COMUNE DI PANDINO

Provincia di Cremona

Area Affari Generali

26025 - Via Castello n° 15 - P.IVA 00135350197

☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

CODICE ENTE: 107708 PANDINO

DELIBERAZIONE N° 21 del 21/02/2022

V E R B A L E D I D E L I B E R A Z I O N E D E L L A G I U N T A C O M U N A L E

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

L'anno **DUEMILAVENTIDUE**, addì **VENTUNO** del mese di **FEBBRAIO** alle ore **13:00,** convocata nei modi di legge, si è riunita la Giunta Comunale.

La seduta viene svolta interamente in videoconferenza e si attesta la contestuale presenza dei componenti:

All'appello risultano:

COGNOME E NOME	QUALIFICA	PRESENTE
BONAVENTI PIERGIACOMO	Sindaco	SI
SAU FRANCESCA	Assessore e Vice Sindaco	SI
VANAZZI FRANCESCO	Assessore	SI
BOSA RICCARDO	Assessore	SI
SGRO' SARA	Assessore	SI

PRESENTI: 5 ASSENTI: 0

I componenti sono tutti collegati da remoto con videocamera e dispositivo informatico

Partecipa e verbalizza il Segretario Comunale Dott. Cameriere Enrico Antonio collegato da remoto con dispositivo informatico.

Il Presidente, accertato con l'ausilio del Segretario Comunale, il numero legale dei componenti della Giunta presenti in videoconferenza simultanea, nonché accertato che gli stessi hanno dichiarato che il collegamento in videoconferenza assicura una qualità sufficiente per comprendere gli interventi e constatare le votazioni, dichiara aperta la seduta ed invita la Giunta Comunale a trattare il seguente argomento:

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

LA GIUNTA COMUNALE

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale é 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;

CONSIDERATO che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:
- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

TENUTO presente che tale evoluzione ha indotto l'Unione europea ad adottare 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 (di seguito solo "GDPR");

DATO ATTO che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

RILEVATO che, con il GDPR, è stato richiesto agli Stati membri:
- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

VISTO il D. lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

DATO ATTO che il GDPR introduce l'obbligo di notificare all'autorità di controllo nazionale (Garante Privacy) incidenti sulla sicurezza che comportino la violazione dei dati personali (data breach) e di rendere nota la violazione stessa alle persone fisiche interessate;

DATO ATTO che la notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:
- descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;

- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o da adottare 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. Tenuto presente che la violazione dei dati personali è da intendersi come 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 tale da impedire al titolare del trattamento di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del GDPR;

DATO ATTO che, 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, e che tale comunicazione deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali, contenendo obbligatoriamente i seguenti contenuti minimi:
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi;

RILEVATO che, per quanto sopra, è necessario istituire:
1) una procedura data breach;
2) un registro interno data breach, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere i seguenti dati:
- i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
- gli effetti e le conseguenze della violazione;
- i provvedimenti adottati per porvi rimedio;
- il ragionamento alla base delle decisioni prese in risposta a una violazione (con particolare riferimento alle violazioni non notificate ed alle violazioni notificate con ritardo);

DATO ATTO che la Procedura data breach, avente lo scopo di indicare le modalità di gestione del data breach, garantisce la realizzabilità tecnica e la sostenibilità organizzativa;

DATO ATTO che il responsabile del procedimento, è il Segretario Comunale e che lo stesso, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità sulle azioni da intraprendere e sui comportamenti da adottare in caso di data breach, è tenuto a garantire la pubblicazione della Procedura data breach sul sito web istituzionale nella sezione "Amministrazione Trasparente", sottosezione di primo livello "Altri Contenuti", sottosezione di secondo livello "Privacy", nonché a garantire la conoscibilità della stessa a tutti i dipendenti dell'Ente;

DATO ATTO che il procedimento di adozione e approvazione della Procedura data breach e del registro data breach e il presente provvedimento, risultano mappati dal PTPC e che sono stati effettuati i controlli previsti dal Regolamento Sistema controlli interni ed è stato rispettato quanto previsto dal Piano Triennale di Prevenzione della corruzione e dal Programma per la trasparenza;

VISTI:
- il D.Lgs. 267/2000;

- la Legge 241/1990;
- il D.Lgs. 196/2003;
- la Legge 190/2012;
- il D.Lgs. 33/2013;
- il Regolamento (UE) n. 679/2016;
- lo Statuto Comunale;
- il Regolamento di organizzazione degli uffici e dei servizi;
- il Regolamento sul trattamento dei dati sensibili;
- il Codice di comportamento interno dell'Ente;

VISTO il parere favorevole espresso dal Responsabile del Settore in ordine alla regolarità tecnica del presente atto (art. 49, 1° comma, D.Lgs. 267/2000);

CON VOTI unanimi favorevoli espressi nelle forme di legge per appello nominale ed in forma palese ed espressa, in conformità alla lett. c) delle linee guida sullo svolgimento delle giunte a distanza di cui alla delibera di Giunta Comunale n. 42 del 18/03/2020,

DELIBERA

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1) di approvare la Procedura per la gestione di data breach ai sensi del Regolamento (UE) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale;

2) di disporre che al presente provvedimento venga assicurata:
a) la pubblicità legale con pubblicazione all'Albo Pretorio:
b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione Trasparente, sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";

3) di dare atto che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell'art.5 comma 2 D.Lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto;

4) di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

Con votazione separata,

CON VOTI unanimi favorevoli espressi nelle forme di legge per appello nominale ed in forma palese ed espressa, in conformità alla lett. c) delle linee guida sullo svolgimento delle giunte a distanza di cui alla delibera di Giunta Comunale n. 42 del 18/03/2020,

DELIBERA

di dichiarare il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 134, comma 4, del decreto legislativo 18 agosto 2000, n. 267.

