COMUNE DI PIZZALE

Provincia di Pavia

Procedura Data Breach

05.12.2024

Sommario

1 SCOPO

La presente procedura regolamenta la gestione degli eventi di Data Breach o quelli che vengono, in prima battuta considerati come tali.

2 OGGETTO

Si considerano eventi di Data Breach quelli che comportano in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trattati dal Titolare. Tali eventi comportano rischi per i diritti e le libertà degli interessati.

I principali rischi sono i seguenti:

- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)*
- *danni fisici, materiali o immateriali a persone fisiche*
- *perdita del controllo dei dati degli interessati*
- *limitazioni dei diritti/discriminazione*
- *furto o usurpazione di identità*
- *perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Titolare)*
- *decifratura non autorizzata della pseudonimizzazione*

Le cause che possono portare a tali situazioni possono essere:

- *errore umano volontario o involontario*
- *circostanze impreviste come incendio, alluvione, terremoto, ecc.*
- *attacco hacker*
- *mancato funzionamento delle misure di mitigazione previste*
- *reati "blagging" in cui le informazioni sono ottenute ingannando l'organizzazione che lo detiene*

3 CAMPO DI APPLICAZIONE

La presente procedura si applica a COMUNE DI PIZZALE (PV) (da qui in avanti anche solo Ente) sia che ricopra funzioni di Titolare del trattamento, che di Responsabile del Trattamento, che di con-Titolare.

4 NORMATIVA DI RIFERIMENTO

Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679

Decreto Legislativo 196/2003 come novellato dal D. Lgs 101/2018

Linee Guida EDPB European Data Protection Board (ex Working Party article 29 o WP29)

5 SOGGETTI COINVOLTI

Titolare in persona del SINDACO – SEGRETARIO COMUNALE

DPO nominato

Amministratore di sistema (A.D.S.)

Funzioni di volta in volta coinvolte nell'evento

6 DEFINIZIONI DELLE AZIONI

È necessario che il Titolare dia notizia a tutti gli operatori in merito alla presente procedura mediante idonea delibera e circolare.

Il referente privacy è opportuno che sia affiancato da un gruppo privacy (gruppo multidisciplinare di professionisti che supportano il referente privacy per specificità tecniche quali ICT, SIC, area giuridica, area del personale).

6.1 TEAM CRISI

Al fine della corretta gestione dei possibili Data Breach si costituisce un team crisi composto da:

- Titolare – SINDACO o SEGRETARIO COMUNALE
- DPO nominato
- Amministratore di sistema (A.D.S.)
- altre funzioni responsabili, di volta in volta coinvolte in base all'evento

Il Team crisi o soggetti da questo delegati, sono i soli autorizzati a trattare con il Garante e con gli interessati (vedi paragrafo "Comunicazione").

6.1.1 FORMAZIONE DEL TEAM CRISI

All'atto della costituzione il Team crisi effettua una formazione mirata sulla applicazione della presente procedura; tale formazione è effettuata nel caso di introduzione di un nuovo membro nel Team. La formazione e la verifica dell'adeguatezza della procedura debbono essere verbalizzate. Il documento viene archiviato nel dossier "privacy".

6.1.2 VERBALIZZAZIONE DELLE ATTIVITÀ

Tutte le attività e le riunioni del Team crisi debbono essere verbalizzate; i verbali sono conservati dal Responsabile del Team, nel dossier "privacy" e conservate per almeno 10 anni (o in relazione agli effetti che il Data Breach può avere sui diritti degli interessati). In ogni verbale (sottoscritto dai partecipanti alla riunione) deve essere indicato:

- chi partecipa (membro del Team/invitato all'incontro)
- decisioni assunte nel corso dell'incontro
- stato di avanzamento delle decisioni assunte nel corso di incontri precedenti

6.1.3 DISPONIBILITÀ E POSIZIONE DEL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento, qualora non presente, è tenuto informato degli sviluppi e delle decisioni del Team in ogni fase dell'indagine ed ha potere di imporre misure più restrittive a tutela dei diritti degli interessati. Qualora il Titolare non fosse disponibile a fornire il contributo richiesto, il Referente Privacy ha l'autorità per procedere autonomamente nelle decisioni prese.

