Codice identificativo di gara) Z88347BE09.
9. Ai fini della fatturazione elettronica il codice IPA è: UFRO68.
10. Per quanto non previsto dalla presente disposizione si fa rinvio alla disciplina stabilita dall'art. 102 del D.lgs. n. 50/2016 s.m.i. in tema di verifica di conformità del servizio reso.
11. Qualora il pagamento della prestazione non sia effettuato per causa imputabile all'amministrazione entro il termine di cui sopra, resta fermo quanto previsto dal D.lgs. n. 231/2002 e s.m.i..
12. Sono a totale carico della Ditta appaltatrice ogni spesa ed oneri fiscali per bolli e registrazione del contratto, comprese imposte e tasse se ed in quanto dovute, senza diritto di rivalsa. Resta ad esclusivo carico di questo Comune l' I.V.A.
13. Non è ammessa la revisione del prezzo del servizio nel corso della validità del contratto, ai sensi dell'art. 106 del D.lgs. 50/2016 e s.m.i.
14. L'aggiudicatario non potrà pretendere, per nessun titolo, interessi o rivalutazioni o quant'altro sulle somme da corrispondere
15. Eventuali controlli e verifiche sull'applicazione di quanto disposto dalle normative vigenti potranno essere eseguiti in qualsiasi momento dagli incaricati comunali

ART. 25 - TRACCIABILITA' DEI FLUSSI FINANZIARI

1. Ai fini di cui alla legge 136/2010 e s.m.i., riguardante la tracciabilità dei flussi finanziari l'aggiudicatario è tenuto:
a) ad utilizzare uno o più conti correnti bancari o postali, accesi presso banche o presso la società Poste Italiane S.p.A., dedicati alle commesse pubbliche per i movimenti finanziari relativi alla gestione del presente affidamento;
b) a comunicare alla stazione appaltante gli estremi identificativi dei conti correnti di cui al punto precedente, nonché le generalità e il codice fiscale delle persone delegate ad operare su di essi, entro sette giorni dalla loro accensione;
c) a prevedere nei contratti che saranno sottoscritti con imprese a qualsiasi titolo interessate a servizi/forniture oggetto del presente affidamento, quali ad esempio subappaltatori, la clausola con la quale

ciascuna di esse assume gli obblighi di tracciabilità dei flussi finanziari di cui alla citata legge, a pena di nullità assoluta dei contratti stessi;
d) se ha notizia dell'inadempimento agli obblighi di tracciabilità finanziaria da parte dei soggetti di cui alla precedente lettera c), a risolvere immediatamente il rapporto contrattuale con la controparte, informando contestualmente sia la stazione appaltante che la prefettura-ufficio territoriale del governo territorialmente competente.

ART. 26 - FORO COMPETENTE

1. Ogni e qualsiasi controversia che dovesse insorgere tra le parti, anche in corso d'opera, in ordine all'interpretazione, esecuzione, risoluzione del presente capitolato nonché in ordine ai rapporti da esso derivanti e che non si sia potuta risolvere in via amministrativa, sarà rimessa alla competenza del Foro di Torino, ai sensi dell'art. 20 del codice di procedura civile, con esclusione del ricorso al giudizio arbitrale.

ART. 27 - SPESE CONTRATTUALI

1. Sono ad esclusivo carico dell'aggiudicatario tutte indistintamente le spese contrattuali di bollo, registrazione e diritti di segreteria, nonché eventuali spese conseguenti a tutte le tasse ed imposte presenti e future inerenti ed emergenti dal servizio, a meno che sia diversamente disposto da espresse norme legislative.

ART. 28 - OSSERVANZA DI NORME E DISPOSIZIONI

1. Per quanto non previsto nel presente capitolato si fa espresso riferimento, in quanto applicabili, a tutte le disposizioni di legge e di regolamenti vigenti in materia.
2. Particolare osservanza dovrà essere riservata alle norme contenute nel/nella:
- regolamento comunale di polizia mortuaria, approvato con delibera del Consiglio comunale n. 31 del 16/10/2018, esecutiva ai sensi di legge;
- regio decreto 27 luglio 1934, n. 1265 "Testo unico delle leggi sanitarie",
- DPR 285/90 "Regolamento Nazionale di Polizia Mortuaria" e s.m.i.;
- legge marzo 2001, n. 130 "Disposizioni in materia di cremazione e dispersione delle ceneri";
- circolare del Ministero della Sanità n. 24 del 24/6/1993;
- circolare del Ministero della Salute, prot. 818 del 11.01.2021 – DGPRE-MDS-P e smi;
- legge regionale n. 20 del 31/10/2007 "Disposizioni in materia di cremazione, conservazione, affidamento e dispersione delle ceneri",
- legge regionale n. 15 del 3/08/2011 e smi "Disciplina delle attività e dei servizi necroscopici, funebri e cimiteriali. Modifiche della legge regionale del 31 ottobre 2007, n. 20" (Disposizioni in materia di cremazione, conservazione, affidamento e dispersione delle ceneri),
- regolamento 8 agosto 2012 n. 7/R, Regolamento in materia di attività funebre e di servizi necroscopici e cimiteriali, in attuazione dell'articolo 15 della legge regionale 3 agosto 2011, n. 15 (Disciplina delle attività e dei servizi necroscopici, funebri e cimiteriali)
- regolamento n. 10/R del 07 novembre 2013 "Ulteriori modifiche degli articoli 2, 3 e 11 del regolamento regionale 8 agosto 2012.
- deliberazione della Giunta Regionale 5 agosto 2002, n. 115-6947, Deliberazione del Consiglio regionale 17 marzo 2015, n. 61 – 10542, Articolo 14, legge regionale 3 agosto 2011, n. 15 (Disciplina delle attività e dei servizi necroscopici, funebri e cimiteriali. Modifiche della legge regionale del 31 ottobre 2007, n. 20 'Disposizioni in materia di cremazione, conservazione, affidamento e dispersione delle ceneri'): approvazione del Piano regionale di coordinamento per la realizzazione di nuovi cimiteri e crematori,
- deliberazione della Giunta Regionale 5 agosto 2002, n. 115-6947
- deliberazione del Consiglio regionale 17 marzo 2015, n. 61 – 10542, Articolo 14, legge regionale 3 agosto 2011, n. 15 (Disciplina delle attività e dei servizi necroscopici, funebri e cimiteriali. Modifiche della legge regionale del 31 ottobre 2007, n. 20 'Disposizioni in materia di cremazione, conservazione, affidamento e dispersione delle ceneri'): approvazione del Piano regionale di coordinamento per la realizzazione di nuovi cimiteri e crematori;
- delle disposizioni in materia di smaltimento rifiuti speciali.

ART. 29 - RESPONSABILE DEL PROCEDIMENTO

Il responsabile del procedimento è il Dott. Abbate Maurizio in qualità di Responsabile dell'area amministrativa del Comune di Frossasco.

ART. 30 - TRATTAMENTO DATI

1. Titolare del trattamento dei dati in questione è il Comune di Frossasco. Il Titolare rende noto di aver provveduto alla nomina del Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'art. 37, par. 1, lett a) del GDPR, individuando quale soggetto idoneo l'Avv. Massimo Ramello e che il medesimo è raggiungibile ai seguenti recapiti:
Telefono: 01311826681 - Pec: dpo@pec.gdpr.nelcomune.it
2. L'informativa sul trattamento dei dati personali ai sensi degli articoli 13 e 14 del regolamento UE 2016/679 (GDPR) in relazione ai contratti pubblici stipulati dall'ente è reperibile sull'home page del sito internet del Comune di Frossasco alla voce "privacy" ovvero all'URL https://privacy.nelcomune.it/comunefrossasco.it/informativa_comune_contratti_pubblici#content.
3. L'affidatario del servizio tratterà i dati personali di cui verrà a conoscenza nell'ambito del servizio medesimo in qualità di responsabile esterno del trattamento, come da disciplinare allegato al presente capitolato speciale.
4. L'Appaltatore ha l'obbligo di mantenere riservati i dati e le informazioni di cui venga in possesso e comunque di non divulgarli in alcun modo ed in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del contratto.

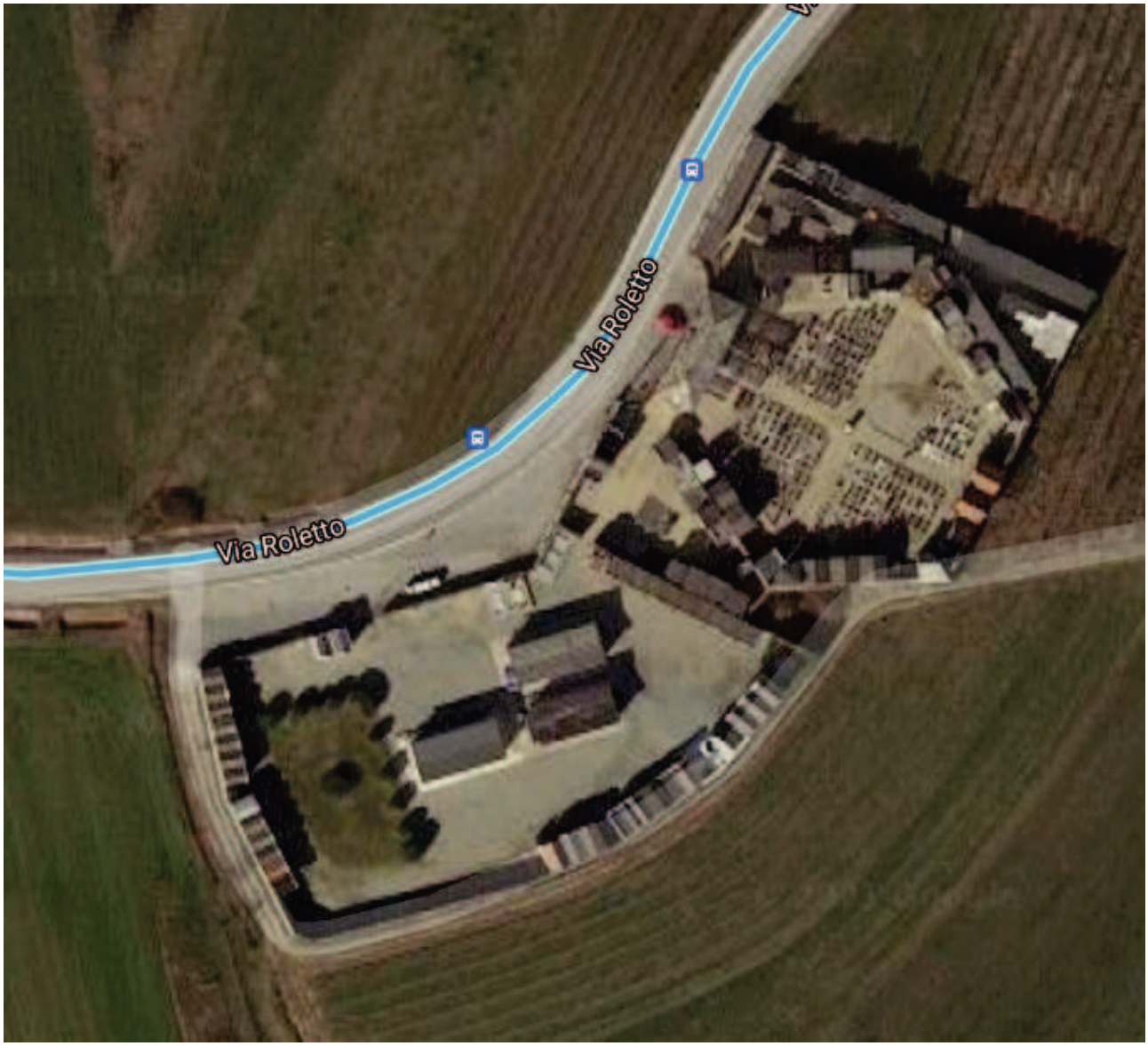
Allegati al capitolato:

- Fotografia del cimitero comunale;
- nomina a responsabile esterno del trattamento dei dati personali;
- D.U.V.R.I.
- disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (c.d. *data breach*) approvata con deliberazione di giunta comunale n. 53 del 30.07.2021;

Frossasco, lì 28.01.2022

Il Responsabile del Servizio Amministrativo
dott. Maurizio Abbate

Fotografia del cimitero comunale



Documento Unico di Valutazione dei Rischi da Interferenze
D.U.V.R.I.
(Art. 26 del D. Lgs. N. 81/2008 e s.m.i.)

INDIVIDUAZIONE DEI RISCHI SPECIFICI DEL LUOGO DI LAVORO MISURE ADOTTATE PER ELIMINARE LE INTERFERENZE APPALTO PER L'AFFIDAMENTO DEL SERVIZIO NECROFORICO, PULIZIA E DI MANUTENZIONE ORDINARIA DEL CIMITERO COMUNALE DI FROSSASCO IN VIA ROLETTO, 3. BIENNIO 2022/2023

(Codice CIG Z88347BE09)

1. Premessa

Il presente documento è redatto ai fini della previsione di cui all'art. 26, comma 1, lett. b) del d.lgs. 81/2008 che prevede di fornire all'impresa appaltatrice dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività. Il Servizio necroforico, di pulizia e di manutenzione ordinaria del cimitero comunale di Frossasco in via Roletto, 3 di cui al capitolato di appalto non risulta superiore a cinque uomini-giorno.

Il presente preliminare Documento Unico di Valutazione dei Rischi da Interferenze, **(DUVRI),** contiene le misure minime di prevenzione e protezione da adottare al fine di ridurre al minimo i rischi derivanti da possibili interferenze tra le attività svolte dall'appaltatore, gli utenti/visitatori e le imprese che, a vario titolo, potrebbero operare nel cimitero (imprese funebri, marmisti, ecc.), ed è predisposto in linea alla Determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture n. 3 del 5 marzo 2008 "*Sicurezza nell'esecuzione degli appalti relativi a servizi e forniture. Predisposizione del documento unico di valutazione dei rischi (DUVRI) e determinazione dei costi della sicurezza*" (G.U. n. 64 del 15/03/2008) che, in tale materia, afferma*"...Deve, inoltre, essere sottolineato che la valutazione dei rischi da interferenze, in particolare negli edifici quali, a titolo esemplificativo, ospedali e scuole, deve avvenire con riferimento non solo al personale interno ed ai lavoratori delle imprese appaltatrici, ma anche agli utenti che a vario titolo possono essere presenti presso la struttura stessa quali degenti, gli alunni ed anche il pubblico esterno*."

L'Appaltatore, nella comunicazione dei rischi specifici connessi alla propria attività, può presentare proposte di integrazione al **DUVRI**, ove ritenga di poter meglio garantire la sicurezza sul lavoro sulla base della propria esperienza.

