



CITTA' DI CASTELLAMONTE

Città Metropolitana di Torino



COPIA

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

**n. 183
del 17/12/2019**

OGGETTO: REGOLAMENTO (UE) 2016/679 - APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

L'anno **2019** addì **diciassette** del mese di **dicembre** alle ore otto e minuti trenta nella sala delle adunanze.

Previo l'osservanza delle formalità prescritte dalla vigente Legge, vennero per oggi convocati a seduta i componenti la Giunta Comunale.

All' appello risultano :

Cognome e Nome	Carica	Pr.	As.
MAZZA Pasquale Mario	Sindaco	X	
MEDAGLIA Teodoro	Vice Sindaco	X	
ADDIS Patrizia	Assessore	X	
BERNARDI GHISLA Marco	Assessore	X	
FALETTO Chiara	Assessore	X	
Totale		5	0

Assiste alla adunanza il Segretario Comunale **Dott. Sergio MAGGIO** il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti il Signor **Pasquale Mario MAZZA** nella sua qualità di **SINDACO** assume la presidenza e dichiara aperta la seduta per le trattative dell'oggetto sopra indicato.

Si esprime parere favorevole sulla proposta di deliberazione in ordine alla regolarità tecnica (art.49 c.1 T.U.EE.LL. approvato con D.Lgs. 267/2000).

Il Responsabile del Servizio
F.to Dott.ssa Marcella GIRINO

OGGETTO: REGOLAMENTO (UE) 2016/679 - APPROVAZIONE PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH).

LA GIUNTA COMUNALE

PREMESSO CHE:

- la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei Diritti Fondamentali dell'Unione Europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione Europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;
- il Comune di Castellamonte, in quanto Titolare del trattamento, 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 (data breach), incluse eventuali notifiche all'Autorità di controllo competente ed eventuali comunicazioni agli interessati;

VISTO:

- il **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, di seguito "Regolamento");
- il **Decreto Legislativo 30 giugno 2003, n. 196**, recante il Codice in materia di protezione dei dati personali, così come modificato dal Decreto Legislativo 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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» (di seguito "Codice");
- il **Decreto Legislativo 18 maggio 2018, n. 51**, recante Attuazione della direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (di seguito "D.Lgs. n. 51/2018");
- le "**Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679**" (WP250) del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato Europeo per la protezione dei dati il 25 maggio 2018;
- la **Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities**, adottata ai sensi dell'art. 64 del Regolamento, dal Comitato Europeo per la protezione dei dati in data 12 marzo 2019;
- il **Provvedimento del Garante** sulla notifica delle violazioni dei dati personali (data breach) - **30 luglio 2019** [doc-web n. 9126951]

CONSIDERATO CHE:

- in caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante 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 (artt. 33 e 55 del Regolamento, art. 2-bis del Codice);
- il titolare del trattamento è tenuto altresì a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del Pubblico Ministero (artt. 26 e 37, comma 6, del D.Lgs. n. 51/2018);
- per «violazione dei dati personali» (data breach) si intende la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del D.Lgs. n. 51/2018);
- per la omessa notifica di data breach all'Autorità di controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, sono previste pesanti sanzioni amministrative (art. 83 GDPR), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui all'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- 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).
- lo stesso GDPR, all'art. 83 paragrafo 2, indica dei fattori che possono mitigare o aggravare la violazione e, tra questi, un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta, inoltre, sicuramente un'attenuazione delle sanzioni applicabili;

RITENUTO PERTANTO:

- a) 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 già 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;

b) strategico per l'ente:

- 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;
- stabilire che le procedure contemplate nell'approvando documento siano 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;
- stabilire che il rispetto dell'adottanda 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 particolare le procedure medesime sono rivolte a tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:
 - i. 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 del prestazioni richieste per conto del Titolare del trattamento;
 - ii. 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, ogniqualevolta 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;

VISTI:

- il Decreto del Sindaco numero 13 in data 23 maggio 2018 con il quale è stato designato l'avv. Massimo Ramello quale Responsabile della Protezione dei Dati Personali (DPO), nel rispetto della vigente normativa;
- visto il provvedimento di designazione del Referente, dott.ssa Marcella Girino, al Responsabile della protezione dei dati personali in data 30 aprile 2019;
- la deliberazione della Giunta Comunale n. 163 del 29 ottobre 2019, con la quale è stato approvato il Piano di Protezione e modello organizzativo per la tutela dei dati personali;

VISTE le disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (c.d. data breach) e loro allegati (lettere da A a G) e ritenute le stesse corrispondenti alla struttura organizzativa dell'Ente e adeguate sotto il profilo operativo alle esigenze del medesimo;

VALUTATA pertanto l'opportunità di procedere all'approvazione;

VISTI:

- il Regolamento sull'Ordinamento degli Uffici e dei Servizi;
- il D. Lgs. 267/2000 e s.m.i.;
- Visto Il D.Lgs. n. 165/2001 e s.m.i.