6.1.4 RUOLO DI EVENTUALI ESPERTI ESTERNI

Per le azioni previste dalla procedura possono essere coinvolte eventuali esperti esterni che saranno incaricati previa sottoscrizione di un vincolo di riservatezza.

6.1.5 RIFERIMENTI PER GLI INTERESSATI

Nella informativa che fornisce il Titolare agli interessati è prevista la comunicazione dei riferimenti mail per la comunicazione di problematiche che potrebbero sfociare in Data Breach.

6.1.6 TEMPISTICA

Il calcolo della tempistica (considerando che il GDPR fornisce 72 ore al Titolare per la eventuale notifica al Garante e la comunicazione all'interessato) decorre dal ricevimento della segnalazione.

6.1.7 RENDICONTAZIONE DELLE ATTIVITÀ DEL TEAM CRISI

Almeno annualmente il Titolare del trattamento/ Referente privacy predispone una relazione sulla attività del Team Crisi nel corso dell'anno. Tale relazione viene trasmessa all'Organo di governo del Titolare.

La relazione, per quanto possibile è integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

6.2 GESTIONE EVENTO DI DATA BREACH

Alla gestione di evento di Data Breach è richiesta la massima attenzione e sensibilità da parte di tutte le funzioni coinvolte.

6.2.1 SEGNALAZIONE

La segnalazione di un evento può provenire dall':

- Interno – ogni autorizzato al trattamento deve, nel caso avvia anche il sospetto di una violazione di dati (compiuta dall'interno o dall'esterno) o sia a conoscenza di una comunicazione da parte di un interessato/terzo (anche esterno) segnalare al Referente Privacy in modo da attivare la procedura di valutazione dell'evento; la segnalazione può avvenire con qualsiasi forma, purché avvenga nel minor tempo possibile; anche un solo sospetto deve essere comunicato perché si proceda con la valutazione.
- Esterno (segnalazione da Interessato/Garante/organi di stampa) –
    - il Referente Privacy/altri componenti team crisi raccolgono le segnalazioni di possibile Data Breach provenienti dall'esterno in qualsiasi forma
    - il Referente Privacy/altri componenti team crisi consultano regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio che potrebbero riguardare anche il Titolare.

In entrambi i casi il Referente Privacy comunica via mail con gli altri membri del Team crisi utilizzando la loro casella di posta (al fine di lasciare una traccia) e procede quindi alla comunicazione telefonica.

- Responsabile esterno trattamento/subresponsabile -

  Il Referente Privacy raccoglie le segnalazioni di possibile Data Breach provenienti da figure esterne con le quali è in essere un contratto di responsabile esterno/subresponsabile; attraverso i canali definiti in tali contratti.

  Tutte le comunicazioni che provengono da fonte interna o da Responsabili esterni devono essere identificate con l'orario (riportando, quando possibile un documento – es. mail – che l'attesta in modo univoco).

6.2.2 ID SEGNALAZIONE

Ad ogni segnalazione è assegnato un numero univoco (ID) formato dal numero progressivo/anno. Questo numero permetterà di identificare in modo univoco tutta la documentazione che riguarda l'incidente e, per quanto possibile, deve essere sempre indicato.

Appena ricevuta la segnalazione deve essere aggiornato, da parte del Referente Privacy il REGISTRO degli incidenti.

6.2.3 VALUTAZIONE PER INDIVIDUARE LE AZIONI DA INTRAPRENDERE A SEGUITO DI UNA VIOLAZIONE DEI DATI PERSONALI

In questa prima fase (S0), raccolta la segnalazione, si procede con una valutazione finalizzata a comprendere se si è di fronte ad un data breach.

Il modello utilizzato prende spunto dal modello di autovalutazione messo a disposizione dall'Autorità Garante.

Nel rispondere alle domande indicate in procedura si terrà quindi conto di quanto segue.