Letto, confermato e sottoscritto

IL SINDACO
Bonaventi Piergiacomo
Firmato digitalmente

Il Segretario Comunale
Dott. Cameriere Enrico Antonio
Firmato digitalmente

COMUNE DI PANDINO

Provincia di Cremona

26025 - Via Castello n° 15 - P.IVA 00135350197

☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA COMUNALE

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

PARERE DI REGOLARITA' TECNICA

Si esprime parere favorevole di regolarità tecnica espresso ai sensi dell'art. 49 del T.U. approvato con D.Lgs. 18 Agosto 2000 n. 267, in quanto la proposta che precede è conforme alle norme legislative e tecniche che regolamentano la materia.

Pandino**,** lì **18/02/2022**

Il Segretario Comunale
CAMERIERE ENRICO ANTONIO /
INFOCERT SPA
Firmato digitalmente

COMUNE DI PANDINO

Provincia di Cremona
Area Affari Generali
26025 - Via Castello n° 15 - P.IVA 00135350197
☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

CODICE ENTE: 107708 PANDINO

DELIBERAZIONE N° 21 del 21/02/2022

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

ADEMPIMENTI RELATIVI ALLA PUBBLICAZIONE

La sopra estesa deliberazione:

- ai sensi dell'art. 124, comma primo, D. Lgs. 18/08/2000 n. 267, viene pubblicata all'Albo Pretorio del Comune in data odierna ed ivi rimarrà per 15 giorni consecutivi;

- è stata comunicata in data odierna ai Capigruppo Consiliari ai sensi dell'art. 125 del D. Lgs. 18/08/2000 n. 267.

Pandino, lì 24/02/2022

Responsabile Area Affari Generali
MANZONI MARGHERITA MARIA /
INFOCERT SPA
Firmato digitalmente

COMUNE DI PANDINO

Provincia di Cremona
Area Affari Generali
26025 - Via Castello n° 15 - P.IVA 00135350197
☎ 0373/973300 - 🖷 0373/970056 ✉ e-mail:segreteria@comune.pandino.cr.it

CODICE ENTE: 107708 PANDINO

DELIBERAZIONE N° 21 del 21/02/2022

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

CERTIFICATO DI ESECUTIVITA'

La presente deliberazione è divenuta esecutiva in data odierna, decorsi 10 giorni dalla pubblicazione, ai sensi dell'art. 134, comma 3°, del T.U. approvato con D. Lgs. 18 agosto 2000 n. 267.

Pandino, lì 21/03/2022

Responsabile Area Affari Generali
MANZONI MARGHERITA MARIA /
InfoCamere S.C.p.A.
Firmato digitalmente

Policy Data Breach

COMUNE DI PANDINO - Via Castello,15 26025 Pandino (CR)

PREMESSA
Ai fini del presente documento il Titolare del trattamento è identificato con la figura del Rappresentante Legale del Comune o un Suo delegato/Data Manager in considerazione degli interventi che devono essere decisi in breve tempo. In particolare ci si sta riferendo al Sindaco nel caso di un comune.

SCOPO
La presente procedura regolamenta la gestione degli eventi di Data Breach o quelli che vengono, in prima battuta considerati come tali. 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 da codesto ente. Tali eventi comportano rischi per i diritti e le libertà degli interessati. I principali rischi sono i seguenti:

- *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 Rappresentante Legale);*
- *decifratura non autorizzata della pseudonimizzazione;*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).*

1. GENERALE

1.1 Team crisi

La presente procedura è condivisa con i membri del Team crisi all'atto della loro nomina.
Il team crisi di Comune di Pandino è composto da:

- DPO:
- Data Manager: Segretario Comunale
- Privacy Officer area Economico Finanziario Personale
- Privacy Officer area Affari Generali Segreteria
- Privacy Officer area Affari Generali Servizi Demografici:
- Privacy Officer area Lavori Pubblici , Urbanistica, Ambiente, SUAP, Promozione Culturale e Turismo del Comune di Pandino
- Privacy Officer area Polizia Locale
- Privacy Officer area Servizi Sociali e Istruzione:

Di seguito il Team di Crisi verrà denominato in sigla TdC.
Possono far parte del team Crisi altri Privacy Officer qualora la violazione dei dati si verificasse nell'area di propria competenza nonché a seconda della verificazione dell'evento responsabili esterni o subresponsabili ove necessario.
Il Team crisi o soggetti da questo delegati, sono i soli autorizzati a trattare con il Garante e con gli interessati.

1.1.1 Formazione del Team crisi

Almeno annualmente 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. Nel corso della formazione, si valuta anche la necessità/opportunità di modificare/integrare la procedura sulla base degli eventi eventualmente verificatisi nel corso dell'anno. La formazione e la verifica dell'adeguatezza della procedura debbono essere verbalizzate. Il documento viene archiviato nell'archivio "privacy" dell'ente.