In nessun caso le eventuali integrazioni possono giustificare modifiche o adeguamenti dei costi della sicurezza individuati nel presente documento.

Il **DUVRI**, che deve essere allegato al contratto di appalto, deve essere messo a disposizione dei partecipanti alla gara ai fini di formulazione dell'offerta e costituisce specifica tecnica di cui, all'art. 68 del D.Lgs. 50/2016 e s.m.i. e quelle indicate dal punto 1 dell'allegato XIII.

Il presente **DUVRI** contiene indicazioni di massima che devono essere integrate e dettagliate, a cura e onere dell'Appaltatore, successivamente all'aggiudicazione dell'appalto. Il **DUVRI**, così modificato e integrato, deve essere trasmesso al Responsabile Unico del Procedimento.

Il presente documento riguarda esclusivamente i rischi dovuti alle interferenze ossia alle circostanze in cui si verifica un **"contatto rischioso"** tra i seguenti soggetti esposti a rischi interferenti:

- Ditta appaltatrice: l'unico soggetto operativo per i lavori relativi alla gestione e manutenzione del cimitero comunale è la ditta appaltatrice; pertanto, qualunque rischio da interferenza derivato dalle fasi lavorative di cui alle prestazioni contrattuali, riguarda il personale addetto della ditta stessa.
- altre Ditte presenti nell'area cimiteriale: qualora si eseguano lavori quali manutenzione ovvero costruzione di beni immobili da realizzarsi all'interno del cimitero incaricati dall'ente o da privati su aree in concessione.
- Imprese funebri: durante la celebrazione del funerale può essere presente un rischio di interferenza tra gli addetti delle imprese funebri con i lavoratori dell'impresa appaltatrice;
- Visitatori: i fruitori del cimitero, ovvero i cittadini, anche per questi esiste la possibilità di esposizione a rischio da interferenza.

Relativamente all'effettuazione di eventuali sopraluoghi del personale comunale nell'area del cimitero questi avverranno a seguito di coordinamento con l'appaltatore secondo tempistiche e modalità non interferenti.

Le attività di manutenzione e pulizia dovranno avvenire in zone delimitate ovvero in orari di chiusura al pubblico ed a terzi dell'area cimiteriale.

Le prescrizioni previste nel presente Documento non si estendono ai rischi specifici propri dell'attività cui è soggetta l'Impresa Appaltatrice e per i quali deve conformarsi alla normativa di settore vigente. L'Impresa Appaltatrice, entro il termine massimo di **30 giorni** dalla data di affidamento dell'appalto e possibilmente prima dell'inizio effettivo dello stesso, deve redigere il proprio documento di valutazione dei rischi e provvedere all'attuazione delle misure necessarie per ridurre al minimo tali rischi.

Il **DUVRI**, come ha affermato l'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture (Determinazione n. **3/2008**), non è un documento **"statico"** ma **"dinamico"**, per cui la valutazione dei rischi, effettuata prima dell'espletamento della gara d'appalto, deve essere necessariamente aggiornata in caso di mutamenti, quali l'intervento di subappalti o di forniture, ovvero in caso di modifiche di carattere tecnico, logistico o organizzativo resesi necessarie nel corso dell'esecuzione dell'appalto e incidenti sulla modalità di effettuazione del servizio.

Nel **DUVRI** vengono riportate solo le misure e gli eventuali costi per eliminare i rischi derivanti dalle possibili interferenze presenti nell'effettuazione delle prestazioni (anche verso gli utenti), fermo restando l'obbligo per le imprese di adottare le misure dirette a eliminare i rischi derivanti dalla propria attività.

Tali imprese devono dimostrare di ottemperare a tutti gli adempimenti in materia di salute e sicurezza nei luoghi di lavoro previsti dal D. L/vo **81/2008** e s.m.i. (valutazione dei rischi, informazione, formazione addestramento, utilizzo **DPI**, ecc.).

Sospensione del servizio
In caso di inosservanza di norme in materia di sicurezza o in caso di pericolo imminente per i lavoratori, il Responsabile del Procedimento ovvero il Committente, potrà ordinare la sospensione del servizio, disponendone la ripresa solo quando sia di nuovo assicurato il rispetto della normativa vigente e siano ripristinate le condizioni di sicurezza ed igiene del lavoro.

2. Soggetti coinvolti

Nelle seguenti tabelle sono indicati i soggetti con compiti di sicurezza.

ENTE APPALTANTE	COMUNE DI FROSSASCO	
RUOLO	**NOMINATIVO**	**RECAPITO**
Datore di lavoro	Ing. Comba Federico	Frossasco, Via De' Vitis, n. 10 0121.352104

Responsible del Procedimento	Dott. Abbate Maurizio	Frossasco, Via De' Vitis, n. 10 0121.352104
Responsabile del servizio di prevenzione e protezione	Gruppo POLARIS S.r.l. Ing. Polidoro Giovanni	Pinerolo, Via F.G. Bona, n. 15 0121303768
RLS	Arch. Buffo Giuseppe	Frossasco, Via De' Vitis, n. 10 0121.352104
Medico competente	Dott. Rolfo Alberto	Pinerolo, Via G.B. Rossi, n. 4 0121378842
IMPRESA APPALTARICE	(ragione sociale) (indirizzo) (telefono – fax – mail)	
RUOLO	**NOMINATIVO**	**RECAPITO**
Datore di lavoro		
Responsabile del Procedimento		
Responsabile del servizio di prevenzione e protezione		
RLS		
Medico competente		
Direttore Tecnico		
Codice Fiscale		
Posizione CCIAA		
Posizione INPS		
Posizione INAIL		
Posizione CASSA EDILE		

3. Descrizioni dell'attività oggetto dell'appalto

L'appalto ha per oggetto l'affidamento del servizio necroforico, di pulizia e di manutenzione ordinaria del cimitero comunale di Frossasco in via Roletto, 3. biennio 2022/2023, da effettuarsi mediante la fornitura di tutti i servizi e le prestazioni come specificate nel Capitolato Speciale di Appalto al quale si rinvia.
L'appalto ha la durata di **anni due** con decorrenza dalla data indicata nel capitolato speciale di appalto.

4. Descrizione delle misure di sicurezza attuate

Con il presente documento unico preventivo vengono fornite all'impresa appaltatrice già in fase di gara d'appalto d**ettagliate informazioni sui rischi di carattere generale** esistenti sui luoghi di lavoro oggetto dell'appalto (e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività), sui rischi derivanti da possibili interferenze nell'ambiente/i in cui sono destinate ad operare le ditte appaltatrici nell'espletamento dell'appalto in oggetto e sulle misure di sicurezza proposte in relazione alle interferenze;

Le possibili situazioni di interferenza che possono verificarsi nel corso dell'appalto, valutabili in questa fase di elaborazione del documento, vengono di seguito elencate:

1) Attività dell'Appaltatore e contestuale presenza di utenti o dipendenti comunali: ove non sia possibile differire l'attività dell'Appaltatore, si devono adottare tutte le misure necessarie per ridurre i possibili rischi da interferenza (segnalazioni, transenne, recinzioni, ecc.).
2) Attività dell'Appaltatore e contestuale presenza di altre Imprese (Imprese funebri, marmisti, imprese incaricate da privati): l'Appaltatore ha l'onere di provvedere al coordinamento delle varie imprese e di adottare tutte le misure necessarie per ridurre i possibili rischi di interferenza (segnalazioni, transenne, recinzioni, ecc.).

Di seguito si riporta l'elenco dei possibili rischi da interferenze e le indicazioni delle misure di sicurezza di massima da adottare:

Attività Lavorazioni	Possibili rischi Interferenza	Misure di Sicurezza Interventi di prevenzione e protezione
Inumazione salma a terra	Urto, inciampo, rischio caduta, possibile cedimento di terreno	Delimitazione dell'area interessata, segnaletica, cartellonistica, sbattacchiature
Tumulazione salma in loculo, tomba di famiglia (anche ipogea), cappella privata	Rischio caduta dall'alto rischio caduta materiali dall'alto, rischio inciampo, possibile cedimento terreno	Delimitazione dell'area interessata, segnaletica, cartellonistica, utilizzo di monta feretri, trabattelli/ponteggi, sbatacchiatura
Tumulazione resti ossei - ceneri in ossario - cinerario	Rischio caduta dall'alto, rischio caduta materiali dall'alto, rischio inciampo	Delimitazione dell'area interessata, segnaletica, cartellonistica, utilizzo di trabattelli/ponteggi
Tumulazione resti ossei - ceneri in loculo, tomba di famiglia, tomba a terra, cappella privata	Rischio caduta dall'alto, rischio caduta materiali dall'alto, rischio inciampo	Delimitazione dell'area interessata, segnaletica, cartellonistica, utilizzo di trabattelli/ponteggi
Collocazione resti ossei, ceneri in ossario o cinerario comune	Rischio caduta, rischio inciampo	Delimitazione dell'area interessata, segnaletica, cartellonistica, utilizzo di trabattelli/ponteggi
Inumazione ceneri a terra	Urto, inciampo, rischio caduta,	Delimitazione dell'area interessata, segnaletica,
Esumazione ordinaria	Urto, rischio inciampo, rischio caduta, possibile cedimento di terreno, rischio biologico	Delimitazione dell'area interessata con recinzione idonea ad impedire l'accesso ai non addetti, segnaletica, cartellonistica, sbatacchiature, predisposizione di particolari procedure da parte del Datore di Lavoro
Estumulazione ordinaria salma	Rischio caduta dall'alto, rischio caduta materiali dall'alto, rischio inciampo	Delimitazione dell'area interessata, segnaletica, cartellonistica, utilizzo di monta feretri, trabattelli/ponteggi
Estumulazione resti ossei, ceneri	Rischio caduta dall'alto, rischio caduta materiali dall'alto, rischio inciampo	Delimitazione dell'area interessata, segnaletica, cartellonistica, utilizzo di trabattelli/ponteggi
Esumazione straordinaria	Urto, rischio inciampo, rischio caduta, possibile cedimento di terreno, rischio biologico	Delimitazione dell'area interessata con recinzione idonea ad impedire l'accesso ai non addetti, segnaletica, cartellonistica, sbatacchiature,
Estumulazione straordinaria	Urto, rischio inciampo, rischio caduta, possibile cedimento di terreno, rischio biologico	Delimitazione dell'area interessata con recinzione idonea ad impedire l'accesso ai non addetti, segnaletica, cartellonistica, sbatacchiature, predisposizione di particolari procedure da parte del Datore di Lavoro
Rifiuti derivanti da operazioni cimiteriali	Urto, rischio inciampo, rischio caduta, possibile cedimento di terreno, rischio biologico	Delimitazione dell'area interessata con recinzione idonea ad impedire l'accesso ai non addetti, segnaletica, cartellonistica, sbatacchiature, predisposizione di particolari procedure da parte del Datore di Lavoro

Sfalcio erba/spargimento ghiaia	Rischio inciampo, proiezioni di schegge o di sassi durante la lavorazione, scivolamenti	Delimitazione dell'area interessata con recinzione idonea, segnaletica, cartellonistica
Servizio di pulizia	Urto, rischio inciampo, scivolamenti, in relazione alla natura del prodotto impiegato possibili pericoli di inalazione e/o contatto diretto	Delimitazione dell'area, segnaletica, cartellonistica
Diserbo	Urto, rischio inciampo	Delimitazione dell'area, segnaletica,

A fronte della limitatezza e della particolarità delle operazioni necroforiche oggetto di appalto e del fatto che la principale misura di sicurezza per evitare rischi interferenziali, in relazione soprattutto alle circoscritte operazioni di manutenzione e pulizia, consiste nello svolgimento delle medesime in zone delimitate dell'area ovvero in orari di chiusura al pubblico ed a terzi dell'area cimiteriale non si rinvengono costi per la riduzione o eliminazione di tali rischi interferenziale.

DISCIPLINARE SULLA PROTEZIONE DEI DATI PERSONALI A VALERE SULL'AFFIDAMENTO DEI SERVIZI CIMITERIALI (ARTICOLO 28 DEL REGOLAMENTO (EU) 2016/679)

PREMESSO CHE

1) l'articolo 4, paragrafo 1, n. 8) del Regolamento (UE) 2016/679 (di seguito, per brevità, "GDPR") definisce quale responsabile del trattamento "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*";
2) a norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*";
3) a norma dell'articolo 28, paragrafo 3 del GDPR "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*";
4) a norma dell'articolo 28, paragrafo 9 del GDPR "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*"
5) in conseguenza dell'affidamento del servizio di che trattasi, il fornitore si troverà ad effettuare il trattamento di dati personali per conto dell'Ente (Titolare del trattamento), assumendo la qualifica di Responsabile del trattamento ai sensi e per gli effetti di cui all'articolo 28 del GDPR;
6) è intenzione dell'Ente subordinare l'autorizzazione al trattamento dei dati personali, per proprio conto, al rispetto delle seguenti prescrizioni minime ed a quelle eventualmente contenute in altri atti e documenti, da questo atto richiamati;

SI STABILISCE QUANTO SEGUE

Articolo 1 – Disposizioni generali

1. Le previsioni contenute nel presente disciplinare riguardano espressamente i servizi cimiteriali e si intendono accettate - senza riserva alcuna da parte del fornitore - a seguito dell'invio della propria offerta.
2. Le prescrizioni contenute nel presente Disciplinare possono subire modifiche ed integrazioni in conseguenza della valutazione delle informazioni rese dal Responsabile in ottemperanza a quanto previsto negli atti che hanno dato avvio alla procedura di selezione del contraente. Il Responsabile del trattamento informa immediatamente il Titolare qualora, a suo parere, una specifica prescrizione, in qualunque tempo impartita, violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. L'esecuzione delle operazioni di trattamento per conto del Titolare costituisce manifestazione espressa della volontà di accettare tutte le prescrizioni da esso impartite.
2. I presente disciplinare non costituisce autorizzazione generale, bensì, autorizzazione limitata esclusivamente ai trattamenti relativi al servizio oggetto della presente procedura selettiva.
3. Il Responsabile è tenuto a trattare i dati personali di cui entra in possesso o rispetto ai quali abbia comunque accesso, in adempimento degli obblighi derivanti dall'affidamento e di eventuali servizi accessori allo stesso, nel rispetto dei principi e delle norme contenute nel GDPR ed attenendosi alle istruzioni del Titolare del trattamento, tenendo altresì conto dei provvedimenti, tempo per tempo, emanati dall'Autorità di controllo inerenti al trattamento svolto.