Domanda 1

Un incidente di sicurezza è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può comportare la compromissione dei dati detenuti da un'organizzazione, mettendo a rischio uno o più dei tre principi della sicurezza delle informazioni: riservatezza, integrità e disponibilità.

Un incidente di sicurezza può riguardare contemporaneamente la riservatezza, l'integrità o la disponibilità di dati e informazioni o consistere in una qualsiasi combinazione di esse.

ESEMPI

Un incidente di sicurezza può verificarsi, ad esempio, in seguito ad un attacco informatico, ad un comportamento umano illecito o accidentale, ad una catastrofe naturale, a un malfunzionamento hardware o software.

Si verifica:

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

Domanda 2

Un dato personale è «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» (cfr. art. 4Apertura sito esterno in una nuova scheda per l'articolo 4 del Regolamento (UE) 2016/679, punto 1), del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. a), del D.Lgs 51/2018).

ESEMPI

Sono dati personali tutte quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

L'identificazione richiede elementi che permettono di distinguere una persona dalle altre. Il nome e il cognome, ad esempio, permettono di identificare una persona direttamente, mentre dati personali come il numero di telefono, il codice fiscale, l'indirizzo IP, la targa di un veicolo permettono di identificare una persona indirettamente.

Sono dati personali, ad esempio, i dati anagrafici (nome, cognome, data di nascita, luogo di nascita), i dati di contatto (indirizzo postale, indirizzo di posta elettronica, numero di telefono fisso o mobile), dati di accesso e di identificazione (username, password), dati di geolocalizzazione, dati di pagamento.

Specialmente delicati sono dati appartenenti a categorie particolari (cfr. art. 9Apertura sito esterno in una nuova scheda per l'articolo 9 del Regolamento (UE) 2016/679 del Regolamento), e cioè dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; dati genetici; dati biometrici intesi ad identificare in modo univoco una persona fisica; dati relativi alla salute o alla vita sessuale o all'orientamento sessuale e i dati personali relativi a condanne penali e reati (cfr. art. 10Apertura sito esterno in una nuova scheda per l'articolo 10 del Regolamento (UE) 2016/679 del Regolamento).

In caso di entrambe le risposte di cui sopra positive **l'incidente di sicurezza occorso costituisce una violazione dei dati personali e occorre quindi procedere alle fasi successive.**

6.2.4 VALUTAZIONE DI PERTINENZA DELLA SEGNALAZIONE

Raccolta la segnalazione, attraverso le forme sopra indicate, il responsabile del Team crisi, convoca entro massimo 12 ore dalla segnalazione, una riunione coinvolgendo tutti i membri ed eventuali altri soggetti potenzialmente coinvolti sulla base delle informazioni disponibili. Qualora qualche membro non fosse disponibile si procede comunque con la riunione.

Il Team compila il MODULO Gestione del Data Breach nella sezione S0 ed eventualmente S1; se necessario, il Team procede nella raccolta di eventuali ulteriori informazioni (es. tramite organi di stampa, richieste di approfondimento) al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato.

Il Team crisi valuta prioritariamente eventuali azioni per contenere gli effetti dell'evento; li mette in atto attivando le risorse necessarie e documenta tali azioni nel MODULO Gestione del Data Breach nella sezione S2.

Qualora si verificasse, anche dopo eventuali approfondimenti la non sussistenza di situazioni che mettono a rischio i dati degli interessati il Team compila MODULO Gestione del Data Breach nella sezione S6; comunica la decisione al Titolare (che potrebbe comunque richiedere un ulteriore approfondimento). Il Team

valuta la necessità di procedere ad una eventuale Azione correttiva come indicato nella sezione S8 del MODULO Gestione del Data Breach; aggiorna il Registro degli incidenti.

Negli altri casi il Team procede a:

- informare il Titolare del trattamento
- valutare le conseguenze dell'evento (dati personali colpiti, portata (n. e/o % interessati e n. dati), arco temporale, dati/interessati coinvolti)

Sulla base degli elementi raccolti, valuta la presenza o meno della violazione o presunta tale, tenendo presente che il Team crisi, in caso di dubbio deve assumere un atteggiamento prudenziale a difesa dei diritti dell'interessato, e la documenta MODULO Gestione del Data Breach nella sezione S2.