1.1.2 Nomina di responsabili esterni, subresponsabili

Nell'atto della nomina di responsabili esterni, Subresponsabili, deve essere indicato:

- la richiesta di valutazione delle loro procedure di Data Breach;
- la specificazione dei tempi di comunicazione all'ente che deve tener conto delle 72 ore a capo del Rappresentante legale per la segnalazione;
- le conseguenze nel caso di mancata o ritardata comunicazione;
- i riferimenti di contatto: *segreteria@comune.pandino.cr.it,* di seguito questa email verrà definita in seguito come Email di Riferimento (in sigla EdR).

1.1.3 Verbalizzazione delle attività

Tutte le attività e le riunioni del Team crisi debbono essere verbalizzate.

I Verbali sono conservati dal Data Manager, nell'archivio "privacy" dell'ente e conservati 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.

1.1.4 Disponibilità e Posizione del titolare

Il Titolare o suo delegato 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 Rappresentante Legale non fosse disponibile a fornire il contributo richiesto, il Data Manager ha l'Autorità per procedere autonomamente nelle decisioni prese.

Qualora il Rappresentante Legale non condividesse la decisione presa dal Team e la valutasse eccessiva e tale da impattare negativamente sulla reputazione/immagine del Comune o ledere gli interessi economici dello stesso, si assume la responsabilità di imporre la sua decisione. In questo caso il Team di Crisi verbalizzerà la decisione del Rappresentante Legale nel MODULO Gestione del Data Breach Sezione S9, la posizione del Team ed archivierà la documentazione senza procedere ulteriormente, tramite comunicazioni con data certa (es. tramite PEC) al Rappresentante Legale.

In ogni caso il Data Manager è autonomo nel valutare, in caso di contrasto con il Rappresentante Legale di comunicare l'evento occorso direttamente al Garante nelle forme e modi che ritiene opportuni.

1.1.5 Ruolo di eventuali esperti esterni

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

1.2 Data Breach Policy

La policy è predisposta dall'Organo di Governo dell'ente e verificata ad intervalli a cura del Rappresentante Legale/ Data Manager. La finalità della policy è quella di comunicare all'esterno dell'ente la presenza di una modalità per la gestione delle segnalazioni che possono portare a situazioni anomale/di sospetto o Data Breach.

La mail di contatto di segnalazione: EdR (come da indicazioni al punto 1.1.2) è reindirizzata nella casella di posta elettronica Data Manager.

Il Comune di Pandino ha previsto, al fine di tutelare i suoi dati personali, una Data Breach policy, per affrontare al meglio le ipotesi di violazione dei dati personali.

Ciò, in quanto, una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, causare danni alla persona fisica.

La violazione dei dati personali può consistere nella distruzione, perdita, modifica, divulgazione

non autorizzata o dall'accesso, in modo accidentale od illegale, a dati personali trasmessi, conservati o comunque trattati.
Riteniamo opportuno approfondire i rischi che potrebbero derivare dalle violazioni sopra elencate.
Ai sensi del Regolamento europeo, infatti, i principali rischi per i diritti e le libertà di tutti gli interessati, a seguito dell'avvenuta violazione dei dati sono:

- *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 Rappresentante Legale);*
- *decifratura non autorizzata della pseudonimizzazione;*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).*

Le cause che possono portare a tale 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.*

1.2.1 Data Breach Policy

Nel caso in cui si verifichi una violazione dei suoi dati personali l'ente ha previsto espressamente una procedura d'intervento.

Il Team crisi, composto come indicato in TdC (precedentemente al punto 1.1).

Questo Team si occuperà di analizzare la gravità dell'evento prendendo in considerazione i dati, gli interessati coinvolti, la portata e l'arco temporale secondo precisi parametri individuati da Comune di Pandino
A seguito di tale analisi l'ente realizzerà un'approfondita valutazione del rischio al fine di comprendere l'effettiva sussistenza o meno della violazione.
In caso di esito positivo il Team procederà alla risoluzione del problema.

Inoltre, in caso di violazione dei dati l'ente deve comunicare al Garante Privacy entro 72 ore dal fatto, l'evento.
Per tale ragione, qualora, della violazione ne sia venuto a conoscenza un nostro Responsabile esterno del trattamento o sub responsabile essi sono tenuti a comunicarci la violazione, il primo entro 24 ore, il secondo entro 12 ore dalla scoperta del fatto.
Qualora, infatti, la violazione dei dati abbia cagionato un rischio elevato per i diritti e le libertà fondamentali degli interessati, siamo tenuti a fornire un'opportuna comunicazione al fine di consentirle di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione.

Nella comunicazione siamo tenuti a comunicare agli interessati:

- *il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
- *le probabili conseguenze della violazione dei dati personali;*
- *le misure adottate o di cui si propone l'adozione da parte del Rappresentante Legale per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

Non siamo obbligati ad informare gli interessati nel caso in cui siano state attuate misure tecniche ed organizzative adeguate di protezione sui dati oggetto della violazione o quando abbiamo successivamente adottato misure atte a scongiurare nuovi rischi elevati per i diritti degli interessati ed inoltre, quando la comunicazione richiederebbe sforzi sproporzionati. In questo caso procederemo con una comunicazione pubblica o misura simile. In ogni caso valuteremo l'opportunità, anche se non strettamente obbligatoria di tenere aggiornati gli interessati.