Acquisito il preventivo parere favorevole sulla proposta della presente deliberazione, in ordine alla regolarità tecnica ai sensi dell'art. 49, commi 1, del D. Lgs. 267/00 e s.m.i. e dato atto che la presente deliberazione non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Ente e pertanto, ai sensi del medesimo articolo, non necessita del parere di regolarità contabile;

Con voti favorevoli unanimi espressi in forma palese,

DELIBERA

1. di approvare, per le motivazioni in narrativa esposte che qui si intendono integralmente richiamate, la procedura nel caso di violazione dei dati personali (data breach) del Comune di Castellamonte, richiesta dagli articoli 33 e 34 del GDPR "Regolamento Generale sulla Protezione dei Dati" (Regolamento UE 2016/679) e relativi allegati da A) a G), che costituiscono parte integrante e sostanziale della presente deliberazione.
2. di demandare la concreta attuazione delle misure regolamentari minime contenute nelle disposizioni operative al personale operante all'interno dell'Ente nelle sue articolazioni gerarchiche e secondo le loro rispettive funzioni e competenze;
3. di inviare la procedura nel caso di violazione dei dati personali (data breach) del Comune di Castellamonte al Responsabile del Trattamento dei Dati personali già nominato, in persona dell'Avv. Massimo Ramello;
4. di dare atto che le disposizioni operative sono assoggettate a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

5. di disporre che al presente provvedimento venga assicurata:

- a) la pubblicità legale con pubblicazione all'Albo Pretorio, nonché
- b) la massima diffusione presso tutto il personale operante presso l'Ente e presso tutti i soggetti esterni qualificabili in termini di responsabili del trattamento.

E con successiva votazione, favorevole ed unanime espressa in forma palese,

DELIBERA

Di dichiarare immediatamente eseguibile la presente deliberazione, ai sensi dell'art. 134, comma 4 del D. Lgs. 18.8.2000 n. 267.

Letto, confermato e sottoscritto
IL SINDACO
F.to MAZZA Pasquale Mario

IL SEGRETARIO COMUNALE
F.to Dott. Sergio MAGGIO

REFERTO DI PUBBLICAZIONE

Io sottoscritto Segretario Comunale, attesto che copia del presente verbale viene pubblicato all'Albo Pretorio di questo Comune accessibile al pubblico dal sito istituzionale www.comune.castellamonte.to.it (art. 32 L.69/2009) dal 20/12/2019 per rimanervi per 15 giorni consecutivi decorrenti dal giorno successivo a quello di pubblicazione

La presente deliberazione è stata trasmessa in elenco, il primo giorno di pubblicazione, ai Capi Gruppo Consiliari (art. 125, comma 1 T.U.EE.LL. approvato con D. Lgs. 267/2000).

Li 20/12/2019

IL SEGRETARIO COMUNALE
F.to Dott. Sergio MAGGIO

CERTIFICATO DI ESECUTIVITA'

Divenuta esecutiva in data 17-dic-2019

X è stata dichiarata immediatamente eseguibile (art. 134, comma 4 - del D.lgs 267/2000)
perché decorsi 10 giorni dalla data di pubblicazione (Art.134 c.3 D.Lgs. 267/00)

IL SEGRETARIO COMUNALE
F.to Dott. Sergio MAGGIO

Copia conforme all'originale ad uso amministrativo

Castellamonte, li 20/12/2019

IL SEGRETARIO COMUNALE
Dott. Sergio MAGGIO

Ricorsi

Contro il presente atto è possibile presentare ricorso:
- entro 60 giorni dalla pubblicazione al T.A.R. Piemonte.
- entro 120 giorni al Presidente della Repubblica.

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

_____, li _____

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di _____, in qualità di Titolare del trattamento (con sede in _____; Email: _____; PEC: _____; Telefono: _____), 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 _____, PEC _____). 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.

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 sogetti 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 ridurre 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	<input checked="" type="checkbox"/>	Modulo di segnalazione di una potenziale violazione di dati personali e relativi allegati
	<input type="checkbox"/>	
Numero dei documenti allegati		

ANNOTAZIONI

_____ , li _____

Firma

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di _____, in qualità di Titolare del trattamento (con sede in _____; Email: _____; PEC: _____; Telefono: _____), 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 _____, PEC _____). 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.