Articolo 2 – Durata del trattamento

1. Il trattamento per conto del Titolare deve avere una durata non superiore a quella necessaria ad eseguire la prestazione contrattuale per la quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile, in una forma che consenta l'identificazione degli Interessati, per un periodo di tempo non superiore a quello in precedenza indicato, fatta salva l'osservanza di specifiche disposizioni di legge che ne impongano la conservazione.

2. A seguito della cessazione del trattamento affidato al Responsabile, nonché a seguito della cessazione del rapporto contrattuale sottostante, qualunque ne sia la causa, il Responsabile sarà tenuto, a discrezione del Titolare, a:
- restituire al Titolare i dati personali trattati, oppure a
- provvedere alla loro integrale distruzione, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità (contabili, fiscali, ecc.) od il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.
3. Il Responsabile, su richiesta del Titolare, provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sè, non esiste alcuna copia dei dati personali e delle informazioni trattate per conto del Titolare. Sul contenuto di tale dichiarazione il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.
4. In caso di fallimento o sottoposizione ad altra procedura concorsuale del Responsabile, ovvero in caso di mancato assolvimento da parte di quest'ultimo degli obblighi previsti ai commi che precedono, ovvero ancora in caso di omissione ovvero di sospensione anche parziale, da parte del Responsabile, dell'esecuzione delle obbligazioni qui previste, il Titolare, ove possibile e dandone opportuna comunicazione, potrà sostituirsi al Responsabile nell'esecuzione delle obbligazioni ovvero potrà avvalersi di soggetto terzo in danno ed a spese del Responsabile, fatto salvo il risarcimento del maggior danno.

Articolo 3 - Obblighi in capo al Responsabile
1. Il Responsabile dichiara e conferma la propria diretta ed approfondita conoscenza degli obblighi ed oneri derivanti dall'osservanza delle disposizioni contenute nel GDPR, in conseguenza della relazione contrattuale instaurata con il Titolare. Dichiara inoltre di possedere esperienza, capacità e affidabilità idonee a garantire il rispetto delle disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, ed in ogni caso di essere in grado di fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa e garantisca la tutela dei diritti dell'Interessato.
2. Il Responsabile è tenuto a:
a) trattare i dati nel rispetto dei principi del trattamento previsti nel GDPR e solo per la sola finalità di dare esecuzione al contratto. In particolare, il Responsabile garantisce che i dati da trattarsi per conto del Titolare, saranno:
a1) trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato;
a2) raccolti per le finalità determinate, esplicite e legittime sopra indicate, e successivamente trattati in modo che non sia incompatibile con tali finalità;
a3) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
a4) 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;
a5) 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;
b) trattare i dati secondo le istruzioni documentate del Titolare del trattamento dei dati;
c) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate formalmente alla riservatezza od abbiano un adeguato obbligo legale di riservatezza ed abbiano ricevuto la formazione necessaria in materia di protezione dei dati personali;
d) prendere in considerazione, in termini di strumenti, prodotti, applicazioni o servizi, i principi della protezione dei dati in base alla progettazione e per impostazione predefinita (cc.dd. data protection by design e by default);
e) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;
3. Il Responsabile si impegna ad informare il Titolare di ogni richiesta, ordine o controllo da parte di una o più Autorità e da soggetti da queste autorizzati e/o delegati, in relazione ai trattamenti oggetto di affidamento;

Articolo 4 - Obblighi in capo al Titolare del trattamento

1. Il Titolare del trattamento si impegna a:
a) fornire al Responsabile i dati oggetto del trattamento curandone l'esattezza, la veridicità, l'aggiornamento, la pertinenza e la non eccedenza rispetto alle finalità per le quali sono stati raccolti e saranno successivamente trattati;
b) individuare la base legale del trattamento dei dati personali degli Interessati.
c) documentare, per iscritto, ogni istruzione relativa al trattamento dei dati da parte del Responsabile. Il Responsabile del trattamento informa immediatamente il Titolare qualora, a suo parere, un'istruzione violi il GDPR od altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
d) assicurare, prima e durante l'intero processo, il rispetto degli obblighi su di sé incombenti ai sensi del GDPR e della normativa nazionale di riferimento;
e) supervisionare il trattamento, in tutte le sue fasi, anche effettuando audit ed ispezioni presso il Responsabile;
f) adottare tutte le misure di sicurezza di sua competenza idonee a garantire il rispetto della normativa in materia di privacy e di trattamento dei dati in regime di sicurezza.
2. Il Titolare si dichiara edotto che in caso di violazione di dati personali (c.d. data breach) rimane a suo carico, ai sensi dell'art. 33 del GDPR, l'obbligo di notifica all'Autorità di controllo senza ingiustificato ritardo e, comunque, entro 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione di dati personali.
3. Il Titolare si impegna, altresì, a comunicare al Responsabile del trattamento qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati.
4. Il Titolare rimane Responsabile del trattamento dei dati personali attuato tramite procedure applicative sviluppate secondo sue specifiche e/o attraverso propri strumenti informatici o di telecomunicazioni.
5. Il Titolare si impegna ad informare il Responsabile di ogni richiesta, ordine o controllo da parte di una o più Autorità e da soggetti da queste autorizzati e/o delegati, in relazione ai trattamenti oggetto di affidamento;

Articolo 5 - Incaricati e persone autorizzate

1. Il Responsabile dovrà identificare e designare le persone autorizzate ad effettuare operazioni di Trattamento sui dati per conto del Titolare identificando l'ambito autorizzativo consentito ai sensi dell'art. 29 del GDPR e provvedendo alla relativa formazione. Allo stesso tempo, il Responsabile dovrà fornire ai soggetti da sé autorizzati le dovute istruzioni relativamente alle operazioni ed alle modalità di trattamento dei dati personali.
2. Il Responsabile garantisce che i propri dipendenti e collaboratori sono affidabili ed hanno piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali.

Articolo 6 - Sub-responsabile del trattamento e Terze parti

1. Il Responsabile del trattamento non ricorre ad un altro Responsabile se non previa autorizzazione scritta, del Titolare del trattamento. Qualora, anche successivamente all'affidamento, il Responsabile ravvisasse la necessità di avvalersi di un altro responsabile del trattamento (Sub-responsabile) per l'esecuzione di specifiche attività di trattamento per conto del Titolare, è tenuto a richiederne l'autorizzazione al Titolare con congruo preavviso. La mancata autorizzazione non consentirà il ricorso al Sub-responsabile.
2. Nel caso in cui il Responsabile del trattamento (Responsabile primario) ricorra ad un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile sono imposti, mediante un contratto od un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente Disciplinare per il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della legge vigente.
3. Nel caso in cui l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è imputabile.

4. Il Responsabile si impegna a non comunicare, trasferire o condividere, i dati personali trattati per conto del Titolare a Terze parti, salvo qualora legislativamente richiesto e, in ogni caso, informandone preventivamente il Titolare.

Articolo 7 - Misure di sicurezza

1. Il Responsabile, in considerazione della conoscenza maturata in relazione ai progressi tecnici e tecnologici, della natura dei dati personali e delle caratteristiche delle operazioni di trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate e dovrà assicurare che le misure di sicurezza progettate ed implementate siano in grado di ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi agli scopi di cui alla presente Appendice.
2. Ai fini della sicurezza dei dati e dei sistemi IT, il Responsabile si obbliga:
- ad adottare adeguate misure IT per la sicurezza dei dati personali, ai sensi dell'art. 32 del GDPR, in modo da garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- ad adottare adeguate misure che consentano di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- a non trasferire i dati personali oggetto di trattamento per conto del Titolare, senza il preventivo consenso di questi, al di fuori dell'usuale luogo di lavoro, a meno che tale trasferimento non sia autorizzato dalle competenti pubbliche autorità, anche regolamentari e di vigilanza;
- a fornire, in caso di richiesta, al Titolare una descrizione dettagliata delle misure fisiche, tecniche ed organizzative applicate al trattamento dei dati personali;
- ad impiegare sistemi di cifratura per i dati personali memorizzati su dispositivi di archiviazione digitali od elettronici, come computer portatili, CD, dischetti, driver portatili, nastri magnetici o dispositivi similari. I dati personali dovranno essere cifrati nel rispetto della normativa vigente ed il Responsabile dovrà compiere ogni ragionevole sforzo per assicurare l'aggiornamento degli standard di cifratura in modo da tenere il passo dello sviluppo tecnologico e dei rischi ad esso connaturati, includendo ogni richiesta o indicazione emanata da qualsiasi pubblica autorità competente, anche regolamentare e di vigilanza;
- ad adottare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

Articolo 8 - Registro delle categorie di trattamento

1. Il Responsabile del trattamento adotta, aggiorna e conserva una registrazione scritta di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, avente il contenuto minimo previsto dall'articolo 30, paragrafo 2 del GDPR e, su richiesta, lo rende disponibile all'Autorità di controllo ed al Titolare.

Articolo 9 - Violazioni di dati personali

1. In eventuali casi di violazione della sicurezza dei dati personali che comporti, accidentalmente od in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve osservare le disposizioni organizzative contenute nella data breach policy adottata dal Titolare e, in ogni caso:
a) informare il Titolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire al Titolare tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare e sugli Interessati coinvolti e le misure adottate per mitigare i rischi. Spetta unicamente al Titolare del trattamento di effettuare la valutazione circa la probabilità di rischio derivante dalla violazione stessa;
b) fornire assistenza al Titolare per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare ed attuando tutte le azioni correttive approvate e/o richieste dal Titolare. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito;

2. Il Responsabile del trattamento si impegna a predisporre e tenere aggiornato un registro interno delle violazioni di dati personali nonché a raccogliere e conservare tutti i documenti relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Articolo 10 - Accordo relativo al trasferimento dei dati all'estero

1. Il Responsabile si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei Dati personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server od in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).
2. Il Responsabile, pertanto, non dovrà trasferire od effettuare il Trattamento dei Dati personali per conto del Titolare al di fuori dell'Unione Europea, per nessuna ragione, in assenza di autorizzazione scritta del Titolare. Qualora il Titolare rilasci l'autorizzazione di cui al presente articolo e venga pertanto effettuato un trasferimento dei dati personali del Titolare al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare le previsioni di cui al GDPR sopra indicate. Resta inteso tra le Parti che il Responsabile dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata della presente Appendice.
Il Responsabile è obbligato a comunicare immediatamente al Titolare il verificarsi di una delle seguenti fattispecie:
(a) mancato rispetto delle clausole contrattuali standard di cui sopra, oppure
(b) qualsiasi modifica della metodologia e delle finalità trasferimento dei dati personali all'estero.

Articolo 11 - Diritti delle persone interessate

1. È compito del Responsabile del trattamento fornire adeguata informativa agli Interessati dalle operazioni di trattamento, nel momento in cui i dati vengono raccolti presso di loro. L'informativa dovrà evidenziare il fatto che la raccolta avviene per conto del Titolare.
2. Il Responsabile, per quanto di propria competenza, si obbliga ad assistere ed a supportare il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare riscontro alle richieste per l'esercizio dei diritti dell'Interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile) nel rispetto dei termini previsti dall'art. 12 del GDPR.
3. In particolare, qualora il Responsabile riceva richieste provenienti dagli Interessati, finalizzate all'esercizio dei propri diritti, esso dovrà:
- darne tempestiva comunicazione scritta al Titolare via posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate dal Titolare per gestire le relazioni con gli Interessati;

Articolo 12 - Verifiche circa il rispetto delle regole di protezione dei dati personali

1. Il Responsabile riconosce al Titolare il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali per conto del Titolare. A tal fine, il Titolare ha il diritto di disporre – a propria cura e spese – verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.
2. Il Responsabile del trattamento fornisce al Titolare tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire al Titolare od a qualsiasi soggetto dal medesimo autorizzato o delegato di condurre audit, comprese le ispezioni, e per contribuire a tali verifiche.
3. Il Responsabile del trattamento deve informare e coinvolgere tempestivamente il Titolare in tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità di controllo;

Articolo 13- Manleva e Responsabilità per violazione delle disposizioni

1. Il Responsabile s'impegna a mantenere indenne il Titolare da qualsiasi responsabilità, danno, incluse le spese legali, od altro onere che possa derivare da pretese, azioni o procedimenti avanzate da terzi a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento dei dati personali che sia imputabile a fatto, comportamento od omissione del Responsabile (o di suoi dipendenti e/o collaboratori), ivi incluse le eventuali sanzioni che dovessero essere comminate ai sensi del GDPR.
2. Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità alla prestazione dei servizi dedotti nel Contratto.
3. Il Titolare ha il diritto di reclamare dal Responsabile la parte dell'eventuale risarcimento di cui dovesse essere chiamato a rispondere nei confronti di terzi per le violazioni commesse dal Responsabile ai sensi dell'art. 82, paragrafo 5, del GDPR.
4. Fatti salvi gli articoli 82, 83, e 84 del GDPR, in caso di violazione delle disposizioni contenute nella presente Appendice, relative alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute od in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal GDPR, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà direttamente, anche dal punto di vista sanzionatorio.

Articolo 14 - Responsabile della Protezione dei dati personali

1. Il Titolare rende noto di aver provveduto alla nomina del Responsabile della Protezione dei Dati personali (RPD o DPO) in conformità alla previsione contenuta nell'art. 37, par. 1, lett a) del GDPR, individuando quale soggetto idoneo l'Avv. Massimo Ramello e che il medesimo è raggiungibile ai seguenti recapiti:
Telefono: 01311826681 - Pec: dpo@pec.gdpr.nelcomune.it
Detto nominativo è stato altresì comunicato all'Autorità Garante per la Protezione dei dati personali con procedura telematica.

Articolo 15 – Comunicazioni

1. Qualsiasi comunicazione relativa al trattamento dei dati personali nel contesto del servizio in oggetto dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna.

Articolo 16 – Disposizioni finali

1. Per quanto non espressamente qui stabilito, il Titolare ed il Responsabile del trattamento rinviano al GDPR, alle disposizioni nazionali di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo competente e del Comitato Europeo per la Protezione dei Dati Personali (EDPB).

DISPOSIZIONI OPERATIVE
IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONE DI DATI PERSONALI (c.d. DATA BREACH)

Versione del documento	
Data emissione	30.07.2021
Stato del documento	
Nome del file	"Data-breach_policy.docx"

Sommario

FINALITÀ E AMBITO DI APPLICAZIONE

Il Comune di Frossasco ai sensi del Regolamento Europeo 2016/679 (da qui in avanti **GDPR**), in quanto Titolare del trattamento (di seguito, per brevità, "**Titolare del trattamento**" o anche solo "**Titolare**"), è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività istituzionali e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi (di seguito, per comodità, "**data breach**"), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati.