Se un terzo esterno all'azienda venisse a conoscenza di una violazione dei dati personali potrà comunicarla scrivendoci al seguente indirizzo e-mail : EdR (come da indicazioni al punto 1.1.2) *tale comunicazione verrà presa in esame dal team crisi, che procederà come sopra descritto.*

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

1.4 Rendicontazione delle attività del Team Crisi
Almeno annualmente il Dpo/Data Manager predispone una relazione sull'attività del Team Crisi nel corso dell'anno. Tale relazione viene trasmessa all'Organo di governo dell'ente.
La relazione, per quanto possibile è integrata da dati numerici per comprendere l'entità degli eventi ed i tempi di reazione.

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.

2.1 Segnalazione
La segnalazione di un evento può provenire:
- interno – ogni autorizzato al trattamento deve, nel caso abbia 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 ad uno dei membri del Team di crisi 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 (interessato/Garante/stampa) –
  - il Data Manager raccoglie le segnalazioni di possibile Data Breach provenienti dall'esterno in qualsiasi forma;
  - il Data Manager consulta regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio che potrebbero riguardare anche il Comune di Pandino;
  - in entrambi i casi il Data Manager comunica via mail con gli altri membri del Team crisi utilizzando la loro casella di posta e quella di: EdR (come da indicazioni al punto 1.1.2) (al fine di lasciare una traccia) e procede quindi alla comunicazione telefonica.
- Responsabile esterno trattamento/subresponsabile/ - il Data Manager 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. e-mail – che l'attesta in modo univoco).

2.1.1 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 Data Manager il REGISTRO degli incidenti.

2.2 Valutazione di pertinenza della segnalazione

Raccolta la segnalazione, attraverso le forme sopra indicate, il Data Manager crisi convoca entro massimo 12 ore dalla segnalazione[1], una riunione coinvolgendo tutti i membri ed eventuali altri soggetti potenzialmente coinvolti sulla base delle informazioni disponibili. Qualora qualche membro non fosse disponibile si proceda comunque con la riunione.
Il team compila il MODULO Gestione del Data Breach nella sezione 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 porta 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 Rappresentante Legale (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 Rappresentante Legale;
- valutare la 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 nel MODULO Gestione del Data Breach nella sezione S2.
In caso di esito positivo procede con l'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 Data Manager, nel REGISTRO degli incidenti. Se la segnalazione non risulta pertinente il Data Manager traccerà una riga per annullare la compilazione degli altri campi previsti dal REGISTRO.

2.3 Analisi del rischio

Il Team crisi procede all'analisi del rischio ed alla sua documentazione compilando il MODULO Gestione del Data Breach nella sezione S3. Nella compilazione del modulo devono tenere conto del significato associato a:

- riservatezza: stima del danno/impatto che la perdita di riservatezza riguardante l'asset comporterebbe per il business dell'ente o/tutela interessato (1-3);
- integrità: stima del danno/impatto che la perdita di integrità riguardante l'asset comporterebbe per il business dell'ente /tutela interessato (1-3);

[1]Considerare che, nel caso di comunicazione da parte del subresponsabile (situazione più critica) l'azione si avvia entro 36 ore dalla sua rilevazione

- disponibilità: stima del danno/impatto che la perdita di disponibilità riguardante l'asset comporterebbe per il business dell'ente /tutela interessato (1-3).

Per la valutazione della stima della perdita di Riservatezza, Integrità e Disponibilità viene utilizzata la seguente tabella.

Liv[2].	R- Riservatezza	I – Integrità	D- Disponibilità
1 - Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere;. - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; − esclusione; − perdita di liberta; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; − esclusione; − perdita di liberta; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.

2

2 - Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.

3 - Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di **disponibilità** ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.

4 - Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatto sulla sopravvivenza degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di integrità ha impatto sulla sopravvivenza degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà; − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. **Interessati** La mancanza di disponibilità ha impatto sulla sopravvivenza degli interessati in termini di: − perdita di autonomia; − esclusione; − perdita di libertà − danni fisici; − stigmatizzazione; − squilibrio di potere; − perdita di fiducia; − perdita economica.

2.3.1 Tipologia di dato violato

Si indicano i valori da attribuire in base alle tipologie di dato violato:
- dati sanitari: 0 se non sono oggetto di violazione oppure 3 se lo sono;
- documenti di identità: 0 se non sono oggetto di violazione e 2 se lo sono;
- n. carta di credito: 0 se non sono oggetto di violazione e 2 se lo sono;
- reddito, fatturato: 0 se non sono oggetto di violazione e 1 se oggetto di violazione;
- brevetti, strategie di marketing, segreti professionali: 0 se non sono oggetto di violazione e 2 se violati;
- biometria es impronte digitali, riconoscimento vocale ecc: 0 se non sono oggetto di violazione e 3 se sono oggetto di violazione;
- facilità di identificazione degli interessati: 0 se non presente e 1 se sussiste;
- gravità delle conseguenze degli individui: 0 se non presente e 3 se sussiste;
- dati giudiziari: 0 se non oggetto della violazione e 3 se presenti;
- dati sui minori: 0 se non oggetto della violazione e 3 se lo sono;
- dati sulla geolocalizzazione: 0 se oggetto di violazione e 3 se presenti;

- dati su abitudini dell'interessato, dati comportamentali: 0 se non oggetto della violazione e 3 se presenti;
- violazione massiva o individuale in base all'universo di riferimento: 0 se non sussiste, 1 se individuo singolo, 2 se gruppo limitato e 3 violazione massiva;
- criptazione: 0 se presente e 3 se non presente;
- copia back up: 0 se presente e 3 se non presente.