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	<input type="checkbox"/> Riguarda dati personali	<input type="checkbox"/> 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

<p>Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione e</p>	

<p>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)</p>	

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 sogetti 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

<p>Misure tecniche ed organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurre gli effetti negativi per gli interessati</p>	

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

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

_____ , li _____ _____ Firma

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Comune di _____, in qualità di Titolare del trattamento (con sede in _____; Email: _____; PEC: _____; Telefono: _____), 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 _____, PEC _____). 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.



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).



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

Sez. B - Titolare del trattamento

Denominazione³:
Codice Fiscale/P.IVA:
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:
Soggetto privo di C.F./P.IVA

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

- o Responsabile della protezione dei dati⁴ - prot. n.
- o Altro soggetto⁵

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 trattamento⁶, rappresentante del titolare non stabilito nell'Ue)

Denominazione⁷ *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA
Ruolo: o Contitolare o Responsabile o Rappresentante

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

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

Denominazione *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA
Ruolo: o Contitolare o 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
- Altro⁸

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 confidenzialità¹⁰
- b) Perdita di integrità¹¹
- c) Perdita di disponibilità¹²

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 violazione¹³

- 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 violazione¹⁴**
2. **Descrizione delle categorie di dati personali oggetto della violazione¹⁵**
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 coinvolti¹⁶**

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
 - Decifrazione 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. 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 valutazioni²¹
- 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 violazione²²

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 Europeo²³?**
 - 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 controllo²⁴?**
 - SI (indicare quali):

 - NO
- 4. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative²⁵?**
 - 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.

**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 _____



CITTA' DI CASTELLAMONTE
Città Metropolitana di Torino



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

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

Sommario

FINALITÀ E AMBITO DI APPLICAZIONE	3
DEFINIZIONI	5
PIANO DI AZIONE	7
PROCEDURA.....	8
1. Individuazione della violazione	9
2. Rilevazione della violazione	13
2.1. Acquisizione della notizia	13
2.2. Fonte della notizia	13
2.3. Il monitoraggio degli eventi di sicurezza con impatto sulla protezione dei dati personali	14
2.4. Trasmissione della notizia	15
3. Analisi e Valutazione della violazione.....	16
3.1. Analisi tecnica dell'evento.....	17
3.2. Valutazione della violazione al fine del rispetto degli obblighi di notifica e comunicazione	17
3.3. Valutazioni supplementari	22
4. Notifica della violazione dei dati personali all'Autorità di controllo	23
4.1. Quando effettuare la notificazione	23
4.2. Come effettuare la notificazione.....	24
4.3. Eventuali ulteriori notificazioni (o denunce).....	24
5. Recepimento della eventuale risposta dell'Autorità di controllo	25
6. Comunicazione della violazione dei dati personali all'interessato	25
6.1. Quando effettuare la comunicazione.....	25
6.2. Come effettuare la comunicazione	26
6.3. Quali informazioni comunicare	26
6.4. Quando non effettuare la comunicazione	26
7. Altre segnalazioni	27
8. Documentazione della violazione.....	27
8.1. il Registro delle violazioni	28
8.2. Altri documenti ed informazioni	29
9. Fase di miglioramento	29
10. Fattispecie di contitolarità e responsabilità del trattamento	29
FONTI.....	31

FINALITÀ E AMBITO DI APPLICAZIONE

Il Comune di Castellamonte, 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. Cooperava 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;

«**DECITTOGRAFIA**»: 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;

	<ul style="list-style-type: none"> – 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 e dell'Ufficio Legale per gli aspetti giuridici, 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 GDPR 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**:

<p>Violazione della riservatezza (<i>Confidentiality breach</i>)</p>	<p>divulgazione o accesso non autorizzato o accidentale ai dati personali come, ad esempio:</p> <ul style="list-style-type: none"> • 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.
<p>Violazione dell'integrità (<i>Integrity breach</i>)</p>	<p>alterazione non autorizzata o accidentale dei dati personali La "<i>alterazione</i>" 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).</p>
<p>Violazione della disponibilità (<i>Availability breach</i>)</p>	<p>accidentale o non autorizzata perdita di accesso o distruzione di dati personali (Fattispecie non sempre di facile individuazione. La "<i>perdita di dati</i>" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi; la "<i>distruzione</i>" 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)</p>

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 **raccolgendo 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 guardiana 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 verifica.

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 considerevole 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	<p>facilità di identificazione, diretta o indiretta tramite abbinamento con altre informazioni, di specifiche persone fisiche sulla base dei dati personali compromessi dalla violazione.</p> <p>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</p>
Gravità delle conseguenze per le persone fisiche	<p>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).</p> <p>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.</p> <p>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.</p>
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 <i>disagi minori</i> , che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);
	MEDIO: gli individui possono andare incontro a <i>significativi disagi</i> , 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 <i>conseguenze significative</i> , 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

PROBABILITÀ	GRAVITÀ				
		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.