Il **mancato rispetto** dell'obbligo di notifica ex articolo 33 del GDPR comporta l'applicabilità da parte dell'autorità di controllo delle **sanzioni amministrative** previste dall'art. 83, con la possibilità di infliggere sanzioni fino a 10.000.000 di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4). L'autorità potrebbe inoltre applicare le misure correttive previste dall'art. 58 GDPR e, quindi, rivolgere al titolare avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti provvisori o definiti al trattamento e di divieti, ordini di rettifica e cancellazione dei dati, revoche di certificazioni, ordini di sospendere i flussi di dati verso paesi terzi o organizzazioni internazionali.

Il GDPR prevede poi espressamente che al momento della decisione in merito alla sanzione amministrativa pecuniaria da infliggere ed alla definizione del suo ammontare, è necessario tenere conto nel caso concreto anche delle misure adottate dal titolare per attenuare il danno subito dagli interessati, come pure del grado di responsabilità del titolare (o del responsabile) alla luce delle misure tecniche e organizzative messe in atto ai sensi degli artt. 25 e 32. La stessa mancata notifica all'autorità di controllo, e/o comunicazione all'interessato, potrebbero d'altro canto essere considerate nel caso specifico indici di una mancata adozione di misure di sicurezza che potrebbe portare all'irrogazione di specifiche sanzioni al riguardo.

Inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il **risarcimento del danno** dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

E' pertanto di fondamentale importanza predisporre una procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa europea ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'Ente (**data breach policy**). A tale riguardo si precisa che, presso il Titolare, sono state attivate procedure a tutela della sicurezza dei dati, tra cui:

− l'adozione di misure organizzative e tecniche per garantire un livello di sicurezza adeguato al rischio connesso al trattamento dei dati personali e alle altre informazioni trattate, comprese misure volte al tempestivo ripristino della disponibilità in caso di incidente sulla sicurezza;
− l'organizzazione, a cadenza periodica, di corsi di formazione per i dipendenti/collaboratori sui principi cardine della normativa sul trattamento dati, sulla sicurezza dei dati personali e dei sistemi;
− la predisposizione di un sistema di protezione, mediante apposite misure tecniche (firewall, antivirus, …) dell'accesso a internet e ai dispositivi elettronici.

I dati oggetto di riferimento sono i dati personali trattati "*da* "e "*per conto*" del Titolare, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

Il presente documento ha lo scopo di indicare le **modalità di gestione di un data breach**, ovvero di un episodio di violazione di dati personali (come meglio spiegato nel prosieguo), nel

rispetto dei principi e delle disposizioni contenute nel Regolamento (UE) 679/2016 sulla protezione dei dati personali (GDPR).

L'obiettivo del presente documento è, pertanto:

- sensibilizzare il personale in ordine alle responsabilità in materia di protezione dei dati personali ed all'importanza della collaborazione nella tempestiva segnalazione e risoluzione degli incidenti sulla sicurezza (inclusi i data breach);
- definire processi per identificare, tracciare e reagire ad un incidente sulla sicurezza e ad un data breach, per valutarne il rischio, contenere gli effetti negativi e porvi rimedio nonché stabilire se, in caso di data breach, si renda necessario procedere alla (i) notifica al Garante e (ii) comunicazione agli Interessati;
- definire ruoli e responsabilità per la risposta agli incidenti sulla sicurezza ed i data breach;
- assicurare un adeguato flusso comunicativo all'interno della struttura del Titolare tra le parti interessate.

Le procedure qui contemplate sono applicabili a **tutte le attività svolte dal Titolare**, con particolare riferimento alla gestione di tutti gli archivi e documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati, anche con il supporto di fornitori esterni.

Le procedure descritte nel presente documento sono rivolte a **tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare**, quali:

a) I lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento;

b) qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti 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 questo documento si sintetizzano le regole per garantire la realizzabilità tecnica e la sostenibilità organizzativa nella gestione del data breach, sotto i diversi aspetti relativi a:

- modalità e profili di segnalazione al Titolare del trattamento;
- valutazione dell'evento accaduto;
- modalità e profili di notificazione all'Autorità di controllo;
- eventuale comunicazione agli interessati

garantendo al tempo stesso:

- l'identificazione della violazione;
- l'analisi delle cause della violazione;

- la definizione delle misure da adottare per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi;
- la registrazione delle informazioni relative alla violazione, delle misure identificate e dell'efficacia delle stesse.

DEFINIZIONI

Fermo restando che le uniche definizioni "ufficiali" e vincolanti sono quelle contenute nell'articolo 4 del GDPR e quelle contenute nel Codice per la protezione dei dati personali (D.Lgs. 30 giugno 2003 n. 196), si riporta la terminologia maggiormente utilizzata nel contesto del presente documento, per semplificarne la lettura.
«**GDPR**» o «**RGPD**» o «**Regolamento**»: il Regolamento (UE) n. 679/2016 "General Data Protection Regulation", in italiano indicato come "Regolamento generale sulla protezione dei dati";
«**CODICE PRIVACY**»: il Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali";
«**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;
«**CATEGORIE PARTICOLARI DI DATI PERSONALI**»: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
«**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;
«**DATI GENETICI**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
«**DATI BIOMETRICI**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
«**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;
«**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;
«**PSEUDONIMIZZAZIONE**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure

tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
«**COMUNICAZIONE**»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies del Codice privacy, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
«**DIFFUSIONE**»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
«**INTERESSATO**»: la persona fisica cui si riferiscono i dati personali;
«**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;
«**RESPONSABILE DEL TRATTAMENTO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
«**RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**» o «**DPO**»: soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire consulenza sugli obblighi derivanti dal GDPR e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (GDPR, art. 37, 38, 39);
«**DESTINATARIO**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
«**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;
«**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;
«**MINACCIA**»: una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale;
«**DANNO**»: conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto interessato;
«**MALWARE**»: software di tipo malevolo che causa danni ai sistemi informativi;
«**MISURA DI SICUREZZA**»: accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti;

«**CRITTOGRAFIA**»: tecnica che permette di "cifrare" un messaggio rendendolo incomprensibile a tutti fuorché al suo destinatario;
«**DECRITTOGRAFIA**»: il processo per "sbloccare" i dati criptati cioè cifrati;
«**AUTORITÀ DI CONTROLLO**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. In Italia, il Garante per la Protezione dei Dati Personali;
«**WP ARTICOLO 29**»: gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito della protezione dei dati personali e della vita privata, istituito ai sensi dell'art. 29 della direttiva 95/45/CE. A decorrere dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB) ai sensi del regolamento generale sulla protezione dei dati dell'UE (GDPR) (regolamento (UE) 2016/679);

PIANO DI AZIONE

Si individua il seguente piano d'azione per assicurare la conformità (compliance) del Titolare alle previsioni normative in tema di protezione dei dati personali. Il piano evidenzia in rosso le azioni "obbligatorie" ed in giallo quelle "non obbligatorie ma vivamente consigliate". Trattasi ovviamente di indicazioni di massima, debitamente integrate dalle regole contenute nel prosieguo del documento, che sono suscettibili di modifica ed integrazione in considerazione dell'evoluzione normativa e tecnica e delle peculiari caratteristiche organizzative del Titolare.

Azione	Annotazioni
Adottare una procedura interna di gestione dei data breach (obbligatorio)	Attraverso la presente policy sono definiti i ruoli e le responsabilità nella gestione degli incidenti e delle violazioni
Istruire il personale autorizzato al trattamento dei dati in materia di sicurezza e gestione di possibili violazioni (obbligatorio)	Il personale dev'essere in grado di identificare e gestire eventuali violazioni di dati personali
Verificare lo stato delle misure di sicurezza implementate presso l'Ente (consigliato)	Condurre audit sui sistemi informatici e non. Il GDPR richiede infatti che siano implementate tutte le misure tecnologiche ed organizzative per valutare se sia avvenuta una violazione di dati; tali misure aiutano anche a stabilire se sia necessaria o meno la notifica
Cifrare o pseudonimizzare i dati di cui agli articoli 9 e 10 del GDPR (obbligatorio)	
Limitare l'accesso ai dati personali solo al personale autorizzato (obbligatorio)	E' opportuno limitare l'accesso per ridurre le possibilità di eventuali violazioni, che spesso sono provocate anche da errore umano
Verificare le misure di sicurezza installate sui computer al fine di eliminare le vulnerabilità ed implementare misure di sicurezza logiche e fisiche adeguate (obbligatorio)	Occorre valutare le misure di sicurezza anche al fine di dimostrare la c.d. "accountability"
Preparare un piano di risposta alle violazioni (obbligatorio)	Il piano dovrebbe prevedere le seguenti azioni: – assicurare che i dati non siano più compressi; – mettere in sicurezza tutti i dati ed i sistemi;

	– identificare i dati compromessi, le categorie di Interessati coinvolte, la tipologia di violazione; – isolare i dati compromessi; – modificare le chiavi di codifica e le relative password immediatamente; – documentare tutte le fasi di gestione della violazione e tutte le informazioni relative alla violazione stessa; – determinare quando sia effettivamente avvenuta la violazione (al fine di notificare la violazione entro 72 ore)
Coinvolgere le autorità competenti ove si sospettino attività illecite (obbligatorio)	Non è strettamente richiesto dal GDPR, ma è opportuno notificare la violazione anche ad altre autorità, ove applicabile e richiesto dalla normativa vigente
Selezionare adeguatamente i fornitori che erogano attività che comportano un trattamento di dati (obbligatorio)	E' opportuno verificare e selezionare il fornitore e assicurare che la designazione come Responsabile contenga previsioni e istruzioni specifiche in materia di data breach
Conclusa la gestione urgente della violazione, valutare i "gaps" e l'efficacia dei sistemi interni, della formazione del personale e delle ulteriori procedure che mirano a tutelare i dati personali (obbligatorio)	Tale attività potrebbe essere inclusa in una fase di post-assessment
Testare frequentemente i sistemi interni (consigliato)	
Conservare un registro dei data breach ed aggiornarlo frequentemente (obbligatorio)	Il Titolare è tenuto a comunicare ogni informazione sulla violazione all'Autorità di controllo e per tale motivo è opportuno implementare un registro di data breach

PROCEDURA

Si individuano di seguito i soggetti coinvolti ed il flusso delle principali attività previste per la rilevazione e gestione di un incidente di sicurezza che possa comportare una violazione di dati personali.

La **tempestività** è un fattore determinante nella risposta agli incidenti sulla sicurezza ed ai data breach ed è dovere di ciascun soggetto, nell'ambito del proprio ruolo nella struttura e nella catena di comunicazione, non ritardare iniziative di reazione all'incidente e rispettare le procedure e le tempistiche di comunicazione individuate dal presente documento.

La risposta a un Incidente sulla sicurezza o ad un data breach deve avvenire secondo le fasi descritte di seguito. Considerando, tuttavia, che gli Incidenti possono avere molteplici cause o coinvolgere diversi soggetti ed avere conseguenze caratterizzate da vari livelli di gravità, tali fasi potrebbero sovrapporsi o richiedere tempistiche differenti o aggiornamenti. È tuttavia fatto obbligo ad ogni soggetto sotto la responsabilità del Titolare di collaborare e seguire le istruzioni che di volta in volta gli vengano fornite dallo stesso Titolare o dal DPO.

Considerati i rischi e, in caso di data breach, le ridotte tempistiche per effettuare la notifica e per la comunicazione agli interessati, occuparsi degli incidenti di sicurezza deve essere obiettivo prioritario per tutti i soggetti coinvolti nella loro gestione. Nella gestione di un qualunque incidente di sicurezza devono essere considerate le seguenti due priorità:

o **prima priorità**: proteggere tutti gli assets del Titolare, incluse le risorse colpite dall'incidente, fino al ripristino della normale operatività;

o **seconda priorità**: raccogliere informazioni e prove per supportare le eventuali e appropriate azioni correttive, disciplinari o legali;

Tutti gli incidenti di sicurezza ed i data breach devono essere trattati con il **massimo livello di riservatezza**: le informazioni devono essere condivise esclusivamente con il personale identificato nella presente procedura e solo quando strettamente necessario. Eventuali comunicazioni a soggetti non coinvolti nella gestione dell'Incidente dovranno limitarsi all'indicazione che si è verificato un problema e che lo stesso è in fase di gestione.

Tutte le attività di gestione devono essere **tracciate e documentate** per quanto possibile a partire dall'istante di rilevazione.

Il **coordinamento delle attività di gestione** di una violazione di dati personali, con particolare riferimento agli obblighi di comunicazione e notifica imposti dal GDPR, è assicurato dal DPO con il supporto dell'Amministratore di sistema (od altra figura analoga) per gli aspetti tecnici, nonché dal Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto. Il DPO ha comunque piena facoltà di convocare e coinvolgere altri soggetti che ritenga utili alle necessità del caso.

1. Individuazione della violazione

Le violazioni dei dati personali sono una tipologia di incidente per la sicurezza delle informazioni nel quale sia coinvolto qualsiasi genere di dato di natura personale (anagrafici, numeri di carte personali, codici identificativi, dati sanitari, dati biometrici, dati relativi a conti correnti, ecc.). **Tuttavia, come indicato all'articolo 4, punto 12, il GDPR si applica soltanto in caso di violazione di dati personali**.

La conseguenza di tale violazione è che il Titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

L'art. 33 del GDPR prescrive che "*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

Per *data breach* si intende quindi un evento in conseguenza del quale si verifica una "*violazione dei dati personali*". Nello specifico, l'articolo 4 punto 12 del GPDR definisce la violazione dei dati personali come "*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*". Non è quindi corretta la comune associazione tra data breach ed attacco o problema informatico poiché tale violazione può avvenire anche (ad esempio) a causa di un dipendente infedele che sottragga documentazione cartacea ovvero la smarrisca.

Il Gruppo di lavoro ex art. 29 ("WP29") ha adottato il 6 febbraio 2018 la versione definitiva delle linee guida sulla notifica delle violazioni dei dati personali (cd. "data breach") ai sensi del Regolamento UE n. 679/2016 (cd. "GDPR").

Con il termine "**Distruzione"** (*destruction*) si intende che non esistono più i dati ovvero i dati non esistono più in una forma che possa essere utilizzata dal Titolare. La violazione può essere determinata da una eliminazione logica (es. cancellazione dei dati) oppure fisica (es. rottura dei supporti di memorizzazione) non autorizzata e relativa impossibilità di ripristinare i dati entro i sette giorni.