2.3.2 Dati violati oggetto di DPIA (valutazione d'impatto del rischio).

Nel caso in cui il trattamento oggetto di violazione sia stato in precedenza sottoposta ad una DPIA (valutazione d'impatto del rischio). tenendo conto sia dell'art 35 GDPR nonché di quanto indicato nelle "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati[3]" pubblicate dal WP 29, il punteggio base da attribuire, al fine di valutare la sussistenza di un "rischio elevato", ai sensi del regolamento 2016/679", è pari a 6.

In tal caso, considerato che il punteggio minimo associato ad ogni evento è pari a 3, ne consegue che in caso di almeno una DPIA (valutazione d'impatto del rischio). il punteggio minimo associato all'evento di data breach è pari a 9 (vedi punto C del paragrafo "2.4 Esito della analisi del rischio e decisioni"), quindi, è necessario procedere con la notifica al Garante.

Posto che un'unica DPIA può avere ad oggetto più trattamenti che presentino analogie in termini di natura, ambito, contesto, finalità e rischi, il punteggio da associare (valore 6) riguarda il numero di trattamenti e non quello delle DPIA effettuate.

In ogni caso, qualora il trattamento oggetto della violazione non fosse stato sottoposto ad una DPIA (valutazione d'impatto del rischio)., ma nel corso dell'analisi emergesse un'errata valutazione sulle ragioni che avevano determinato l'omessa valutazione d'impatto del rischio ex art 35 GDPR o qualora si prendesse semplicemente atto della mancanza di una DPIA (valutazione d'impatto del rischio). nel calcolo del rischio si ritiene di applicare la posizione più prudenziale, quindi, risulta necessario associare al trattamento oggetto della valutazione, il punteggio massimo (valore 6).

2.4 Esito della analisi del rischio e decisioni

Il risultato del calcolo del rischio deve essere interpretato come segue, considerando che, in base ai criteri assegnati il valore minimo è 3 ed il massimo è 56 ed in caso di più dpa superiore ad esso :

[3]I criteri da considerare per l'effettuazione di una PIA si basano sul rischio per gli interessati e possono riguardare un trattamento o un insieme di trattamenti simili. Tali criteri riguardano i seguenti aspetti:
I dati sono oggetto di

- valutazione, assegnazione di un punteggio, incluso la profilazione
- decisione automatiche che hanno effetti giuridici o simili con un impatto significativo per l'interessato
- i dati sono sensibili con elaborazione sistematica e su larga scala
- elaborazione su larga scala (in termini assoluti – numero interessati, numero di dati trattati -, di incidenza %, durata e/o permanenza del trattamento, estensione geografica del trattamento/elaborazione- si veda anche quanto indicato nel considerando 91 del GDPR)
- abbinamento e combinazione dei dati provenienti da più operazioni di trattamento
- di un uso innovativo
- trasferimento fuori dai confini della UE (considerando 116 del GDPR), possibile oggetto di trasferimento o probabilità di trasferimento basate su deroghe a situazioni specifiche stabilite dal GDPR

attraverso i dati è possibile effettuare:

- un controllo sistematico (osservazione, monitoraggio, controllo) degli interessati
- applicazione di soluzioni tecnologiche o organizzative innovative

gli interessati a cui appartengono i dati:

- sono vulnerabili (considerando 75 del GDPR) e/o in presenza di un notevole squilibrio di potere tra l'interessato ed il titolare
- sono impediti nell'esercizio di un diritto o di utilizzare un servizio o un contratto (considerando 91 ed articolo 22 del GDPR)

- caso 1 - 6 = nessun rischio calcolato (non fare NOTIFICA e COMUNICAZIONE e valutare eventuale AC vedi S8);
- caso 2- da 7 a 18 = rischio che implica: la adozione di trattamento dell'evento vedi S7 ed eventuale AC vedi S8 del MODULO Gestione del Data Breach;
- caso 3- da 19 a 34 = rischio che implica: la adozione di trattamento dell'evento vedi S7, la NOTIFICA obbligatoria all'autorità di controllo trattamento dell'evento vedi S4 e l'AC vedi S8 del MODULO Gestione del Data Breach;
- caso 4 – oltre 35 = rischio che implica: quanto previsto al caso 3 ed anche la COMUNICAZIONE obbligatoria agli interessati coinvolti vedi S5.

I risultati dell'esito della analisi del rischio vanno riportati nel MODULO Gestione del Data Breach nella sezione S3 massimo entro 4 ore[4], dall'inizio della riunione del Team crisi. Dell'esito della decisione si informa il Rappresentante legale.
L'esito della casistica in cui cade la segnalazione deve essere riportato, a cura del Data Manager, REGISTRO degli incidenti.