Rischio	Descrizione	Notifica all'Autorità	Comunicazione agli interessati
	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 verificano 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 *“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”*. 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 riporterà:

(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. Si suggerisce al riguardo l'adozione del modello ALLEGATO F "Accordo di contitolarità".

Sulla scorta della previsione di cui all'articolo 28 del GDPR, laddove il Titolare necessita 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. Si suggerisce al riguardo l'adozione del modello ALLEGATO G "Appendice contrattuale".

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, decifrazione 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, decifrazione 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 analogo 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.

ACCORDO DI CONTITOLARITA'
AI SENSI DELL'ART. 26 DEL REGOLAMENTO (EU) 2016/679

allegato F

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____

E

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, entrambe le parti saranno identificate, congiuntamente, quali "Contitolari" o "Parti")

PREMESSO CHE

- 1) è in essere tra le Parti un progetto comune consistente in _____, il quale comporta la necessità di determinare congiuntamente le finalità e le modalità del trattamento dei dati personali coinvolti nella realizzazione del medesimo progetto comune;
- 2) che in data 25 maggio 2018 è divenuto pienamente operativo il 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) (d'ora innanzi, più semplicemente, "GDPR");
- 3) l'articolo 4, paragrafo 1, n. 7) del GDPR definisce quale 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*";
- 4) a norma dell'articolo 26, paragrafo 1 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*";
- 5) a norma dell'articolo 26, paragrafo 2 del GDPR "*L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato*";
- 6) è intenzione delle Parti contraenti regolamentare in modo trasparente i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, nonché i rispettivi ruoli nella comunicazione delle informazioni agli interessati, addivenendo alla sottoscrizione della presente accordo;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. Nell'ambito delle rispettive responsabilità come determinate dal presente Accordo, i Contitolari dovranno in ogni momento adempiere ai propri obblighi conformemente ad esso e in modo tale da trattare i dati senza violare le disposizioni di legge vigenti e nel pieno rispetto delle linee guida e dei codici di condotta applicabili, di volta in volta approvati dall'Autorità di controllo.
2. Resta inteso tra le Parti che, ai sensi dell'art. 26, comma 3, del Regolamento (EU) 2016/679, indipendentemente dalle disposizioni del presente Accordo, l'interessato potrà esercitare i propri diritti nei confronti di e contro ciascun Contitolare del trattamento.
3. In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.

4. Il presente accordo non determina l'insorgere di alcun diritto alla revisione di prezzi od altre forme di impegno, anche economico, già definiti tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.
5. Il presente accordo annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla sua stipulazione, i loro rapporti saranno regolati esclusivamente dal presente accordo.
6. Qualsiasi modifica od integrazione del presente accordo potrà farsi soltanto per iscritto a pena di nullità.
7. Il contenuto essenziale di questo accordo di Contitolarità è messo a disposizione dell'Interessato nella sezione Trasparenza del Portale di ciascuno dei Contitolari.

Articolo 2 - Oggetto del trattamento

1. I Contitolari dichiarano, in merito al trattamento dei Dati Personali, di condividere le decisioni relative alle finalità e modalità del trattamento di dati e, in particolare:

- le seguenti banche dati; dipendenti e collaboratori, _____;
- le finalità del trattamento di dati personali, ciascuna con le proprie specificità legate alle attività concretamente svolte;
- i mezzi del trattamento e le modalità del trattamento di dati personali;
- la politica di conservazione dei dati;
- lo stile e le modalità di comunicazione delle informative art. 13 del GDPR;
- la procedura di gestione dei consensi (ove necessari);
- la designazione e la formazione dei soggetti autorizzati;
- istruzioni sull'uso degli strumenti informatici per il personale;
- la gestione delle comunicazioni e nomine dei responsabili ai sensi dell'art. 28 del GDPR;
- la tenuta dei registri del trattamento ai sensi dell'art. 30 del GDPR;
- le procedure nel caso di trasferimento dei dati fuori UE;
- gli strumenti ed i mezzi utilizzati per l'attuazione delle decisioni e in parte anche per l'operatività dei Contitolari soprattutto in relazione alle misure di sicurezza fisiche, organizzative e tecniche;
- l'approccio basato sul rischio;
- i profili e la politica di sicurezza dei dati personali, la procedura del Data Breach e la procedura di valutazione di impatto sulla protezione dei dati personali (DPIA);
- la gestione della procedura di esercizio dei diritti dell'Interessato;
- una raccolta congiunta delle procedure sulla protezione dei dati personali attraverso la tenuta comune e gestione di un modello organizzativo.

2. La contitolarità è riferita al trattamento dei dati personali ed ha ad oggetto il trattamento di tutti i dati già presenti, in tutti gli archivi sia cartacei che informatizzati, e di tutti quelli che si acquisiranno in futuro. Il flusso dei dati personali sarà così strutturato: _____.