Con il termine "**Modifica"** (*alteration, damage*) si intende la possibilità che avvengano modifiche improprie dei dati degli interessati non autorizzate, effettuate al di fuori dei processi operativi di trattamento dei dati svolti dagli incaricati autorizzati, oppure modifiche con finalità fraudolente eseguite dagli incaricati autorizzati all'accesso.

Con il termine "**Perdita"** (*loss*) si intende che i dati esistono ancora, ma il Titolare potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Perdita del supporto fisico di memorizzazione dei dati (dischi esterni, pendrive ecc.) in termini di privazione, sottrazione, smarrimento dei dispositivi contenenti i dati degli interessati oppure dei documenti cartacei. La perdita può essere anche temporanea ma superiore a sette giorni. Può riguardare le copie o gli originali dei supporti contenenti i dati personali dei soggetti interessati.

Per "**rivelazione**" si intende la trasmissione non autorizzata o impropria dei dati personali degli interessati verso terze parti (persone fisiche, persone giuridiche, gruppi di soggetti, pubblico) anche non precisamente identificabili.

Per "**accesso**" si intende l'accesso non autorizzato o improprio ai dati degli interessati. Accessi ai dati (anche in sola visualizzazione, sia in caso di accessi logici ai sistemi informatici sia agli archivi cartacei) effettivamente avvenuti al di fuori dei processi operativi di trattamento dei dati previsti e autorizzati.

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 GDPR.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione in base ai seguenti **tre principi di sicurezza delle informazioni**:

Violazione della riservatezza *(Confidentiality breach)*	**divulgazione** o accesso non autorizzato o accidentale ai dati personali come, ad esempio: • quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza; • quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento; • quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone prendono visione di informazioni; • quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato.
Violazione dell'integrità *(Integrity breach)*	**alterazione** non autorizzata o accidentale dei dati personali La "*alterazione*" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).
Violazione della disponibilità *(Availability breach)*	accidentale o non autorizzata **perdita di accesso** o **distruzione** di dati personali (Fattispecie non sempre di facile individuazione. La "*perdita di dati*" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi; la "*distruzione*" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal Titolare. Ci sarà sempre una violazione della Disponibilità del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione)

Ci si potrebbe chiedere se una **perdita temporanea della disponibilità** dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*" e "*la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico*".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrà essere documentata in conformità all'articolo 33, paragrafo 5, mediante annotazione nell'apposito registro delle violazioni. Ciò aiuta il Titolare del trattamento a dimostrare l'assunzione di responsabilità all'Autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'Autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il Titolare del trattamento dovrà comunque valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il Titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Va notato che, sebbene una perdita di disponibilità dei sistemi del Titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il medesimo Titolare consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi.

A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sopra indicati o una combinazione di essi.

La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione o perdita di documenti con dati personali (furto, smarrimento, abbandono, etc.). La casistica è molto ampia.

A mero **titolo esemplificativo** e senza pretesa di esaustività, l'oggetto della segnalazione di un data breach può essere:

- l'accesso abusivo (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- dati cancellati accidentalmente o da soggetti non autorizzati;
- perdita della chiave di decriptazione;
- dati persi dall'ambiente di produzione che non possano essere ripristinati integralmente dalle copie di sicurezza e si debba provvedere manualmente alla loro ricostruzione;
- interruzione significativa di un servizio ("*black out*" elettrico o attacchi di tipo "*denial of service*");
- divulgazione di dati confidenziali a persone non autorizzate;
- errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi;
- divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato;
- pubblicazione erronea delle informazioni personali (non di dominio pubblico) sul portale web istituzionale del Titolare;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- perdita o il furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o il furto di documenti cartacei;
- pirateria informatica;
- virus o altri attacchi al sistema informatico o alla rete dell'Ente;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "*owner*";

- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- formattazione di dispositivi di memorizzazione;
- malfunzionamenti software quali esecuzione di uno script automatico non autorizzato; errori di programmazione che causano output errati, ecc.;
- distruzione dolosa dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali;
- distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e di elettricità, umidità, corto circuito, caduta accidentale, eventi catastrofici/incendi, ecc.;
- guasti alla rete aziendale: a titolo di esempio caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

2. Rilevazione della violazione

La prima fase nella gestione del data breach è quella che conduce alla rilevazione della violazione o presunta violazione di sicurezza e della sua comunicazione al Titolare. Nell'ipotesi in cui ci si dovesse accorgere di essere stati vittima di un data breach la prima cosa da fare è quella di **non farsi prendere dal panico ed agire in modo scomposto** ma, anzi, applicare subito le procedure previste dalla presente policy.

2.1. Acquisizione della notizia

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia **affrontata immediatamente e correttamente** al fine di minimizzare l'impatto della violazione e prevenire che si ripeta. Ai fini di una corretta analisi della segnalazione, è necessario raccogliere fatti concreti prima di segnalare qualsiasi tipo di violazione, illecito ed irregolarità in ambito di tutela dei dati personali.

È importante che la raccolta della segnalazione o l'esecuzione della segnalazione da parte degli uffici avvenga **raccogliendo quante più informazioni possibili** (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc..). **Le segnalazioni, pertanto, devono essere fondate su elementi di fatto precisi, circostanziati e concordanti**.

Se al momento della rilevazione dell'incidente di sicurezza non è disponibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla comunicazione dell'incidente al Dirigente o Titolare di P.O., competente in ragione del servizio o settore coinvolto, per una prima valutazione d'impatto, anche con **informazioni incomplete**. Laddove necessario, alla prima valutazione possono seguirne altre, in base alle informazioni che vengono acquisite nella prosecuzione dell'indagine.

2.2. Fonte della notizia

La segnalazione di un data breach può essere **interna** (da personale dipendente, convenzionato, stagisti, tirocinanti, amministratori, DPO, …) o **esterna all'Ente** (Agid, Polizia, altre Forze dell'Ordine, giornalisti, utenti di servizi, RPD, Responsabili del trattamento, interessati, ecc.). Inoltre, ogni **interessato** può segnalare, anche solo in caso di sospetto, che i propri dati personali

siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'interessato può richiedere al Titolare la verifica dell'eventuale violazione.

Il pubblico e, in genere, i soggetti che non sono legati al Titolare del trattamento da rapporti contrattuali od altrimenti vincolanti, possono segnalare anomalie, disservizi o potenziali incidenti sulla sicurezza mediante comunicazione scritta inviata al protocollo. Il Titolare rende disponibili presso i propri uffici e sul **sito web istituzionale**, la **modulistica** e le **informazioni** utili allo scopo. Sebbene la segnalazione possa avvenire in forma libera, si ritiene opportuno suggerire al segnalante l'utilizzo di un apposito modello ALLEGATO A "Modulo di segnalazione di una potenziale violazione di dati personali", predisposto in modo tale da agevolare l'attività istruttoria e valutativa da parte del Titolare.

Nel caso in cui la segnalazione sia raccolta presso persone fisiche, senza l'utilizzo della modulistica e delle procedure di cui sopra, è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul segnalante (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica) che potranno, nel caso, essere utili durante la fase di gestione tecnica, per reperire maggiori informazioni circa la violazione segnalata. Ove possibile è sempre opportuno invitare il segnalante a rendere la propria dichiarazione per iscritto., anche in forma libera. In questa fase è opportuno non raccogliere dati personali appartenenti alle categorie particolari di cui all'art. 9 del GDPR, se non strettamente necessari.

Qualora la segnalazione pervenisse per **posta elettronica** certificata od ordinaria su una casella qualsiasi (istituzionale o meno) non è sufficiente il solo inoltro del messaggio ma occorre, comunque, seguire le modalità di seguito riportate. Allo stesso modo, ove la segnalazione pervenisse su **supporto cartaceo** non è sufficiente la sua mera registrazione al protocollo, occorrendo comunque che si segua la procedura di cui *infra*. Questo per accertarsi che la segnalazione non passi inosservata.

Anche le **segnalazioni anonime e/o verbali** devono essere raccolte e trasmesse conformemente a quanto *infra*, al fine di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

La **segnalazione di una potenziale violazione di dati personali da parte del personale operante all'interno della struttura del Titolare** deve avvenire solamente utilizzando l'apposito modello ALLEGATO A "Modulo di segnalazione di una potenziale violazione di dati personali".

2.3. Il monitoraggio degli eventi di sicurezza con impatto sulla protezione dei dati personali

L'individuazione di potenziali violazioni dei dati personali può anche avvenire a seguito di **attività di monitoraggio** degli eventi che possono arrecare violazioni dei dati, sia digitale ed automatizzata che cartacea. Il monitoraggio viene effettuato tramite il controllo delle attività di trattamento definite nel Registro dei trattamenti, in particolare per quei trattamenti che sono stati valutati con rischio non trascurabile in fase di valutazione d'impatto. Le attività di monitoraggio si possono suddividere in due tipologie:

A) Il monitoraggio degli eventi generati dai sistemi ICT: tale monitoraggio include l'insieme delle attività di controllo finalizzate al rilevamento degli eventi tracciati dai sistemi informatici e dalle infrastrutture di sicurezza perimetrale che assumono carattere di rilevanza ai fini della sicurezza informatica. Tali eventi relativi ai sistemi ICT sono monitorati e gestiti dall'Amministratore di Sistema od altra figura equivalente, incaricata delle attività di gestione operativa della sicurezza ed alla quale siano assegnati i privilegi di accesso in lettura dei file di tracciamento. Di seguito sono enunciate, a titolo esemplificativo e non esaustivo, alcune categorie di eventi ICT sottoposte a monitoraggio:

- log generati dalle attività svolte con account riconducibili agli amministratori di sistema, con particolare attenzione a:
    - orari di connessione/disconnessione (log-on / log-off);
    - log afferenti alla gestione dei profili utente (es. creazione di nuove utenze, modifica dei privilegi di accesso, blocco di utenze, forzato cambio password, riassegnazione di account ad altro utente);
    - modifiche alle configurazioni di sistema;
    - escalation o tentata escalation a profili con privilegi di accesso superiori;
    - qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
    - qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dalle attività svolte da utenti ordinari, con particolare attenzione a:
    - orari di connessione/disconnessione (log-on / log-off);
    - accessi negati;
    - escalation o tentata escalation a profili con privilegi di accesso superiori;
    - qualsiasi attività svolta da remoto al di fuori dei consueti orari di lavoro;
    - qualsiasi attività bloccata dalle misure di sicurezza e controllo accessi (es. accessi negati; user-id o password errata);
- log generati dai sistemi di sicurezza
    - tentativi di violazione delle politiche di firewalling (es. drop/reject);
    - allarmi generati dai sistemi antivirus;
    - allarmi generati dai sistemi antispamming;
    - allarmi generati dai directory server/service.

B) Il monitoraggio dei luoghi fisici del trattamento e dell'archiviazione di dati personali. I luoghi fisici preposti al trattamento di informazioni personali riconducibili alle categorie di cui agli articoli 9 e 10 del GDPR, con particolare riferimento agli eventuali archivi cartacei, devono essere controllati periodicamente dal personale preposto alla vigilanza, ove previsto, ed anche con l'ausilio di eventuali dispositivi di videosorveglianza. In ogni caso sia il personale di guardiania o di vigilanza, sia il personale operativo, autorizzato all'accesso ai locali o al trattamento dei dati personali, è tenuto a comunicare tempestivamente qualsiasi evento di presunta o palese violazione della privacy come ad esempio:

- smarrimento o furto di documenti cartacei contenenti informazioni personali;
- smarrimento o furto di supporti digitali o di computer fissi o mobili contenenti dati personali;
- constatazione di effrazione o tentativi di effrazione alle porte di accesso od alle serrature di chiusura degli armadi che custodiscono documenti;
- presenza di personale non autorizzato nei locali preposti al trattamento di informazioni personali.

Qualunque constatazione di violazione o sospetta violazione, emersa in sede di monitoraggio, deve essere comunicata al Dirigente o Titolare di P.O. responsabile in ragione del servizio o settore coinvolto **entro e non oltre 4 ore** dalla sua verificazione.

2.4. Trasmissione della notizia

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza la medesima è immediatamente **trasmessa al Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto o, in caso di incertezza sulla sua**

individuazione, assenza o indisponibilità, **al DPO**, compilando il documento di cui all'ALLEGATO B "Modulo di inoltro di segnalazione di una potenziale violazione di dati personali", senza ritardo e, comunque, entro 4 ore dalla sua ricezione. Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, …) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Contestualmente alla **trasmissione documentale** della segnalazione è necessario **l'avvertimento** del destinatario anche in modo **verbale** allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Ricevuta la segnalazione, il Dirigente o Titolare di P.O. coinvolto, provvede ad **informarne prontamente e, comunque non oltre 12 ore dalla conoscenza della segnalazione, il DPO a mezzo PEC**, al seguente indirizzo: dpo@pec.gdpr.nelcomune.it

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, anche insieme ai soggetti coinvolti nell'incidente e sotto la supervisione del DPO, coordina la raccolta delle informazioni nel più breve tempo possibile ed **informa prontamente il Sindaco** o suo sostituto o delegato.

Nel caso la violazione coinvolga **più servizi o settori** del Titolare, il coordinamento dei Dirigenti o Titolari di P.O. avviene a cura del Dirigente o Titolare di P.O. competente in ragione del servizio o settore maggiormente coinvolto. In casi di incertezza o contrasto, spetta al DPO individuare la figura del coordinatore. Resta inteso che, l'utilizzo nel presente documento, della terminologia "Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto" sta ad indicare altresì la figura del coordinatore di cui sopra.

Nel caso in cui si tratti di violazione di dati contenuti in un **sistema informatico**, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto dovrà coinvolgere in tutta la procedura indicata nel presente documento anche il Responsabile dell'Area IT o un suo delegato, in caso di assenza e/o l'Amministratore di sistema.

3. Analisi e Valutazione della violazione

Questa fase si compone di tutte quelle operazioni, accertamenti e verifiche tese a supportare la valutazione dell'accaduto. Una volta stabilito che un data breach è avvenuto, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, insieme al DPO ed all'Amministratore di sistema od altra figura analoga, dovrà stabilire:

a) se esistono azioni che possano **limitare i danni** che la violazione potrebbe causare;
b) una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
c) se sia necessario **notificare** la violazione all'Autorità di controllo;
d) se sia necessario **comunicare** la violazione agli interessati.

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto e tutti i soggetti coinvolti nella gestione degli incidenti (a mero titolo esemplificativo, Amministratore di sistema od altra figura analoga, Responsabile IT, altri dirigenti o titolari di P.O., …) sono responsabili, sulla base delle rispettive competenze ed in base alla tipologia della violazione, dell'analisi tecnica dell'evento e delle azioni da mettere in atto tempestivamente per il contenimento del danno.