2.5 Azioni a seguito delle decisioni

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

- caso 1 – si aggiorna il MODULO Gestione del Data Breach Sezione 3; l'evento si chiude; non vengono effettuate ulteriori comunicazioni;
- caso 2 e 3 - si aggiorna il MODULO Gestione del Data Breach Sezione 3; si procede con le eventuali AC; si comunica internamente al Responsabile dell'area interessata dall'evento la adozione di trattamento dell'evento;
- caso 4 - si aggiorna il MODULO Gestione del Data Breach Sezione 3 ed il REGISTRO degli incidenti; si procede la adozione di trattamento dell'evento con le AC; si comunica internamente al Responsabile dell'area interessata dall'evento; si NOTIFICA all'autorità di controllo. Il Data Manager prepara un comunicato stampa che verifica con il Titolare. Il Titolare comunica all'Organo di governo dell'ente;
- caso 5 – implica, oltre a quanto previsto dal caso 4 anche la COMUNICAZIONE obbligatoria agli interessati coinvolti preparata a cura del Data Manager secondo il Modello e verificata da dal Titolare. Il Titolare comunica all'Organo di governo dell'ente.

Il caso 4 ed il caso 5, per le comunicazioni (NOTIFICA e COMUNICAZIONE obbligatorie agli interessati) debbono avvenire massimo entro 8 ore[5] dalla decisione presa.
Per le comunicazioni agli interessati ed al Garante si vedano le specifiche sezioni.
Da considerare che il trattamento dell'evento senza l'avvio della AC deve essere una situazione eccezionale: di norma deve contenere semplicemente la violazione e continuare con lo *status quo*, non è accettabile.

2.6 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.

2.7 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

[4]4 Considerare che, nel caso di comunicazione da parte del sub responsabile (situazione più critica) l'azione si conclude entro 52 ore dalla sua rilevazione
[5]5 Considerare che, nel caso di comunicazione da parte del sub responsabile (situazione più critica) l'azione si conclude entro 60 ore dalla sua rilevazione

avanzamento delle azioni e l'efficacia delle stesse. Viene valutata la necessità di aggiornare l'analisi dei rischi ed eventualmente la DPIA 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.

2.8 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.

2.8.1 Comunicazioni al Garante

La comunicazione al Garante deve contenere almeno i seguenti elementi:

- riferimenti dell' azienda e del Rappresentante Legale;
- indirizzo PEC e/o E-MAIL per eventuali comunicazioni;
- recapito telefonico per eventuali comunicazioni;
- eventuali Contatti (altre informazioni);
- natura della comunicazione;
- breve descrizione della violazione dei dati personali trattati;
- quando si è verificata la violazione dei dati personali trattati Specificare arco temporale o se la violazione è ancora in corso;
- dove è avvenuta la violazione dei dati? (es. se avvenuta a seguito di smarrimento di dispositivi o di supporti portatili);
- tipo di violazione;
- lettura (presumibilmente i dati non sono stati copiati);
- copia (i dati sono ancora presenti sui sistemi del Rappresentante Legale);
- alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- cancellazione (i dati non sono più sui sistemi del Rappresentante Legale e non li ha neppure l'autore della violazione);
- furto (i dati non sono più sui sistemi del Rappresentante Legale e li ha l'autore della violazione);
- dispositivo oggetto della violazione ed eventuale ubicazione (es. Computer, Rete, Dispositivo mobile, Archivio/File o parte di un archivio/file, Strumento di *backup,* Documento cartaceo) Altro:
- quanti interessati sono state colpiti dalla violazione dei dati personali N. interessati ed incidenza % sull'universo della popolazione/ Un numero (ancora) sconosciuto di interessati;
- che tipo di dati sono oggetto di violazione?
- Misure tecniche e organizzative applicate ai dati oggetto di violazione;
- eventuali azioni già intraprese per contenere la violazione;
- eventuali azioni già intraprese per ripristinare lo status quo (quando possibile);
- eventuali azioni correttive;
- la violazione è stata comunicata anche agli interessati?
- Sì, è stata comunicata il …e mezzo utilizzato.
- No, perché.
- Allegare l'analisi del rischio estrapolata dal MODULO Gestione del Data Breach e l'eventuale comunicazione inviata agli interessati.

2.8.2 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.

La comunicazione deve essere congruente con quanto indicato nella data Breach Policy.
Il data Manager ha la responsabilità per:

- individuare la/le forma/e di comunicazione da utilizzare;
- la responsabilità per la stesura ed approvazione delle comunicazioni;
- il livello di coinvolgimento del Team crisi nella comunicazione verso l'esterno; in ogni caso il Team crisi non può essere escluso.

Il Team crisi decide la strategia di *crisis communication* da mettere in atto da quando è a conoscenza 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 informale (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 sono reperibili ulteriori informazioni 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 dati personali.