3. Con il presente accordo i Contitolari convengono che i dati personali presenti negli archivi tanto cartacei quanto informatizzati, nonché quelli futuri, verranno trattati per le seguenti finalità: _____.

4. Le attività alla base del presente accordo comportano il trattamento delle seguenti categorie di dati personali: _____.

5. Le categorie di Interessati sono: _____.

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto

1. Il presente accordo diviene efficace tra le parti immediatamente all'atto della sua sottoscrizione e sarà valido ed efficace sino alla scadenza, originale o prorogata del rapporto convenzionale che lega i Contitolari, ovvero alla sua cessazione di validità ed efficacia a qualsiasi causa dovuta.

2. Il Trattamento dei dati personali in regime di contitolarità, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati dei Contitolari in una forma che consenta l'identificazione degli Interessati per un periodo di tempo non superiore a quello in precedenza indicato, fatto salvo che il trattamento e la conservazione dei dati medesimi ad opera di ciascuno dei Contitolari sia imposta dalla normativa vigente.

3. A seguito della cessazione del trattamento, nonché a seguito della cessazione del rapporto convenzionale sottostante, qualunque ne sia la causa, i Contitolari saranno tenuti a provvedere alla integrale distruzione dei dati personali trattati, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità od il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del

trattamento dei dati da parte dei singoli Contitolari, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.

4. Ciascun Contitolare provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sé, non esiste alcuna copia dei dati personali e delle informazioni trattate nell'ambito del progetto comune. Sul contenuto di tale dichiarazione l'altro Contitolare si riserva il diritto di effettuare controlli e verifiche volte ad accertarne la veridicità.

Articolo 4 – Obblighi tra le parti

1. La tutela dei dati personali è fondata sull'osservanza dei principi illustrati nel presente documento che i Contitolari si impegnano a diffondere, rispettare e far rispettare ai propri amministratori, ai propri dipendenti e collaboratori ed ai soggetti terzi con cui collaborano nello svolgimento della propria attività istituzionale. In particolare i Contitolari sono impegnati affinché la politica della protezione dati personali, e quanto ne consegue, sia compresa, attuata e sostenuta da tutti i soggetti, interni ed esterni, coinvolti nelle attività dei Contitolari, tenuto conto della loro realtà concreta, delle loro possibilità anche economiche e dei loro valori.

2. I Contitolari si impegnano a mantenere e garantire la riservatezza e la protezione dei dati personali raccolti, trattati e utilizzati in virtù del rapporto di contitolarità. In particolare essi, anche disgiuntamente tra loro, si impegnano a:

- a) comunicare e diffondere la propria politica in merito alla protezione dei dati personali;
- b) prestare ascolto e attenzione a tutte le parti interessate proprie – a mero titolo esemplificativo, amministratori, personale dipendente e collaboratore, cittadini, utenti e beneficiari di prestazioni anche di natura assistenziale, fornitori, consulenti – e tenendo in debito conto le loro istanze in materia di trattamento di dati personali e dando pronto riscontro;
- c) trattare i dati personali in modo lecito, corretto e trasparente in linea con i principi costituzionali e con la normativa vigente in materia, in particolare il GDPR, e solo per il tempo strettamente necessario alle finalità previste, comprese quelle per ottemperare agli obblighi di legge;
- d) raccogliere i dati personali limitandosi a quelli indispensabili per effettuare le attività costituenti il progetto comune (dati personali pertinenti e limitati);
- e) trattare i dati personali secondo i principi di trasparenza per le sole finalità specifiche ed espresse nelle proprie informative;
- f) adottare processi di aggiornamento e di rettifica dei dati personali trattati per assicurarsi che i dati personali siano, per quanto possibile, corretti e aggiornati;
- g) conservare e tutelare i dati personali di cui è in possesso con le migliori tecniche di preservazione disponibili;
- h) garantire il continuo aggiornamento delle misure di protezione dei dati personali. Tale impegno sarà costantemente seguito nell'ambito del principio di responsabilizzazione mettendo in atto, con costanza, misure tecniche e organizzative adeguate e politiche idonee, per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR tenuto conto dello stato dell'arte, della natura dei dati personali custoditi e dei rischi ai quali sono esposti. Ciascun Contitolare eseguirà un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio;
- i) garantire il tempestivo recupero della disponibilità dei dati personali in caso di incidente fisico o tecnico
- l) rendere chiare, trasparenti e pertinenti le modalità di trattamento dei dati personali e la loro conservazione in maniera da garantirne un'adeguata sicurezza;
- m) favorire lo sviluppo del senso di responsabilizzazione e la consapevolezza dell'intera organizzazione verso i dati personali, visti come dati di proprietà dei singoli interessati;
- n) assicurare il rispetto delle disposizioni legislative e regolamentari applicabili alla tutela dei dati personali aggiornando eventualmente la gestione della protezione dei dati personali;
- o) prevenire e minimizzare, compatibilmente con le risorse disponibili, l'impatto di potenziali violazioni o trattamenti illeciti e/o dannosi dei dati personali;
- p) promuovere l'inserimento della protezione dati personali nel piano di miglioramento continuo che il Contitolare persegue con i propri sistemi di gestione.