In caso di esito positivo procede con la analisi del rischio. In caso negativo procede con la compilazione del MODULO Gestione del Data Breach nella sezione S6.

L'esito della valutazione di pertinenza della segnalazione deve essere riportato, a cura del Referente Privacy, nel REGISTRO degli incidenti. Se la segnalazione non risulta pertinente il Referente Privacy traccerà una riga per annullare la compilazione degli altri campi previsti dal REGISTRO.

6.2.5 ANALISI DEL DATA BREACH

Nell'analizzare la gravità delle violazioni dei dati personali il Titolare ha deciso di utilizzare la metodologia ENISA.

La violazione deve essere valutata secondo il livello di rischio definito sulla base di due parametri:

- **gravità**
- **probabilità**

Gravità: rilevanza degli effetti dannosi che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte.

Probabilità: grado di possibilità che si verifichino uno o più eventi temuti a danno di persone fisiche a causa della violazione dei dati personali **in relazione alle misure di sicurezza in essere** quali:

- discriminazioni
- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale
- decifratura non autorizzata della pseudonimizzazione
- danno economico o sociale significativo
- privazione o limitazione di diritti o libertà
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

Il valore della **gravità** viene valutato sulla base della tabella che segue:

Liv.	R- Riservatezza	I - Integrità	D- Disponibilità
1 - Basso	**Interessati** Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	**Interessati** Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	**Interessati** Gli interessati possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
2 – Medio	**Interessati** Gli interessati possono incontrare inconvenienti significativi, che riusciranno a superare a dispetto di alcuni problemi (costi aggiuntivi, impossibilità di accesso a servizi, timore o mancanza di comprensione, stress, disagi o disturbi fisici minori, ecc.).	**Interessati** Gli interessati possono incontrare inconvenienti significativi, che riusciranno a superare a dispetto di alcuni problemi (costi aggiuntivi, impossibilità di accesso a servizi, timore o mancanza di comprensione, stress, disagi o disturbi fisici minori, ecc.).	**Interessati** Gli interessati possono incontrare inconvenienti significativi, che riusciranno a superare a dispetto di alcuni problemi (costi aggiuntivi, impossibilità di accesso a servizi, timore o mancanza di comprensione, stress, disagi o disturbi fisici minori, ecc.).
3 - Alto	**Interessati** Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita del posto di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	**Interessati** Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita del posto di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	**Interessati** Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita del posto di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
4 - Molto alto	**Interessati** Gli interessati possono avere conseguenze significative, o addirittura irreversibili, che potrebbero non superare (incapacità di lavorare, gravissima perdita economica, disturbi psicologici o fisici a lungo termine, morte, ecc.)	**Interessati** Gli interessati possono avere conseguenze significative, o addirittura irreversibili, che potrebbero non superare (incapacità di lavorare, gravissima perdita economica, disturbi psicologici o fisici a lungo termine, morte, ecc.)	**Interessati** Gli interessati possono avere conseguenze significative, o addirittura irreversibili, che potrebbero non superare (incapacità di lavorare, gravissima perdita economica, disturbi psicologici o fisici a lungo termine, morte, ecc.)

Il valore della **probabilità** viene valutato **in relazione alle misure di sicurezza in essere**, sulla base della tabella che segue:

valore	Livello	Minaccia
1	BASSO	è improbabile che la minaccia si materializzi
2	MEDIO	è possibile che la minaccia si materializzi
3	ALTO	la minaccia potrebbe materializzarsi

6.2.5 ESITO DELLA ANALISI DEL DATA BREACH E DECISIONI

A seguito dell'analisi del Data Breach, in considerazione dei singoli valori attribuiti alla violazione di riservatezza, integrità, disponibilità, si procederà come segue:

A. Valore Data Breach – fino a 3 = MISURE: non fare NOTIFICA e COMUNICAZIONE e valutare eventuale AC vedi S8 nel MODULO Gestione del Data Breach
B. Valore Data Breach - da 4 a 6 = MISURE: fare NOTIFICA e non COMUNICAZIONE all'interessato, effettuare il trattamento dell'evento vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach;
C. Valore Data Breach - da 7 a 8 = MISURE: fare NOTIFICA, fare la COMUNICAZIONE all'interessato, effettuare il trattamento dell'evento vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach;
D. Valore Data Breach – oltre 8 = MISURE: fare NOTIFICA, fare la COMUNICAZIONE all'interessato, effettuare il trattamento dell'evento vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach;

I risultati dell'esito della analisi del rischio vanno riportati nel MODULO Gestione del Data Breach nella sezione S3 massimo entro 4 ore[1], dall'inizio della riunione del Team crisi. Dell'esito della decisione si informa il Titolare del trattamento (vedi parte Generale).

L'esito della casistica in cui cade la segnalazione deve essere riportato, a cura del Referente Privacy, nel REGISTRO degli incidenti.

SI RICORDA CHE:

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

a) Sono state messe 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; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;

[1] Considerare che, nel caso di comunicazione da parte del subresponsabie (situazione più critica) l'azione si conclude entro 52 ore dalla sua rilevazione

b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche – in tal caso è necessario documentare le misure nella scheda di violazione;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

6.2.6 AZIONI A SEGUITO DELLE DECISIONI

Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni:

- caso A – si aggiorna il MODULO Gestione del Data Breach Sezione S3; l'evento si chiude; non vengono effettuate ulteriori comunicazioni.
- caso B – si aggiorna il MODULO Gestione del Data Breach Sezione S3; si procede con le eventuali AC; si comunica internamente con il Responsabile dell'area interessata dall'evento, si NOTIFICA all'Autorità di controllo e si compila S4;
- caso C – si aggiorna il MODULO Gestione del Data Breach Sezione 3 ed il REGISTRO degli incidenti; si procede con la adozione di trattamento dell'evento, con le AC; si comunica internamente con il Responsabile dell'area interessata dall'evento; si NOTIFICA all'Autorità di controllo – compilare S4. Il Referente Privacy prepara un comunicato per gli interessati che verifica con il Titolare del trattamento – compilare S5. Il Titolare del trattamento comunica all'Organo di Governo.
- caso D – si aggiorna il MODULO Gestione del Data Breach Sezione 3 ed il REGISTRO degli incidenti; si procede con la adozione di trattamento dell'evento, con le AC; si comunica internamente con il Responsabile dell'area interessata dall'evento; si NOTIFICA all'Autorità di controllo – compilare S4. Il Referente Privacy prepara un comunicato per gli interessati che verifica con il Titolare del trattamento – compilare S5. Il Titolare del trattamento comunica all'Organo di Governo.

Il caso C ed il caso D, per le comunicazioni (NOTIFICA e COMUNICAZIONE obbligatorie agli interessati) debbono avvenire massimo entro 8 ore[2] dalla decisione presa.

Per le comunicazioni agli interessati ed al Garante vedi specifiche sezioni.

Da considerare che il trattamento dell'evento senza l'avvio della AC deve essere una situazione eccezionale: di norma contenere semplicemente la violazione e continuare con lo *status quo*, non è accettabile.

SI RICORDA CHE:

Non è richiesta la comunicazione all'Interessato se è soddisfatta una delle seguenti condizioni:

a) Sono state messe 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

[2] Considerare che, nel caso di comunicazione da parte del subresponsabie (situazione più critica) l'azione si conclude entro 60 ore dalla sua rilevazione

Personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei Dati Personali degli Interessati;
b) sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche – in tal caso è necessario documentare le misure nella scheda di violazione;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

6.2.7 INDICIZZAZIONE SUI MOTORI DI RICERCA

Nel caso in cui il Data Breach abbia riguardato la pubblicazione di dati in rete (ad esempio per errore sono state messe on line delle pagine), deve essere verificato, sui principali motori di ricerca che le pagine contenenti tali dati non siano stati indicizzati e, nel caso in cui fosse avvenuto, richiedere, ai motori di ricerca la rimozione (diritto all'oblio). Tale indagine deve essere fatta sia appena a monte del Data Breach sia ripetuta a distanza di una settimana, due settimane ed un mese dall'evento.