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

- divulgati;
- distrutti;
- persi;

- Modificati
- è stato eseguito l'accesso;
- atro [specificare];

da persone non autorizzate.
La 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:

Se avete quesiti in merito alla violazione dei dati, potete contattare Comune di Pandino via e-mail all'indirizzo : EdR (come da indicazioni al punto 1.1.2) o via posta raccomandata all'indirizzo dell'ente, specificato nella copertina di questo documento o recuperabile sul sito internet dell'ente.
La modalità di invio della comunicazione ed i riferimenti degli interessati coinvolti deve essere riportata nel MODULO Gestione del Data Breach Sezione 7.
Di seguito esempio di comunicazione:
Comunicato stampa (ESEMPIO)
AAA, una APP per la pianificazione della pubblicazione di messaggi sui social media, è stata hackerata nell'ottobre del 20xx ma è riuscita a gestire in modo esemplare la situazione perché ha tempestivamente avvertito direttamente i clienti prima che la notizia andasse sui media.
Il livello di sincerità, proattività e commitment nella comunicazione via e-mail ai clienti ha determinato un effetto di fidelity e di trust presso i clienti e salvato l'azienda da una pericolosa perdita di reputation.
L'azienda non ha avuto paura di rivelare il Data Breach e ha strategicamente gestito la crisi per informare direttamente ed in modo costante i clienti. Hanno espresso vero rammarico e preso la situazione con grande serietà.
La prima cosa che ha fatto l'azienda immediatamente dopo il Data Breach è stata quello di mandare un'e-mail mandata direttamente dal CEO che ha evitato di "indorare" la situazione ma si è da una parte scusato in modo sincero e dall'altra ha rassicurato che tutta l'azienda era impegnata 24/7 per gestire la situazione.

Comunicazione agli interessati (ESEMPIO)
Volevo mettermi in contatto per scusarmi per la sgradevole esperienza che abbiamo causato a molti di voi durante il fine settimana. AAA è stato violato circa 1 ora fa, e molti di voi potrebbero aver avuto dei messaggi spam inviati tramite AAA. Posso comprendere quanto dovete essere arrabbiati e delusi in questo momento.
Non tutti coloro che si sono registrati su AAA sono stati interessati, ma potreste voler controllare i vostri account. Stiamo lavorando al massimo per risolvere questo problema in questo momento e ci aspettiamo di riportare tutto alla normalità a breve.
Stiamo pubblicando aggiornamenti continui sulla pagina Facebook di AAA e sulla pagina Twitter di AAA per tenervi aggiornati su tutto. I migliori passi da fare per voi adesso e informazioni importanti per voi:
Rimuovete qualsiasi messaggio dalla vostra pagina Facebook o Twitter che assomiglia a spam
Tenete d'occhio la pagina Twitter e la pagina Facebook di AAA
Le password di AAA non sono interessate.
Nessuna informazione di fatturazione o pagamento è stata influenzata o esposta.
Tutti i post di Facebook inviati tramite AAA sono stati temporaneamente nascosti e riappariranno una volta risolta questa situazione.
Siamo incredibilmente dispiaciuti per ciò che è successo che ha colpito voi e la vostra società. Stiamo lavorando tutto il giorno per risolvere il problema e continueremo a pubblicare aggiornamenti su Facebook e Twitter.

Se avete domande, rispondete a questa e-mail. Comprensibilmente, molte persone ci hanno inviato un'e-mail, quindi potremmo metterci un po' di tempo per rispondere a tutti, ma risponderemo ad ogni singola e-mail.
Nome referente e il team AAA.

Aggiornamento della comunicazione (ESEMPIO)
Buongiorno,
Volevo riprendere il discorso con voi dopo l'incidente di hacking di ieri. Per molti di voi questo ha seriamente rovinato la vostra giornata - Mi dispiace di aver causato questa terribile esperienza. La squadra AAA ha lavorato tutto il giorno e sono felice di dire che siamo di nuovo operativi. Abbiamo anche passato tutto oggi aggiungendo diverse misure di sicurezza.
C'è un passaggio chiave per usare di nuovo AAA: dovrete ricollegare tutti i vostri account Twitter, anche se lo avete già fatto. Andate alla dashboard web di AAA per riconnettervi.
Altre cose importanti per voi da sapere:
La riconnessione non funzionerà con le APP mobili, tutti gli account Twitter dovranno essere ricollegati sulla dashboard web.
Il vostro post su Facebook sarà ripreso normalmente, non c'è nulla che dovrete fare.
L'accesso o la connessione di un nuovo account Twitter nell'app per iPhone non funzionerà finché il nostro nuovo aggiornamento non sarà approvato da Apple.
Voglio scusarmi ancora e dire che sono incredibilmente dispiaciuto per ciò che è accaduto a voi e in molti casi anche alla vostra azienda. Abbiamo scritto un post sul blog con aggiornamenti in corso mentre scopriamo tutti i dettagli.
Ciò che ci rimane da fare adesso è completare la nostra analisi tecnica e adottare ulteriori misure di sicurezza.
Ci sarà presto un altro aggiornamento su questo.
Voglio invitarvi di nuovo a rispondere a questa email o a pubblicare un commento sul nostro blog. Siamo sicuri di rispondervi il più velocemente possibile.
Nome referente e il team AAA.

2.8 Comunicazione all'Organo di governo di Comune di Pandino.
A seguito di un evento che ricade nei casi 4 e 5, ed in ogni caso qualora il Rappresentante Legale lo ritenesse opportuno, deve essere tenuto aggiornato l'Organo di governo di Comune di Pandino Tale attività è a cura del Rappresentante Legale e deve avvenire con modalità, per quanto possibili rintracciabili.