3. I Contitolari si impegnano con particolare riguardo all'esercizio dei diritti dell'Interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, ad uniformare le modalità, lo stile i modelli e soprattutto le procedure per la protezione dei dati personali a favore dell'Interessato.

4. La comunicazione dei dati personali necessari a garantire il perseguimento del progetto comune avverrà 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.

Articolo 5 - Incaricati e persone autorizzate

1. Ciascuno dei Contitolari dovrà identificare e designare le persone autorizzate ad effettuare operazioni di trattamento sui dati trattati nel perseguimento del progetto comune, identificando l'ambito autorizzativo consentito ai sensi dell'art. 29 del GDPR e provvedendo alla relativa formazione, anche in merito ai principi di liceità e correttezza a cui deve conformarsi la presente politica per la protezione dei dati personali e il trattamento dei dati personali nonché al rispetto delle misure di salvaguardia adottate.
2. Ciascuno dei Contitolari 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.
3. Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte.

Articolo 6 - Responsabili del trattamento

1. Ciascuno dei Contitolari il quale ravvisasse la necessità di avvalersi di un responsabile del trattamento per l'esecuzione di specifiche attività richieste nell'ambito del progetto comune, è tenuto a comunicarlo all'altra parte con congruo preavviso.
2. Su tale responsabile del trattamento sono imposti, mediante un contratto od un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, specifici obblighi in materia di protezione dei dati, 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. I rapporti tra i Contitolari e gli eventuali responsabili del trattamento restano disciplinati dall'articolo 28 del GDPR.

Articolo 7 – Valutazione d'impatto e Violazioni di dati personali

1. Nei casi previsti dall'art. 35 del GDPR, la valutazione d'impatto sulla protezione dei dati personali ed il suo eventuale riesame, così come la consultazione preventiva di cui all'art. 36 del GDPR, sono a carico di _____, il quale informa tempestivamente l'altro Contitolare della relativa necessità e dell'attività compiuta.
2. 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 nel contesto del progetto comune, l'attività di coordinamento ai fini dell'adempimento degli obblighi di cui agli articoli 33 e 34 del GDPR è affidata a _____ il quale curerà la predisposizione di un apposito documento (data breach policy), ove non già esistente ed adottato.
3. Al verificarsi di una violazione di dati personali, il Contitolare non assegnatario dell'attività di coordinamento provvederà:
 - a) ad informare l'altro Contitolare 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 fornendogli 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 sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
 - b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Esso si inoltre attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive ed attuando tutte le azioni correttive approvate e/o richieste dal Contitolare assegnatario dell'attività di coordinamento. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al Trattamento eseguito.
4. Ciascun Contitolare 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 8 - Decisioni in merito ai trasferimenti internazionali di dati personali

1. Il presente accordo prevede che i dati personali saranno trattati all'interno del territorio dell'Unione Europea.

2. Nell'ipotesi in cui per questioni di natura tecnica e/o operativa si rendesse necessario avvalersi di soggetti ubicati al di fuori dell'Unione Europea, il trasferimento dei dati personali, limitatamente allo svolgimento di specifiche attività di Trattamento, sarà regolato in conformità a quanto previsto dal capo V del GDPR. Saranno quindi adottate tutte le cautele necessarie al fine di garantire la più totale protezione dei dati personali basando tale trasferimento: (i) su decisioni di adeguatezza dei paesi terzi destinatari espresse dalla Commissione Europea; (ii) su garanzie adeguate espresse dal soggetto terzo destinatario ai sensi dell'articolo 46 del GDPR; (iii) sull'adozione di norme vincolanti d'impresa.

Articolo 9 - Condivisione della procedura per l'esercizio dei diritti dell'Interessato

1. I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.

2. In particolare, qualora il referente unitario riceva richieste provenienti dall'Interessato, finalizzate all'esercizio dei propri diritti, esso dovrà:

- darne tempestiva comunicazione scritta a ciascun Contitolare via posta elettronica certificata, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate da ciascun Contitolare per gestire le relazioni con l'Interessato;
- verificare la sussistenza dei presupposti e consentirne, differirne o rifiutarne l'esercizio, dandone tempestiva comunicazione scritta a ciascun Contitolare via posta elettronica certificata.