È importante che questa fase, nella sua prima esecuzione, **si concluda nel più breve tempo possibile, massimo 24 ore**, per consentire il primo processo decisionale di valutazione da parte del Titolare e permettergli di eseguire le eventuali notifiche e comunicazioni entro i termini previsti.

Si ricorda che l'art. 33 paragrafo n. 4 del GDPR recita "*Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*". Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni relative alla violazione di dati personali e, anche in caso queste non siano per il momento ritenute esaustive, effettuare comunque la notificazione all'Autorità di controllo.

3.1. Analisi tecnica dell'evento

Per identificare le modalità di gestione di una violazione e gli eventuali obblighi di notifica e/o di comunicazione, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto (con il supporto dell'Amministratore di sistema od altra figura) effettua, anzitutto, un'analisi tecnica della segnalazione, all'interno della quale, **dovrà essere accertato se la violazione segnalata sia considerabile o meno un data breach**.

Questa fase dev'essere condotta con **estrema celerità**, anche se non si riescono ad individuare tutti gli elementi utili, ad eccezione della determinazione della sussistenza della violazione. Le verifiche potranno eventualmente proseguire anche dopo una prima valutazione. Inoltre l'Autorità di controllo o gli alti organi nazionali (polizia, magistratura, CERT-PA ecc, …) potrebbero richiedere o ritenere necessari approfondimenti. Dunque, l'incompletezza delle informazioni, così come la necessità di approfondimenti potrebbero rendere necessario ripetere la fase anche più volte.

Nessuna segnalazione deve concludersi in questa fase unicamente sulla base di un **giudizio di inaffidabilità del segnalante**: occorrerà comunque appurare se la violazione si è effettivamente verificata. Parimenti, nessuna segnalazione che sia relativa unicamente ad operazioni svolte con strumenti informatici potrà concludersi durante l'analisi tecnica per il solo fatto che non sussiste una violazione di dati personali, in quanto potrebbe in ogni caso rendersi necessario informare altre Autorità competenti (ad es., CERT-PA).

Si dovranno, ove possibile, rilevare:

- la causa e la natura del disservizio o della rottura;
- valutazione delle eventuali vulnerabilità collegate con l'incidente ed individuazione delle azioni di mitigazione delle vulnerabilità individuate;
- l'esistenza di misure adottate precedentemente all'evento per contrastare il rischio;
- valutazione dei tempi e modalità di riparazione e ripristino dei sistemi, dell'infrastruttura e delle configurazioni;
- verifica dei sistemi recuperati;
- l'eventualità di perdita di dati durante il ripristino, la loro tipologia, se i dati sono reperibili in altre aree dei sistemi o presso terzi e le tempistiche per il recupero.

3.2. Valutazione della violazione al fine del rispetto degli obblighi di notifica e comunicazione

Esaurita l'analisi tecnica, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, dovrà svolgere tutte le operazioni necessarie a raccogliere gli elementi per l'ulteriore valutazione dell'evento, ai fini dell'adempimento degli obblighi imposti dal GDPR. Più precisamente il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto (con il supporto dell'Amministratore di sistema od altra figura) dovrà **accertare che i dati oggetto di violazione siano dati personali nonché la probabilità o meno che l'evento abbia comportato dei**

rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato. Nello specifico verrà effettuato:
a) il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr. Linee Guida sulla notifica delle Violazioni dei dati personali ai sensi del Regolamento UE 2016/79 WP 250 Par. 1. punto 2);
b) l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
c) l'identificazione degli interessati;
d) il contenimento del danno;

Tutte le operazioni effettuate devono essere tracciate e riconducibili a specifiche persone.

3.2.1. valutazione dell'impatto sugli interessati

Nella fase di valutazione, sulla base delle informazioni rinvenute, occorre innanzitutto stabilire se nell'incidente sono coinvolti i **dati personali**. In caso di risposta positiva occorre valutare l'impatto sugli interessati:

a) ove si tratta di una *violazione di riservatezza* occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in uso rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note);
b) in caso di *perdita di integrità o disponibilità* di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

I fattori da considerare nella valutazione del rischio per i diritti e le libertà delle persone fisiche interessate dalla violazione possono così essere esemplificati (trattasi di elencazione non esaustiva né vincolante):

FATTORE	OSSERVAZIONI
Aspetti **generali**	Valutazione della gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e della probabilità che tale impatto si verifichi. Se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore sarà anche il rischio
Tipo di **violazione**	distruzione, modifica, perdita, divulgazione (ad esempio, una violazione della riservatezza può avere conseguenze diverse rispetto ad una violazione in cui i dati siano stati persi e non più disponibili)
Natura, carattere sensibile e volume dei **dati** personali	Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato a malintenzionati. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate. Inoltre, di norma, una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.

	Una violazione che interessi grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.
Facilità di **identificazione** delle persone fisiche	facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali
Gravità delle **conseguenze** per le persone fisiche	danno potenziale alle persone fisiche che potrebbe derivare dalla violazione comprese le categorie degli interessati e dei dati personali coinvolti e la permanenza a lungo termine delle conseguenze del danno (furto di identità, danni fisici, disagio psicologico, danni reputazionali). Il fatto che si sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.
Caratteristiche particolari del **Titolare**	La natura e il ruolo del Titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione
Caratteristiche particolari dell'**interessato**	Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili (minori, anziani, pazienti, …), queste ultime potrebbero essere esposte a un rischio maggiore di danni
Numero di persone fisiche interessate	Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi.

Qualora il numero degli interessati dalla violazione, o potenziali interessati, sia ridotto e questi siano identificabili è opportuno stilare degli elenchi da utilizzare nel caso in cui il sia necessario inviare loro delle comunicazioni personalizzate.

3.2.2. valutazione della gravità del rischio

La gravità di una violazione di dati personali è definita come la **stima dell'entità del potenziale impatto sulle persone fisiche derivante dalla violazione medesima**. Tale valutazione di impatto permette di stabilire la necessità di notifica della violazione all'Autorità di controllo, in particolare se probabile un rischio per la libertà e diritti delle persone fisiche, e la comunicazione anche agli interessati, nel caso in cui tale rischio sia elevato.

La violazione dei dati può comportare elevati **rischi per i diritti e le libertà delle persone** fisiche. I rischi principali sono connessi alla possibilità che l'interessato subisca danni fisici, materiali o immateriali connessi perdita del controllo dei dati personali quali, ad esempio:

a) limitazione dei diritti;
b) discriminazione;
c) furto o usurpazione di identità;
d) perdite finanziarie;
e) decifratura non autorizzata della pseudonimizzazione;
f) pregiudizio alla reputazione;
g) perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari);
h) qualsiasi altro danno economico o sociale, significativo.

Le linee guida elaborate dal Gruppo ex art. 29 suggeriscono di ritenere, il rischio elevato per i diritti e le libertà delle persone fisiche, quantomeno come "probabile" quando la violazione riguardi dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza.

I considerando 75 e 76 del GDPR suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la **probabilità** quanto la **gravità** del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva:
- **gravità**: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- **probabilità**: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

le **tabelle** che seguono rappresentano visivamente quanto deve essere oggetto di valutazione

GRAVITÀ	**Impatto della violazione sui diritti e le libertà delle persone coinvolte**
	BASSO: gli individui possono andare incontro a *disagi minori*, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);
	MEDIO: gli individui possono andare incontro a *significativi disagi*, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.);
	ALTO: gli individui possono andare incontro a *conseguenze significative*, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.);
	MOLTO ALTO: gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)
PROBABILITÀ	**Possibilità che si verifichino uno o più eventi temuti**
	BASSA: è improbabile che la minaccia si materializzi
	MEDIA: c'è una ragionevole possibilità che la minaccia si materializzi
	ALTA: la minaccia potrebbe materializzarsi
	MOLTO ALTA: l'evento temuto si è realizzato

PROBABILITA'	**GRAVITA'**			
	MA	A	M	B
MA				
A				
M				
B				

Tuttavia va considerato che nel caso di una violazione di dati personali effettiva, l'evento si è già verificato, quindi l'attenzione si concentra **esclusivamente sul rischio** risultante dell'impatto di tale violazione sulle persone fisiche.

	Descrizione	Notifica all'Autorità	Comunicazione agli interessati
Rischio	BASSO: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	MEDIO: possibile pregiudizio sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	NO
	ALTO e MOLTO ALTO: pregiudizio certo sui diritti e sulle libertà degli interessati e sulla sicurezza dei dati personali coinvolti	SI	SI

Sulla base degli elementi di cui sopra, acquisito un ragionevole grado di certezza del fatto che sia avvenuto un incidente per la sicurezza delle informazioni che abbia compromesso dati personali, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto:
a) stima la gravità e la probabilità della violazione e classifica il rischio;
b) documenta la decisione presa a seguito della valutazione del rischio nel Registro delle violazioni.
Gli elementi a supporto del procedimento e degli esiti della valutazione del rischio sono documentati utilizzando il modello ALLEGATO C - "Modulo di valutazione del rischio connesso al violazione di dati personali" e tale documentazione è conservata in apposito archivio.

Scenari al termine della fase valutativa

A) ove i **rischi per gli interessati siano trascurabili**, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. Una eventuale fase di miglioramento può essere innescata per incrementare ulteriormente la protezione del dato, ma non è obbligatoria.

L'art. 33 paragrafo 1 chiarisce, infatti, che **non vi è obbligo di notifica della violazione quando è "*improbabile*" che questa comporti un rischio per i diritti e le libertà delle persone fisiche**: un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e **il rischio dovrebbe essere rivalutato**.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

B) nel caso che i **rischi per l'interessato non siano trascurabili** occorre procedere alla notificazione all'Autorità di controllo sulla scorta delle indicazioni di cui al successivo paragrafo 4. In questo caso, la procedura deve dare le giuste priorità agli sforzi di contenimento dell'incidente. In ogni caso va condotta una fase di miglioramento.

C) qualora i **rischi per l'interessato siano elevati** occorre procedere alla comunicazione della violazione alle persone fisiche interessate, di cui al successivo paragrafo 6, in aggiunta alla notificazione all'Autorità di controllo, salvo che quest'ultima richieda di omettere o ritardare la comunicazione stessa. In ogni caso va condotta una fase di miglioramento.

3.3. Valutazioni supplementari

Ulteriori analisi dell'accaduto possono rendersi necessarie qualora:

a) il Titolare ritenga necessario un approfondimento finalizzato ad es. all'integrazione di una precedente notifica all'Autorità di controllo;
b) l'Autorità di controllo, gli organi di polizia o la magistratura ritengano necessarie informazioni aggiuntive od approfondimenti di informazioni già fornite;
c) durante una delle fasi del processo di gestione del data breach siano emerse situazioni non approfondibili o non sia stato possibile coinvolgere pienamente responsabili esterni o questi non abbiano comunicato in tempo utile i risultati delle loro analisi.

L'analisi supplementare può essere attivata più volte per la stessa violazione, secondo necessità.

4. Notifica della violazione dei dati personali all'Autorità di controllo

4.1. Quando effettuare la notificazione

La normativa prevede che, **non appena si venga a conoscenza di una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone coinvolte**, sia obbligatorio effettuare la notifica all'Autorità. Pertanto, la notifica all'Autorità dell'avvenuta violazione non è un processo automatico, essendo subordinata alla valutazione del rischio per gli interessati che spetta al Titolare.

Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, versione emendata e adottata il 6 febbraio 2018, chiariscono quando il Titolare del trattamento possa considerarsi "*a conoscenza*" di una violazione.

Il Gruppo di lavoro europeo ritiene che il Titolare del trattamento debba considerarsi "*a conoscenza*" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che abbia portato alla compromissione dei dati personali. Tuttavia, va considerato che il regolamento impone al Titolare del trattamento di attuare tutte le misure tecniche ed organizzative di protezione adeguate a stabilire immediatamente se si sia verificata una violazione ed informare tempestivamente l'Autorità di controllo e gli interessati. Il Gruppo ex art. 29 afferma inoltre che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato.

Il Titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva, in modo da poter adottare le misure appropriate.

Il momento esatto in cui il Titolare del trattamento può considerarsi "*a conoscenza*" di una particolare violazione dipenderà dalle circostanze della violazione.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva notificazione all'Autorità di controllo.

Vi sono casi, tuttavia, in cui è possibile definire se l'evento costituisca una violazione ai sensi del GDPR solo al termine della fase di valutazione. In questo caso la decorrenza della tempistica per la notificazione all'Autorità di controllo è, comunque, dal momento della constatazione.

Qualora i contorni della violazione non siano chiari si può attendere fino ad **un massimo di 72 ore** prima di effettuare una notifica (Non si tratta di un termine puramente indicativo ma **categorico**, il cui mancato rispetto se non adeguatamente motivato, integra una situazione sanzionabile). Alla scadenza delle 72 ore è comunque necessario fare una comunicazione significando che questa è l'inizio di una notifica in fasi. Il GDPR consente infatti una notifica per fasi, a condizione che il Titolare indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1.

In ogni caso, 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.

Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, essa va corredata dei **motivi del ritardo**. Si suggerisce in ogni caso di procedere comunque all'effettuazione della notifica entro il termine, fatto salvo quanto *infra* con riferimento alla notifica per fasi.

Si ricorda che **l'obbligo di effettuare la notifica all'Autorità di controllo, ricorre solo quando:**

a) l'Ente è Titolare del trattamento di dati coinvolti nell'incidente;
b) l'Ente è Contitolare del trattamento con delega alla notifica;
c) l'Ente è Responsabile del trattamento con delega alla notifica. L'Ente non ha il dovere di notificare la violazione all'Autorità di controllo quando agisce come Responsabile del trattamento per conto di altro Titolare, senza delega alla notifica. In questo caso l'Ente deve comunicare al Titolare del trattamento la sospetta violazione e/o l'incidente di sicurezza riguardante dati personali, nei modi convenuti, con la massima tempestività e mettersi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

4.2. Come effettuare la notificazione

Per le violazioni identificate, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto redige il **documento di notifica della violazione, compilando l'apposito modello presente sul sito e secondo le istruzioni dell'Autorità di controllo**, **previa consultazione ed in collaborazione con il DPO**. Si allega al presente documento, a mero titolo esemplificativo, il modello di notificazione approvato dall'Autorità di controllo italiana con provvedimento del 31 luglio 2019, fermo restando che è preciso onere del Dirigente o Titolare di P.O. competente ad effettuare la notifica, verificarne l'attualità, sia in termini di contenuto che di procedura (ALLEGATO D – "Violazione di dati personali – modello di notifica al Garante").