6.2.8 TRATTAMENTO DELL'EVENTO

Quando è previsto un trattamento dell'evento, ovvero una o più azioni volte a minimizzare gli impatti per gli interessati e ripristinare la situazione precedente all'evento (laddove possibile) il Team crisi definisce: modalità, responsabilità e tempi. Il Team tiene sotto controllo lo stato di avanzamento delle azioni di trattamento previste e tiene aggiornato il MODULO Gestione del Data Breach Sezione 7 ed il REGISTRO degli incidenti (sezione data di completamento del trattamento).

6.2.9 AZIONE CORRETTIVA

Quando sono previste una o più azioni correttive volte a rimuovere la causa dell'evento, il Team crisi definisce: modalità, responsabilità e tempi. Il Team tiene sotto controllo lo stato di avanzamento delle azioni e l'efficacia delle stesse. Viene valutata la necessità di aggiornare l'analisi dei rischi ed eventualmente la PIA se prevista per tale trattamento e la documentazione (es. procedure di riferimento nomina a responsabile esterno del trattamento). Il Team crisi tiene aggiornato il MODULO Gestione del Data Breach Sezione 8 ed il REGISTRO degli incidenti (sezione data di completamento della Azione correttiva).

6.2.10 COMUNICAZIONE AL GARANTE ED AGLI INTERESSATI

A seguito di un evento di Data Breach deve essere effettuata la comunicazione al Garante ed agli interessati. La comunicazione è coordinata dal Team Crisi. Le evidenze di tutte le comunicazioni debbono essere conservate.

6.2.10.1 COMUNICAZIONI AL GARANTE

La comunicazione al Garante deve avvenire utilizzando il modello messo a disposizione dall'Autorità Garante stessa e rinvenibile al seguente link:
https://servizi.gpdp.it/databreach/s/

6.2.10.2 COMUNICAZIONE AGLI INTERESSATI

La comunicazione agli interessati può avvenire con modalità diverse tra cui:

- comunicazione diretta agli interessati
- comunicato stampa
- comunicazione tramite sito WEB/social media
- altre forme

Il Titolare del trattamento, supportato dal Referente Privacy, decide la strategia di *crisis communication* da mettere in atto da quando è a conoscenza durante dell'evento di Data Breach ed anche successivamente quando l'evento è stato risolto.

Di seguito le linee guida da considerare per la redazione delle comunicazioni verso gli interessati

Aspetti generali:

- definire il tono della comunicazione che può essere più informare (comunicato) o più formale (dichiarazione ufficiale)
- fornire un titolo "giornalistico" che per quanto possibile rassicuri gli interessati o perlomeno riducano il livello di allarme, utilizzare parole chiave facilmente rintracciabili sui motori di ricerca qualora venissero ricercate informazioni sui motori di ricerca
- le comunicazioni potrebbero non riguardare solo il Data Breach (rilevazione) ma anche le informazioni sull'andamento dello stesso nel tempo
- assicurare forme di comunicazione oneste, concrete e trasparenti
- fare riferimento al Team crisi, il suo ruolo ed il suo impegno
- mettere in evidenza la storia, l'impegno della azienda nell'assicurare l'attenzione al tema, gli investimenti fatti, le misure applicate
- descrivere l'evento in modo facilmente comprensibile, quale impatto ha avuto sui dati (o quale impatto presumibile può avere – informazioni perse, violate, comunicate a terzi non autorizzati, diffuse, ecc), come lo si sta affrontando/è stato affrontato, specificare cosa l'azienda sta facendo concretamente per proteggere i dati degli interessati
- indicare come e quando è stato coinvolto il Garante della Protezione dei dati
- inserire un contatto diretto per contattare l'organizzazione
- considerare di attivare un numero verde per rispondere agli interessati