3. Il referente unitario fornisce altresì assistenza a ciascuno dei Contitolari nell'ambito dei procedimenti amministrativi e giudiziari instaurati dall'Interessato o dall'Autorità di controllo in conseguenza dell'attività di cui al presente articolo.

Articolo 10 - Verifiche circa il rispetto delle regole di protezione dei dati personali

1. Ciascuno dei Contitolari riconosce all'altro il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il trattamento dei dati personali nell'ambito del progetto comune. A tal fine, Ciascuno dei Contitolari 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 dell'altro.

2. Ciascuno dei Contitolari rende disponibile tutta la documentazione necessaria per dimostrare la conformità a tutti i suoi obblighi e per consentire la conduzione di audit, comprese le ispezioni, e per contribuire a tali verifiche.

3. Ciascuno dei Contitolari deve informare e coinvolgere tempestivamente l'altra parte 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 11 - Responsabilità per violazione delle disposizioni

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali.

Articolo 12 - Responsabile della Protezione dei dati personali

1. Ciascuno dei Contitolari 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 - E-mail: _____@gdpr.nelcomune.it - 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 13 – Clausole nulle o inefficaci

Qualora una o più clausole del presente accordo fossero o divenissero contrarie a norme imperative o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità dello stesso,

fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'accordo ove la pura e semplice eliminazione della clausola nulla menomasse gravemente i suoi diritti.

Articolo 14 – Comunicazioni

Qualsiasi comunicazione relativa al presente accordo dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'accordo. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 15 – Disposizioni finali

Per quanto non espressamente indicato nella presente Appendice, i rinviano al GDPR, alle disposizioni di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo.

AFFIDAMENTO DEL SERVIZIO DI _____ allegato G
APPENDICE CONTRATTUALE
AI SENSI DELL'ART. 28 DEL REGOLAMENTO (EU) 2016/679

RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, più semplicemente, Titolare del trattamento)

E

_____ (C.F.: _____ - P. IVA: _____) con sede in _____, PEC: _____, all'uopo rappresentato da _____ (d'ora innanzi, più semplicemente, Responsabile del trattamento)

PREMESSO CHE

- 1) tra le parti è in essere un contratto, stipulato in data _____ avente ad oggetto _____ e durata sino a _____ (d'ora innanzi, più semplicemente, Contratto);
- 2) nel dare esecuzione alle obbligazioni dedotte nel Contratto il Responsabile si troverà ad effettuare operazioni di trattamento di dati personali per conto del Titolare, rimanendo a quest'ultimo di stabilire autonomamente le finalità, le modalità ed i mezzi del trattamento medesimo;
- 3) che in data 25 maggio 2018 è divenuto pienamente operativo il 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) (d'ora innanzi, più semplicemente, GDPR);
- 4) l'articolo 4, paragrafo 1, n. 8) del 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”*;
- 5) 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”*;
- 6) 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”*;
- 7) 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”*
- 8) alla data di sottoscrizione della presente appendice non risulta che la Commissione europea ovvero l'Autorità di controllo nazionale abbiano adottato clausole contrattuali tipo ai sensi dei paragrafi 7 ed 8 del GDPR;
- 9) è intenzione delle Parti contraenti regolamentare i diritti e gli obblighi reciproci quali conseguono alla puntuale osservanza delle norme e dei principi contenuti nel GDPR, addivenendo alla sottoscrizione della presente Appendice contrattuale, da considerarsi parte integrante e sostanziale del Contratto;

SI CONVIENE E SI STIPULA QUANTO SEGUE

Articolo 1 – Pattuizioni preliminari

1. 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 dal Contratto 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.

2. Scopo della presente Appendice è l'identificazione della 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 ed i diritti del Titolare e del Responsabile del trattamento. In particolare la presente Appendice non costituisce autorizzazione generale ma, bensì, autorizzazione limitata esclusivamente ai trattamenti relativi al servizio specificatamente indicato nel Contratto.

3. La presente Appendice contrattuale non determina l'insorgere di alcun diritto del Responsabile alla revisione del prezzo già definito tra le Parti, trattandosi di obblighi ed adempimenti derivanti da norme di legge già conosciute.

4. La presente Appendice annulla e/o sostituisce qualsivoglia regolazione pattizia esistente tra le Parti in relazione al medesimo oggetto, di talché, a far data dalla stipulazione della presente, i loro rapporti saranno regolati esclusivamente dalla presente Appendice.

5. Qualsiasi modifica od integrazione della presente Appendice potrà farsi soltanto per iscritto a pena di nullità.

6. Ciascuna Parte riconosce di essere addivenuta alla stipula della presente Appendice esclusivamente sulla base della rappresentazione dei fatti ricevuta dall'altra Parte e, pertanto, in caso di falsa rappresentazione, la presente Appendice deve intendersi radicalmente nulla sin dall'origine, senza alcuna possibilità di sanatoria, qualsivoglia eccezione intendendosi sin da ora rimossa e/o rinunziata.