Si può valutare di effettuare una **notifica cumulativa** se una stessa compromissione abbia riguardato la stessa tipologia di dati con le stesse modalità e gli stessi siano stati violati in un lasso di tempo relativamente breve. Ove si verifichino diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale.

Si ricorda che è altresì ammessa una **notificazione "per fasi"** allorquando non si disponga di tutte le informazioni necessarie su una violazione, entro 72 ore dal momento in cui se ne è venuti a conoscenza. In tali casi, all'atto della prima notifica all'Autorità di controllo, il Titolare informa quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo.

4.3. Eventuali ulteriori notificazioni (o denunce)

Effettuata la notifica in favore dell'Autorità di controllo, è poi opportuno verificare se:
1) sia necessaria una *seconda notifica*, più approfondita, quale conseguenza di un'analisi tecnica supplementare ovvero di elementi ed informazioni successivamente acquisiti. È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostrasse che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il Titolare del trattamento può informarne l'Autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'Autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione;
2) sia necessario effettuare una comunicazione alle *forze dell'ordine* od all'*Autorità giudiziaria* competente.

5. Recepimento della eventuale risposta dell'Autorità di controllo

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto dispone con sollecitudine ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dall'Autorità di controllo. Parimenti provvede a seguito del ricevimento di indicazioni od ordini relativamente alla comunicazione da effettuare o non effettuare in favore degli interessati.

6. Comunicazione della violazione dei dati personali all'interessato

Contestualmente alla decisione di notificare all'Autorità di controllo, occorre valutare se è il caso di informare anche gli interessati. Il modello di notificazione predisposto dall'Autorità di controllo richiede infatti specifica indicazione e descrizione delle circostanze e valutazioni che hanno condotto ad effettuare o non effettuare la comunicazione agli interessati.

A tale scopo va valutata la gravità del rischio per gli interessati ed i loro diritti.

Nel caso di accertamento di una **violazione di dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, come valutato secondo quanto indicato al precedente paragrafo 3, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio (**la soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica all'Autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati**, il che li protegge da inutili disturbi arrecati dalla notifica). In tale ipotesi occorre quindi valutare:

a) la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv);
b) le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi;
c) le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo ex art. 29 in materia di trasparenza (WP 260), aggiornate in base alle previsioni del Regolamento (UE) 2016/679.

Anche di questa fase deve essere prodotta e conservata appropriata documentazione.

6.1. Quando effettuare la comunicazione

Il GDPR 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**. 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.

Da notare inoltre che il Considerando 86 suggerisce che "T*ali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge*". Parallelamente, il Considerando 88 indica che la notifica di una violazione dovrebbe tenere "*conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali*".

Conseguentemente si ritiene suggeribile, **nel contesto della notifica all'Autorità di controllo, formulare espressa richiesta di indicazioni in tal senso** (non soltanto se provvedere alla comunicazione o no, ma anche quale contenuto della comunicazione e quali canali suggeriti).

6.2. Come effettuare la comunicazione

Per la comunicazione, è possibile identificare **uno o più canali di comunicazione**, a seconda delle circostanze, quali email, SMS, posta, comunicati pubblicitari, banner o notifiche su siti web, scegliendo il canale che massimizza la probabilità che tutti gli interessati siano raggiunti dal messaggio. Caso per caso, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto, dovrà **sempre privilegiare la modalità di comunicazione diretta** con i soggetti interessati (quali e- mail, SMS o messaggi diretti).

Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori.

Non deve essere utilizzato il canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il Titolare del trattamento.

Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Ove non si abbia la possibilità di comunicare una violazione all'interessato perché non si disponga di dati sufficienti per contattarlo, questi sarà informato non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce le informazioni necessarie per essere contattato).

6.3. Quali informazioni comunicare

Sebbene sia preferibile utilizzare il modello ALLEGATO E – "Comunicazione all'interessato della violazione dei dati personali", la comunicazione in altra forma deve comunque contenere, ai sensi dell'art. 34, le seguenti **informazioni**:

1) il nome ed i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
2) una descrizione della natura della violazione;
3) una descrizione delle probabili conseguenze della violazione dei dati personali;
4) una descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
5) se l'Autorità di controllo abbia suggerito od ordinato misure di gestione della violazione e sull'attenuazione del suo impatto;
6) eventuali indicazioni al destinatario sul modo in cui proteggersi dalle possibili conseguenze negative della violazione

6.4. Quando non effettuare la comunicazione

Secondo quanto previsto dal paragrafo 3 dell'art. 34 del GDPR, **la comunicazione non è richiesta** se è soddisfatta una delle seguenti condizioni:

a) 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, quali la cifratura;
b) il Titolare del trattamento ha, successivamente alla violazione, adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o ad una misura simile, ad esempio rendere disponibili le informazioni a richiesta, tramite la quale gli interessati siano informati con analoga efficacia.

Ove si decida di non comunicare una violazione all'interessato, si ricordi che l'articolo 34, paragrafo 4, prevede che l'Autorità di controllo possa richiedere che lo si faccia ugualmente, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato, fatto naturalmente salvo l'esercizio dei poteri e delle sanzioni a propria disposizione.

7. Altre segnalazioni

Il Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto dovrà verificare la necessità di informare altri organi quali, a mero titolo esemplificativo:
- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Al Gestore di Identità Digitale e Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

Ciascuna segnalazione dovrà avvenire nel rispetto delle procedure ed utilizzando la modulistica all'uopo eventualmente predisposta da ciascuna Autorità di vigilanza o controllo.

8. Documentazione della violazione

L'art. 33 paragrafo n. 5 del DGPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, anche se non notificate all'Autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze ed i provvedimenti adottati al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Si ricorda che la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'Autorità di controllo dei suoi poteri ai sensi dell'articolo 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83.

Il Titolare ha, quindi, stabilito di documentare gli incidenti di sicurezza e le violazioni di dati personali come segue:

a) adozione, di un registro "interno" delle (sole) violazioni di dati personali, intendendosi per tale un inventario aggiornato delle violazioni contenente tutte le informazioni necessarie a chiarire le circostanze nelle quali si sono verificate, le conseguenze che le stesse hanno avuto ed i provvedimenti adottati per porvi rimedio. Esso tiene traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione;
b) adozione di modulistica, anche a rilevanza esterna, idonea a documentare gli incidenti di sicurezza e le violazioni di dati personali.

Il GDPR non specifica un **periodo di conservazione** per tale documentazione. Essa sarà dunque conservata nel rispetto dei termini e delle norme di legge sulla conservazione della documentazione amministrativa, anche in considerazione del fatto che la conservazione è, in conformità dell'articolo 33, paragrafo 5, nella misura in cui il Titolare potrà essere chiamato a fornire prove all'Autorità di controllo in merito al rispetto di tale articolo oppure, più in generale, del principio di responsabilizzazione.

8.1. il Registro delle violazioni

Il DPO è responsabile della tenuta e dell'aggiornamento del Registro delle violazioni.

Poiché il GDPR non specifica quale debba essere il **contenuto** e la **forma** del Registro delle violazioni né il tipo di supporto sul quale debba essere redatto, per estensione delle disposizioni contenute nell'art. n. 30 del GDPR (relativamente al registro delle attività di trattamento e registro delle categorie di attività di trattamento) si presume che tale registro possa anche essere **di tipo elettronico**. Il Titolare ha quindi deciso di adottarlo in tale forma.

L'inventario dovrà essere accompagnato da idonee misure di sicurezza atte a garantire **l'integrità e l'immodificabilità dei dati in esso registrati** quali ad esempio la protocollazione, la stampa, …).

I dati presenti nel registro sono trattati nel rispetto del **principio di minimizzazione** e secondo le misure necessarie per mitigare i rischi di violazione dei dati personali.

Ogni segnalazione, comprese quelle **non veritiere**, deve essere soggetta a registrazione nel registro delle violazioni.

Per ogni violazione di cui sia accertata l'esistenza, anche se non notificata all'Autorità di controllo e non comunicata agli interessati, il registro ripoterà:

(con riferimento alla segnalazione)
- numerazione progressiva;
- data ed ora della segnalazione;
- dati identificative del segnalante;
- unità organizzativa coinvolta;
- organi informati;

(con riferimento alla violazione)
- luogo violazione;
- modalità della violazione;
- descrizione dei sistemi, apparati, reti, banche dati oggetto di data breach;
- la natura della violazione dei dati personali;
- altri elementi utili alla descrizione della violazione;

(con riferimento agli interessati)
- indicazione delle categorie di interessati coinvolti;
- indicazione del numero approssimativo di interessati coinvolti;

(con riferimento ai dati personali coinvolti)
- indicazione delle categorie dei dati personali coinvolte;
- indicazione del numero approssimativo di dati personali coinvolti;

(con riferimento alle conseguenze)
- descrizione delle previste (o verificate) conseguenze;

(con riferimento ai rimedi)
- indicazione delle misure adottate per porre rimedio alla violazione;
- indicazione delle misure proposte per porre rimedio alla violazione;

(con riferimento all'attenuazione delle conseguenze)
- indicazione delle misure adottate per attenuare i possibili effetti negativi;
- indicazione delle misure proposte per attenuare i possibili effetti negativi;
(con riferimento ai tempi di ripristino)
- indicazione della tempistica stimata
(con riferimento alla notifica all'Autorità di controllo)
- indicazione se ricorre il rischio per i diritti e le libertà delle persone fisiche;
- effettuazione o meno della notificazione;
- ragioni della omessa notificazione all'Autorità di controllo;
(con riferimento alla comunicazione agli interessati)
- indicazione se ricorre rischio elevato per i diritti e le libertà delle persone fisiche e le relative ragioni;
- effettuazione o meno della comunicazione;
- ragioni della omessa comunicazione agli interessati;

8.2. Altri documenti ed informazioni

Ad integrazione di quanto riportato nel registro, il Dirigente o Titolare di P.O. competente in ragione del servizio o settore competente raccoglie e **conserva tutti i documenti** relativi ad ogni violazione, compresi quelli inerenti alle circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

9. Fase di miglioramento

Una volta contenuti i rischi o le conseguenze della violazione ed adempiuto agli obblighi di notificazione e comunicazione previsti dal GDPR occorre dedicare attenzione alla fase di miglioramento delle misure tecniche ed organizzative in uso presso il Titolare, al fine di evitare il ripetersi di incidenti analoghi.
Le azioni previste in questa fase sono:

- l'analisi della relazione dettagliata sull'incidente;
- la reiterazione del processo di Gestione del rischio informativo;
- l'eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza);
- l'individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- la revisione del sistema di gestione della protezione dei dati;
- la revisione con cadenza almeno annuale della procedura descritta nel presente documento.

10. Fattispecie di contitolarità e responsabilità del trattamento

Sulla scorta della previsione di cui all'articolo 26 del GDPR, laddove il Titolare si trovasse ad operare unitamente ad altri soggetti in fattispecie classificabili in termini di **contitolarità del trattamento** dei dati personali, il relativo accordo o convenzione dovrà contenere espressa determinazione di chi assumerà il comando o sarà responsabile del rispetto degli obblighi di cui agli articoli 33 e 34 del medesimo GDPR.

Sulla scorta della previsione di cui all'articolo 28 del GDPR, laddove il Titolare necessiti che il trattamento di dati personali venga effettuato per suo conto ad opera di altri soggetti qualificabili come **responsabili del trattamento**, il contratto od altro atto giuridico che vincoli tale soggetto al

Titolare dovrà contenere espressa previsione che il responsabile assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

In particolare è necessario prevedere che qualora il responsabile del trattamento venga a conoscenza di una violazione di dati personali che sta trattando per conto del Titolare, provveda a notificargliela senza ingiustificato ritardo e, comunque, entro e non oltre 24 ore dalla scoperta, senza effettuare alcuna valutazione circa la probabilità di rischio derivante dalla violazione stessa; spetta infatti soltanto al Titolare effettuare tale valutazione nel momento in cui ne verrà a conoscenza.

FONTI

Nella redazione del presente documento si è tenuto conto delle indicazioni e delle disposizioni:

1) del 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 - RGDP);
2) del Decreto legislativo 30 giugno 2003, numero 196, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal Decreto legislativo 10 agosto 2018, numero 101;
3) del Gruppo "Articolo 29" all'interno delle Linee-guida in materia di notifica delle violazioni di dati personali, approvate, in via definitiva, il 6 febbraio 2018;
4) del Garante per la protezione dei dati personali nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali";
5) del Garante per la protezione dei dati personali nel Provvedimento 30 luglio 2019 "sulla notifica delle violazioni dei dati personali" (doc. web n. 9126951);

Il presente documento è soggetto a integrazioni e modifiche alla luce dell'evoluzione normativa italiana e comunitaria, della riflessione che si svilupperà a livello nazionale ed europeo, nonché delle prassi che saranno, di volta in volta, riscontrate all'interno della struttura del Titolare.

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)

Considerando (75)

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare 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, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Considerando (76)

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Considerando (85)

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.

Considerando (86)

Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

Considerando (87)

È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

Considerando (88)

Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Articolo 4 - definizioni

Ai fini del presente regolamento s'intende per: (…)
12) «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

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. 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.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 - Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. 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).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) 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, quali la cifratura;
b) 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 di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

ALLEGATO A

MODULO DI SEGNALAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

(Il presente modello non è vincolante, ben potendo la segnalazione essere fornita in forma libera)

Il presente modulo va compilato da chiunque constati un effettivo o potenziale incidente di sicurezza che possa comportare una violazione di dati personali, al fine di consentire al Titolare del trattamento la valutazione e gestione dell'incidente stesso e, in caso di violazione accertata, di notifica al Garante e di comunicazione agli interessati.

Il modulo, compilato in ogni sua parte e debitamente sottoscritto, dev'essere consegnato al più presto con le seguenti alternative modalità:

a) consegna a mani presso l'Ufficio protocollo;
b) consegna via email all'indirizzo:
c) consegna via PEC all'indirizzo:

Ove al momento della rilevazione dell'incidente di sicurezza non sia possibile una descrizione particolareggiata dell'evento, è comunque essenziale procedere immediatamente alla sua segnalazione, anche con informazioni incomplete. Sarà cura del Titolare del trattamento accertare quanto necessario, anche contattando il segnalante ai recapiti forniti.

Dati identificativi del SEGNALANTE ed informazioni di contatto					
Cognome					
Nome					
Documento di identità N.		rilasciato da		scadenza	
Servizio o settore di appartenenza	(questo campo dev'essere compilato solo in caso di segnalazione ad opera di un dipendente/collaboratore del Titolare. In tale ipotesi non vanno indicati i riferimenti al documento di identità)				
Telefono		cellulare			
E-mail		PEC			

Informazioni sulla VIOLAZIONE	
Quando mi sono accorto della violazione?	
Come mi sono accorto della violazione?	