Aspetti specifici per il comunicato stampa/dichiarazione ufficiale:

- prevedere link a pagina del sito web dove è reperibile ulteriore informazione sul Data Breach ed anche lo stato dell'andamento dello stesso nel tempo

Aspetti specifici per la comunicazione tramite sito WEB/social media:

- Considerare di pubblicare (per le situazioni più gravi) anche un video di scuse/spiegazioni coinvolgendo il top management, affidarsi ad un esperto, qualora non si disponesse internamente di tali competenze, per evitare errori o creare più allarme del necessario
- considerare di attivare una APP dedicata all'evento

La comunicazione agli interessati deve contenere almeno i seguenti elementi:

Mittente:

Destinatario: [Nome e indirizzo dell'interessato colpito]

Introduzione...

In data [gg/mm/aaaa] abbiamo riscontrato una violazione dei suoi/tuoi dati personali.

Come conseguenza della sopra menzionata violazione, i suoi/tuoi dati personali potrebbero essere stati:

- € *Divulgati*
- € *Distrutti*
- € *Persi*
- € *Modificati*
- € *È stato eseguito l'accesso*
- € *Altro [specificare]*

da persone non autorizzate.

La/ti informiamo che la violazione dei dati personali potrebbe avere le seguenti conseguenze: [elencare]

Per affrontare la violazione dei dati sono state/saranno implementate le seguenti misure: elencare

Se avete/hai quesiti in merito alla violazione dei dati, potete/puoi contattare [nome] via mail all'indirizzo [...@....], o via posta all'indirizzo [indirizzo fisico].

La modalità di invio della comunicazione ed i riferimenti degli interessati coinvolti deve essere riportata nel MODULO Gestione del Data Breach Sezione 7

6.2.11 COMUNICAZIONE ALL'ORGANO DI GOVERNO DEL TITOLARE

A seguito di un evento che ricade nei casi 4 e 5, ed in ogni caso qualora il Titolare del trattamento lo ritenesse opportuno, deve essere tenuto aggiornato l'Organo di governo.

Tale attività è a cura del Titolare del trattamento e deve avvenire con modalità, per quanto possibili rintracciabili.

6.2.12 VIOLAZIONI DEI DATI SITI IN PAESI TERZI CHE NON GARANTISCONO L'APPLICAZIONE DEL GDPR

Nel caso in cui ciò avvenga deve essere regolamentato (non necessariamente nella presente procedura, ma cmq richiamato dalla presente procedura):

- l'interessato deve dare il suo consenso per tale tipo di trattamento
- il Titolare deve determinare come intende ricevere la comunicazione dal Responsabile sito nel Paese terzo e le azioni e tempistiche da mettere in atto, nonché le istruzioni fornite al Responsabile sito nel Paese terzo e come controlla il rispetto a tali procedure

6.2.13 SITUAZIONI ANOMALE O DI EMERGENZA

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- chiusura temporanea della sede del Titolare (es. periodo di ferie)
- mancanza di figure apicali del Team crisi
- mancanza di collegamenti (es. internet)/energia/situazioni di emergenza dovute a cause di forza maggiore)

Devono essere considerate le seguenti misure:

- Il Team crisi può operare anche con una sola persona tra quelle che compongono il Team
- Le riunioni del Team possono essere effettuate in luoghi diversi dalla sede del titolare ed eventualmente con strumenti quali skype, ecc
- Indisponibilità del server (per manutenzione programmata) o altri eventi che possono non garantire il presidio dei sistemi deve essere comunicato anche nel sito internet (quando possibile)
- Nei periodi di chiusura (settimana di agosto e periodo natalizio) è affisso un cartello sulla porta della sede, è registrato un messaggio specifico sulla segreteria telefonica, comunicazione sulla home page del sito internet

ALLEGATI ALLA PRESENTE PROCEDURA:

- MODULO Gestione del Data Breach
- REGISTRO degli incidenti

Ultima rev, 05.12.2024

Il Titolare

COMUNE DI .....