Articolo 2 - Oggetto del trattamento

1. Le prestazioni già affidate al Responsabile, ai sensi del Contratto, consistono nell'erogazione dei seguenti servizi: _____.

2. Dette prestazioni comportano il trattamento delle seguenti categorie di dati personali: _____.

3. Le categorie di Interessati sono: _____

4. La natura delle operazioni eseguite sui dati è: _____

5. Le finalità del trattamento dei dati medesimi sono: _____

Articolo 3 – Durata ed effetti conseguenti allo scioglimento del Contratto

1. Trattandosi di patto accessorio ed aggiunto al Contratto, esso diviene efficace tra le parti immediatamente all'atto della sua sottoscrizione e sarà valido ed efficace sino alla scadenza, originale o prorogata del Contratto ovvero alla sua cessazione di validità ed efficacia a qualsiasi causa dovuta.

2. Il Trattamento per conto del Titolare, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i 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.

3. 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 verificino 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.

4. Il Responsabile, su richiesta del titolare, provvede a rilasciare apposita dichiarazione scritta contenente l'attestazione che, presso di sé, 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.

5. 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 oggetto della presente Appendice, 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 4 - 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. Dichiaro 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 prende atto che il Contratto in essere viene mantenuto anche successivamente all'operatività del GDPR per l'esclusiva ragione che il profilo professionale / societario, in termini di proprietà, risorse umane, organizzative ed attrezzature, è stato ritenuto dal Titolare idoneo a soddisfare i requisiti di esperienza, capacità ed affidabilità previsti dalla vigente normativa. Qualsiasi mutamento di tali requisiti, che possa sollevare incertezze sul loro mantenimento, dovrà essere preventivamente segnalato al Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di ritenere risolto il rapporto in essere per fatto e colpa del Responsabile.

3. Il Responsabile è tenuto a:

a) trattare i dati nel rispetto dei principi del trattamento previsti nel GDPR e solo per le finalità indicate dal 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;

4. 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 della presente Appendice;

5. Il Responsabile informa il Titolare, per quanto di necessità, che i suoi dati verranno conservati e trattati per l'intera durata del rapporto contrattuale e, all'eventuale termine dello stesso, per il tempo previsto dalla vigente normativa, nazionale e comunitaria, in materia contabile, fiscale, civilistica e processuale.

Articolo 5 - 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 della presente Appendice;

6. Il Titolare informa il Responsabile, per quanto di necessità, che i suoi dati verranno conservati e trattati per l'intera durata del rapporto contrattuale e, all'eventuale termine dello stesso, per il tempo previsto dalla vigente normativa, nazionale e comunitaria, in materia contabile, fiscale, civilistica e processuale.

Articolo 6 - 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 7 - 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 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.

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 nella presente Appendice 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 8 - 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 9 - 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 od al Titolare.

Articolo 10 - 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 eventualmente 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 11 - 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 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 12 - 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.
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 13 - 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 14 - 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 15 - 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 - E-mail: _____@gdpr.nelcomune.it - Pec: dpo@pec.gdpr.nelcomune.it

Detto nominativo è stato altresì comunicato all'Autorità Garante per la Protezione dei dati personali con procedura telematica.

2. Il Responsabile del trattamento dichiara di aver/non aver provveduto alla nomina del proprio responsabile della protezione dei dati (in caso affermativo, indicarne i dati di contatto).

Articolo 16 – Clausole nulle o inefficaci

1. Qualora una o più clausole della presente Appendice fossero o divenissero contrarie a norme imperative o di ordine pubblico, esse saranno considerate come non apposte e non incideranno sulla validità della stessa, fatto salvo il diritto di ciascuna parte di chiedere una modifica dell'Appendice ove la pura e semplice eliminazione della clausola nulla menomasse gravemente i suoi diritti.

Articolo 17 – Comunicazioni

1. Qualsiasi comunicazione relativa alla presente Appendice ed al sottostante Contratto dovrà essere data per iscritto ed a mezzo di posta elettronica certificata, con ricevuta di accettazione e conferma di consegna, purché inviati o consegnati all'indirizzo indicato in testa all'Appendice. Tale indirizzo potrà essere modificato da ciascuna delle Parti, dandone comunicazione all'altra ai sensi del presente articolo.

Articolo 18 – Disposizioni finali

1. Per quanto non espressamente indicato nella presente Appendice, il Titolare ed il Responsabile del trattamento rinviano al GDPR, alle disposizioni di legge vigenti, nonché ai provvedimenti dell'Autorità di controllo.