2.9 Situazioni anomale o di emergenza
In caso di segnalazioni in situazioni anomale o di emergenza, quali:
- chiusura temporanea della sede di Comune di Pandino (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:
- Le riunioni del Team possono essere effettuate in luoghi diversi dalla sede di Comune di Pandino ed eventualmente con strumenti quali Hangout, ecc. Nel caso in cui la persona non sia proprio raggiungibile si procede in assenza. In caso di impossibilità a rintracciare il Data Manager, di procederà a contattare il Rappresentante Legale o membri dell' Amministrazione Comunale.
- Indisponibilità del server (per manutenzione programmata) o altri eventi che possono non garantire il presidio dei sistemi deve essere comunicato anche nella sezione Data Breach Policy del sito internet (quando possibile).

ALLEGATI

- MODULO Gestione del Data Breach
- REGISTRO degli incidenti

	MODULO Gestione del Data Breach (art.33-34) del Comune di Pandino (CR)

S1 Segnalazione

ID N^/anno	
Data:	
Segnalante:	
Modalità di comuncazione	
Segnalazione:	
Allegati eventuali (es. mail)	
Membri presenti del team	
Decisione (Se proocedyre S2	

S2 Team crisi - conseguenze dell'evento

N^ interessati e/o %/N^ dati coinvolti:	
Dati personali:	
Portata dell'evento:	
Arco temporale che interessa	
Formato dati (carteceo/elettronico)	
Eventuali azioni per contenre effetti dell'evento	
Data:	
Violazione:	Sì

S3 Team crisi - analisi del rischio

			Valore del rischio
1	Violazione di riservatezza	da 1 a 4 + descrizione	
2	Violazione di disponibilità	da 1 a 4 + descrizione	
3	Violazione di integrità	da 1 a 4 + descrizione	
4	Natura dei dati violati: sanitari	No / Sì + descrizione	
5	Natura dei dati violati: doc. d'identità	No / Sì + descrizione	
6	Natura dei dati violati: numeri carte di credito	No / Sì + descrizione	
7	Natura dei dati violati: reddito, fatturato	No / Sì + descrizione	
8	Natura dei dati violati: brevetti, strategie di marketing, segreti professionali	No / Sì + descrizione	
9	Natura dei dati violati altri (es biometria) _____	No / Sì + descrizione	
10	Facilità d'identificazione degli interessati	No / Sì + descrizione	
11	Gravità delle conseguenze sugli individui in termini di danni fisici, materiali ed immateriali (approfondimento	No / Sì + descrizione	
12	Speciali caratteristiche dei dati violati: dati sanitari-giudiziari	No / Sì + descrizione	
13	Speciali caratteristiche dei dati violati: dati sui minori	No / Sì + descrizione	
14	Speciali caratteristiche dei dati violati: dati sulla localizzazione dell'interessato	No / Sì + descrizione	

	dati comportamentali			No / Sì + descrizione	
15	Speciali caratteristiche dei dati violati: dati sulle abitudini/preferenze dell'interessato			No / Sì + descrizione	
16	Numero di individui interessati: violazione massiccia o individuale anche in base all'universo di riferimento			No / Sì + descrizione	
	back up			No / Sì + descrizione	
17	Cryptazione dei dati (con crypatzione valore 0)			No / Sì + descrizione	
18	Esistenza di copie dei dati (con esistenza copia valore 0)			No / Sì + descrizione	
19	Presenza di almeno un trattamento oggetto di DPIA in relazione ai dati violati			No / Sì + descrizione	il punteggio attribuito è 6 per ogni trattamento oggetto di DPIAin relazione ai dati violati

Data:

TOTALE = risultato valore minimo 3 | 0

VALORE DATA BREACH = indicare da A) a D)

S4 Titolare: NOTIFICA all'autorità di controllo dello stato in cui è avvenuta la violazione

Documento di notifica:	
Modalità di invio	
Data e ora:	

S5 Titolare: COMUNICAZIONE agli interessati coinvolti

Comunicazione obbligatoria si /no se no motivazione	
Documento di comunicazione:	
Data e ora:	

S6 Decisione a non procedere con la segnlazione

Data:	
Motivazione	
Membri presenti del team	
Comunicazione a TdT	
Eventuale AC? (vai a S8)	

S7 Trattamento _____

Data:	
Trattamento	
Resaponsabile del trattament	
Tempi di effettuazione	
Comunicazione a TdT	
Esito ed azioni in caso di esito negativo	

S8 Azione correttiva

Data:	
Azione correttiva	
Resaponsabile della AC	
Tempi di effettuazione	
Comunicazione a TdT	
Valutazione di efficacia ed azioni in caso di esito negativo	
Eventuale aggiornamento AdR/PIA	
Eventuale aggiornamento documentazione	

S9 Decisione di interruzione della analisi da parte del Titolare

Data:	
Motivazione	
Membri presenti del team	
Comunicazione in data certa	
Allegato	

Registro degli incidenti del Comune di Pandino (CR)

				parte da compilare se si ricade nei casi 3 o 4				
ID	Data segnlazione	Valutazione di pertinenza della segnlazione	N^ Caso (da 1-a 4)	Comunicazione al Garante effettuata in data	Comunicazioni agli interessati effettuata in data	Data di completamento del trattamento	Data di completamento della azione correttiva	Altre informazioni