Breve **descrizione** della violazione	

Quali strutture sono coinvolte (locali, archivi, web, dispositivi elettronici, etc)?	

Quale tipo di violazione?	In caso di perdita di **confidenzialità**	
		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)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Quali dati personali sono coinvolti?		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, descrivere:

Quali potenziali effetti negativi per le persone coinvolte?		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)

E' già stata fatta una segnalazione al Garante della privacy?	(in caso affermativo, allegare la relativa documentazione)
E' già stata fatta una segnalazione alle forze dell'ordine o all'Autorità giudiziaria?	(in caso affermativo, allegare la relativa documentazione)

Documentazione che si allega	(diversa da quella indicata al punto precedente. Indicare anche eventuali fogli aggiuntivi necessari per ragioni di spazio)	
	X	Fotocopia del documento di identità (solo per soggetti esterni al Titolare)
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di Frossasco, in qualità di Titolare del trattamento (con sede in Frossasco, Via S. De' Vitis n. 10; Email: comune.frossasco@comunefrossasco.it; PEC: comune.frossasco.to@legalmail.it; Telefono: 0121352104), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, 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 e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. 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 Titolare 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 al Garante per la protezione dei dati personali, all'Autorità giudiziaria e 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 Titolare, 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 ai seguenti indirizzi (e-mail comune.frossasco@gdpr.nelcomune.it, PEC dpo@pec.gdpr.nelcomune.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. L'informativa sul trattamento dei dati è reperibile sulla pagina internet istituzionale dell'ente raggiungibile al link: https://comunefrossasco.it/.

ALLEGATO B

MODULO DI INOLTRO DI SEGNALAZIONE DI UNA POTENZIALE VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

Ricevuta, da chiunque ed in qualunque modo, la segnalazione di un potenziale od effettivo incidente sulla sicurezza la medesima è immediatamente **trasmessa al Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto o, in caso di incertezza sulla sua individuazione, assenza o indisponibilità**, **al DPO**, esclusivamente utilizzando il presente modulo, senza ritardo e, comunque, entro 4 ore dalla conoscenza dei fatti.

Il modello di segnalazione, debitamente compilato e sottoscritto, dovrà essere consegnato con le modalità più idonee (posta elettronica, consegna a mani, …) a garantirne la pronta e puntuale conoscenza in quanto permetterà di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso e, ciò, al fine di stabilire se si sia effettivamente verificata un'ipotesi di data breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto. Ove possibile, devono essere in questo modello integrate le informazioni richieste e non già fornite dal segnalante.

Contestualmente alla comunicazione scritta della segnalazione è necessario l'**avvertimento** del destinatario **anche in modo verbale** allo scopo di assicurarsi che quanto comunicato non passi inosservato.

Dati identificativi del soggetto che INOLTRA			
Cognome			
Nome			
Servizio o settore di appartenenza			
E-mail		Telefono	

Dati identificativi del soggetto DESTINATARIO				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail		Telefono		
Modalità di inoltro segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

Informazioni sulla SEGNALAZIONE	
Da chi ho ricevuto la segnalazione?	
Quando ho ricevuto la segnalazione?	
Come ho ricevuto la segnalazione?	
(eventuali) ulteriori **informazioni** ricevute oralmente dal segnalante	

(eventuali) **Osservazioni** rispetto al contenuto della segnalazione ricevuta (anche in punto **descrizione** della violazione)	

ATTIVITA' DI RILEVAZIONE INTERNA

Competenza in merito alla segnalazione ricevuta (anche di più uffici)		Servizio o settore che l'ha ricevuta
		Altro/i servizio/i o settore/i (specificare)

Presenza di **Contitolari** del trattamento		NO
		SI (per ciascuno specificare denominazione e tipologia servizio affidato)

Presenza di **Responsabili** del trattamento		NO
		SI (per ciascuno specificare denominazione e tipologia servizio affidato)

descrizione delle **strutture** fisiche e tecnologiche coinvolte	

istruttoria condotta con indicazione delle relative evidenze	

Quale tipo di violazione?	In caso di perdita di **confidenzialità**	
		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)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Possibili **cause** della violazione		Azione intenzionale interna
		Azione accidentale interna
		Azione intenzionale esterna
		Azione accidentale esterna
		Sconosciuta
		Altro (specificare)

Volume (anche approssimativo) dei **soggetti** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Volume (anche approssimativo) dei **dati** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali dati personali sono coinvolti?		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, descrivere:

Quali potenziali effetti negativi per le persone coinvolte?		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)

Stima della **Gravità** della violazione		Trascurabile
		Basso
		Medio
		Alto
	Motivazione:	

AZIONI INTRAPRESE O SUGGERITE

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

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

ALLEGATI E NOTE

Documentazione che si allega	X	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di Frossasco, in qualità di Titolare del trattamento (con sede in Frossasco, Via S. De' Vitis n. 10; Email: comune.frossasco@comunefrossasco.it; PEC: comune.frossasco.to@legalmail.it; Telefono: 0121352104), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, 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 e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. 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 Titolare 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 al Garante per la protezione dei dati personali, all'Autorità giudiziaria e 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 Titolare, 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 ai seguenti indirizzi (e-mail comune.frossasco@gdpr.nelcomune.it, PEC dpo@pec.gdpr.nelcomune.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. L'informativa sul trattamento dei dati è reperibile sulla pagina internet istituzionale dell'ente raggiungibile al link: https://comunefrossasco.it/.

ALLEGATO C

MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO ALLA VIOLAZIONE DI DATI PERSONALI

ai sensi dell'art. 33 del Regolamento Generale sulla Protezione dei Dati

Ricevuta la documentazione relativa alla segnalazione di una potenziale violazione di dati personali ed effettuata la prescritta analisi tecnica, il **Dirigente o Titolare di P.O. competente in ragione del servizio o settore coinvolto** deve stabilire la probabilità o meno che l'evento abbia comportato dei rischi per i diritti e la libertà delle persone e la gravità del rischio così identificato.

Il modello, debitamente compilato e sottoscritto, dovrà essere conservato a documentazione delle valutazioni e decisioni prese.

Dati identificativi del soggetto che effettua l'ANALISI				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Ricevuta la segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

Dati identificativi del soggetto che effettua la VALUTAZIONE (se diverso)				
Cognome				
Nome				
Servizio o settore di appartenenza				
E-mail			Telefono	
Ricevuta la segnalazione		A mani	data e ora	
		E-mail	data e ora	
		Avviso orale	data e ora	
		Altro (specificare)		

ATTIVITA' DI ANALISI

Osservazioni rispetto al contenuto della segnalazione ricevuta (anche in punto **descrizione** della violazione)	

Data della violazione		il	
		Dal	(violazione ancora in corso)
		Dal	Al
		In un tempo non ancora determinato (specificare)	

Natura della violazione		**Riguarda dati personali**		**Non Riguarda dati personali**
		Perdita di confidenzialità		
		Perdita di integrità		
		Perdita di disponibilità		

Competenza in merito alla segnalazione ricevuta (anche di più uffici)		Servizio o settore che l'ha ricevuta
		Altro/i servizio/i o settore/i (specificare)

Presenza di **Contitolari** del trattamento		NO
		SI

Presenza di **Responsabili** del trattamento		NO
		SI

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

Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti (**in essere** al momento della violazione)	

istruttoria condotta con indicazione delle relative evidenze	

Possibili **cause** della violazione		Azione intenzionale interna
		Azione accidentale interna
		Azione intenzionale esterna
		Azione accidentale esterna
		Sconosciuta
		Altro (specificare)

Possibili conseguenze della violazione?	In caso di perdita di **confidenzialità**	
		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)
	In caso di perdita di **integrità**	
		I dati sono stati modificati e resi inconsistenti
		I dati sono stati modificati mantenendo la consistenza
		Altro (specificare)
	In caso di perdita di **disponibilità**	
		Mancato accesso a servizi
		Malfunzionamento e difficoltà nell'utilizzo di servizi
		Altro (specificare)

Volume (anche approssimativo) dei **soggetti** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali soggetti coinvolti?		Il segnalante
		Cittadini
		Dipendenti e titolari di incarichi di collaborazione
		Utenti di servizi pubblici
		Soggetti che ricoprono cariche istituzionali
		Beneficiari o assistiti
		Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
		Minori
		Categorie ancora non determinate
		Altro (specificare)

Sono coinvolti cittadini di altri paesi?	(in caso affermativo, indicare i paesi di riferimento)

Volume (anche approssimativo) dei **dati** coinvolti		Numero
		Circa numero
		Numero (ancora) non definito (specificare)

Quali dati personali sono coinvolti?		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, descrivere:

Quali potenziali **effetti negativi** per le persone coinvolte?		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)

Stima della **Gravità** della violazione		Trascurabile (no notifica, né comunicazione)
		Basso (no notifica, né comunicazione)
		Medio (si notifica, no comunicazione)
		Alto e Molto Alto (si notifica e comunicazione)
	Motivazione:	

AZIONI INTRAPRESE O SUGGERITE

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

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

ADEMPIMENTI

NOTIFICAZIONE ALL'AUTORITA' DI CONTROLLO

	Effettuata	in data e ora	

	No e non sarà effettuata in quanto si ritiene che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (specificare):

NOTIFICAZIONE O SEGNALAZIONE AD ALTRI ORGANISMI

Autorità giudiziaria			
	Effettuata	in data e ora	
	Modalità (specificare):		

Forze di polizia			
	Effettuata	in data e ora	
	Modalità (specificare):		

Altri organismi di vigilanza o controllo			
	Effettuata	in data e ora	
	Specificare l'organismo e le modalità di segnalazione		

COMUNICAZIONE AGLI INTERESSATI

	Effettuata	data e ora	
	Modalità e numero destinatari (specificare):		

	Non ancora effettuata
	in quanto tuttora in corso di valutazione
	Sarà effettuata in data da definire
	Sarà effettuata il

	No e non sarà effettuata in quanto:
	a) si ritiene che la violazione dei dati personali **non presenti un rischio elevato** per i diritti e le libertà delle persone fisiche (specificare):
	b) sono state **messe in atto le misure** tecniche ed 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 (specificare):
	c) sono state **successivamente adottate misure** atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (specificare):
	d) detta comunicazione avrebbe richiesto **sforzi sproporzionati**. Gli interessati sono stati informati con altre modalità, quali:

ALLEGATI E NOTE

Documentazione che si allega	X	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
	X	Modulo di inoltro di una segnalazione di una potenziale violazione di dati personali e relativi allegati
	X	Copia notificazione all'Autorità di controllo (eventuale)
	X	Copia comunicazione agli interessati (eventuale)
Numero dei documenti allegati		

ANNOTAZIONI

Firma

_____, lì _____ _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di Frossasco, in qualità di Titolare del trattamento (con sede in Frossasco, Via S. De' Vitis n. 10; Email: comune.frossasco@comunefrossasco.it; PEC: comune.frossasco.to@legalmail.it; Telefono: 0121352104), tratterà i dati personali conferiti con il presente modulo per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, 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 e, segnatamente, al solo scopo di acquisire ogni necessaria informazione in merito all'evento segnalato, adottare le conseguenti procedure di tutela ed effettuare le comunicazioni previste dalla normativa vigente.
Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio al fine della ricevibilità della segnalazione, ferma restando la facoltà del Titolare di istruire comunque il procedimento volto all'accertamento della violazione di dati personali. 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 Titolare 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 al Garante per la protezione dei dati personali, all'Autorità giudiziaria e 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 Titolare, 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 ai seguenti indirizzi (e-mail comune.frossasco@gdpr.nelcomune.it, PEC dpo@pec.gdpr.nelcomune.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. L'informativa sul trattamento dei dati è reperibile sulla pagina internet istituzionale dell'ente raggiungibile al link: https://comunefrossasco.it/.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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).

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

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

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: garante@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 giugno 2003, 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.

ALLEGATO E

COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI
(ai sensi del Regolamento Europeo 2016/679 sulla Protezione dei dati "GDPR")

(il presente modello costituisce una traccia liberamente modificabile e personalizzabile in considerazione delle circostanze di fatto coinvolte. Esso individua tuttavia il contenuto minimo che dev'essere in ogni caso garantito)

Gentile Signore/a,
Secondo quanto prescritto dall'articolo 34 del GDPR, La informiamo essersi verificato un accidentale ed imprevedibile evento che ha comportato una possibile violazione di dati dei Suoi dati personali. Dagli accertamenti, tuttora in corso, è emerso che l'evento si sarebbe verificato in data _____, alle ore_____ e se ne è avuta conoscenza in data_____, alle ore_____.

DESCRIZIONE DELLA NATURA DELLA VIOLAZIONE

DOVE È AVVENUTA LA VIOLAZIONE

(Specificare ove sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____
_____
_____
_____

TIPO DI VIOLAZIONE

Per esempio: 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 del Titolare 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)

_____
_____
_____
_____

DISPOSITIVO OGGETTO DI VIOLAZIONE

Per esempio: Computer; Rete; Dispositivo mobile; Strumento di backup; Documento cartaceo

_____
_____
_____
_____

TIPO DI DATI OGGETTO DI VIOLAZIONE

Per esempio: Dati anagrafici (nome, cognome, telefono, mail, CF, indirizzo…); Dati di accesso e di identificazione (username, password, ID,…); Dati personali idonei a rivelare l'origine razziale ed etnica; Dati personali idonei a rivelare le convinzioni religiose; Dati personali idonei a rivelare convinzioni filosofiche o di altro genere; Dati personali idonei a rivelare le opinioni politiche; Dati personali idonei a rivelare l'adesione a partiti; Dati personali idonei a rivelare l'adesione a sindacati; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere filosofico; Dati personali idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere sindacale; Dati personali idonei a rivelare lo stato di

salute; Dati personali idonei a rivelare la vita sessuale; Dati giudiziari; Dati genetici; Dati biometrici; Copia per immagine su supporto informatico di documenti analogici; Ancora sconosciuto.

_____
_____
_____
_____

Tale violazione è suscettibile di presentare un rischio elevato per Suoi diritti e le libertà.

DESCRIZIONE DELLE CONSEGUENZE DELLA VIOLAZIONE

_____
_____
_____
_____

DESCRIZIONE DELLE MISURE TECNOLOGICHE E ORGANIZZATIVE ASSUNTE

_____
_____
_____
_____

Per poter ottenere maggiori **informazioni** relativamente alla violazione in oggetto, può contattare

nonché il Responsabile della Protezione dei Dati, i cui dati di contatto sono i seguenti:

Luogo e data

Firma del ____